ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอม และระบบการแฝงข้อมูล

โดย

จิรภัทร ลาภวัฒนวรกุล

มหาวิทยาลัยรังสิต Rangsit University

ดุษฎีนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม
หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี

บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต
ปีการศึกษา 2567

BLOCKCHAIN-BASED AUXILIARY SYSTEM FOR PSEUDONYMIZATION AND CONSENT MANAGEMENT

BY

JIRAPHAT LAPWATTANAWORAKUL

มหาวิทยาลัยรังสิต Rangsit University

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR

THE DEGREE OF DOCTOR OF PHILOSOPHY

IN INFORMATION TECHNOLOGY

COLLEGE OF DIGITAL INNOVATION TECHNOLOGY

GRADUATE SCHOOL, RANGSIT UNIVERSITY

ACADEMIC YEAR 2024

ดุษฎีนิพนธ์เรื่อง

ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอม และระบบการแฝงข้อมูล

โดย

จิรภัทร ลาภวัฒนวรกุล

ได้รับการพิจารณาให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยรังสิต
ปีการศึกษา 2567

ศ. ดร.จาตุรงค์ ตันติบัณฑิต ประธานกรรมการสอบ	รศ. ดร.คริชณะ ฉิมมณี กรรมการ
รศ. ดร.สิริพร ศุภราทิตย์ กรรมการ	ผศ. ดร.กานต์ ยงศิริวิทย์ กรรมการ
ผศ. ดร.ภาคภูมิ ชัยศิริประเสริฐ กรรมการ	ผศ. ดร.ธรรณพ อารีพรรค กรรมการและอาจารย์ที่ปรึกษาร่วม

รศ. ดร.เชฏฐเนติ ศรีสอ้าน
กรรมการและอาจารย์ที่ปรึกษา

บัณฑิตวิทยาลัยรับรองแล้ว

(ศ. ดร.สื่อจิตต์ เพ็ชร์ประสาน)
คณบดีบัณฑิตวิทยาลัย
9 พฤษภาคม 2568

มหาวิทยาลัยรังสิต Rangsit University

Dissertation entitled

BLOCKCHAIN-BASED AUXILIARY SYSTEM FOR PSEUDONYMIZATION AND CONSENT MANAGEMENT

by

JIRAPHAT LAPWATTANAWORAKUL

was submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Information Technology

Rangsit University
Academic Year 2024

Prof. Charturong Tantibundhit, Ph.D. Examination Committee Chairperson	Assoc. Prof. Krishana Chimmanee, Ph.D. Member
Assoc. Prof. Siriporn Supratid, Ph.D. Member	Asst. Prof. Karn Yongsiriwit, Ph.D. Member
Asst. Prof. Parkpoom Chaisiriprasert, Ph.D. Member	Asst. Prof. Thannob Aribarg, Ph.D. Member and Co-Advisor

Assoc. Prof. Chetneti Srisa-an, Ph.D.
Member and Advisor

Approved by Graduate School

(Prof. Suejit Pechprasarn, Ph.D.)
Dean of Graduate School
May 9, 2025

กิตติกรรมประกาศ

ดุษฎีนิพนธ์เรื่อง ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล สำเร็จลุล่วงได้เป็นอย่างดีเนื่องมาจากได้รับความอนุเคราะห์จาก รศ. ดร.เชฎฐเนติ ศรีสอ้าน อาจารย์ที่ปรึกษา และ ผศ. ดร.ธรรณพ อารีพรรค อาจารย์ที่ปรึกษาร่วม ผู้ซึ่งให้ความรู้ คำแนะนำ คำปรึกษา และความเอาใจใส่ช่วยเหลือตลอดจนตรวจแก้ไขจนดุษฎีนิพนธ์นี้เสร็จสมบูรณ์ ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอกราบขอบพระคุณ ท่านผู้ทรงคุณวุฒิทุกท่านดังรายนามเหล่านี้ เป็นอย่างสูงยิ่งที่ให้ความกรุณารับเป็นกรรมการตรวจสอบดุษฎีนิพนธ์ และให้คำแนะนำ คำปรึกษา เป็นอย่างดีตลอดมาได้แก่ ประธานกรรมการสอบ ศาสตราจารย์ ดร.จาตุรงค์ ตันติบัณฑิต คณะกรรมการสอบ รศ. ดร.ดริชณะ ฉิมมณี รศ.ดร.สิริพร ศุภราทิตย์ ผศ. ดร.กานต์ ยงค์ศิริวิทย์ และ ผศ.ดร. ภาคภูมิ ชัยศิริประเสริฐ

ขอขอบพระคุณ รศ. ดร.ดริชณะ ฉิมมณี ท่านผู้อำนวยการหลักสูตร อย่างสูงยิ่งที่ทำให้การดูแล ช่วยเหลือ และสนับสนุนการดำเนินงานดุษฎีนิพนธ์นี้จนสำเร็จลุล่วงเป็นอย่างดี

ท้ายสุดขอขอบพระคุณอาจารย์และเจ้าหน้าที่ วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยีทุกท่านที่ให้คำแนะนำ คำปรึกษา และช่วยเหลือการดำเนินงานดุษฎีนิพนธ์นี้จนสำเร็จลุล่วง

จิรภัทร ลาภวัฒนวรกุล

ผู้วิจัย

มหาวิทยาลัยรังสิต Rangsit University

6504122 : จิรภัทร ลาภวัฒนวรกุล
ชื่อดุษฎีนิพนธ์ : ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล
หลักสูตร : ปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา : รศ. ดร.เชฎฐเนติ ศรีสอ้าน
อาจารย์ที่ปรึกษาร่วม : ผศ.ดร.ธรรณพ อารีพรรค

บทคัดย่อ

ในยุคดิจิทัลที่ข้อมูลส่วนบุคคลกลายเป็นทรัพยากรสำคัญสำหรับการดำเนินธุรกิจและการวิเคราะห์ทางสังคม การปกป้องข้อมูลส่วนบุคคลจึงเป็นเรื่องสำคัญอย่างยิ่ง โดยเฉพาะเมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น จีดีพีอาร์ในสหภาพยุโรปและพีดีพีเอในประเทศไทยได้บังคับใช้อย่างเข้มงวด ธุรกิจและองค์กรต่าง ๆ ต้องพัฒนาแนวทางและวิธีการเพื่อบริหารจัดการข้อมูลให้เป็นไปตามกฎหมายเหล่านี้ อย่างไรก็ตาม วิธีการปกป้องข้อมูลแบบเดิม เช่น การลบข้อมูลส่วนบุคคลหรือการทำให้ข้อมูลเป็นนิรนาม ยังคงมีข้อจำกัดและอาจถูกโจมตีเพื่อระบุตัวตนซ้ำได้ งานวิจัยนี้จึงนำเสนอเทคนิคใหม่ในการบริหารจัดการความยินยอมและการแฝงข้อมูลโดยใช้เทคโนโลยีบล็อกเชนเป็นระบบช่วยเหลือ วัตถุประสงค์ของงานวิจัยนี้คือการสร้างระบบที่สามารถบูรณาการสัญญาอัจฉริยะบนบล็อกเชนเพื่อจัดการความยินยอมของผู้ใช้ได้อย่างมีประสิทธิภาพและปลอดภัย อีกทั้งยังพัฒนาเทคนิคการแฝงข้อมูลที่รักษาความถูกต้องของข้อมูลพร้อมกับลดความเสี่ยงต่อการละเมิดความเป็นส่วนตัว วิธีการดำเนินงานเริ่มจากการออกแบบกรอบแนวคิดที่อิงตามข้อกำหนดทางกฎหมาย จากนั้นใช้ชุดข้อมูลมาตรฐานและชุดข้อมูลเพิ่มเติมในการทดลองเพื่อประเมินผลกระทบและประสิทธิภาพของระบบ ผลการวิจัยชี้ให้เห็นว่าระบบที่พัฒนาสามารถลดความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคลได้อย่างมีนัยสำคัญ โดยบล็อกเชนมีบทบาทสำคัญในการเสริมความมั่นใจในความปลอดภัยและความโปร่งใสของข้อมูล นอกจากนี้ระบบที่นำเสนอสามารถรองรับการปรับเปลี่ยนตามข้อกำหนดทางกฎหมายที่หลากหลาย ซึ่งช่วยส่งเสริมความไว้วางใจในกระบวนการจัดการข้อมูลในยุคดิจิทัล งานวิจัยนี้เป็นรากฐานสำคัญที่สามารถพัฒนาเป็นแนวทางปฏิบัติที่ดีในการจัดการข้อมูลส่วนบุคคลในอนาคต และช่วยส่งเสริมมาตรฐานการปกป้องข้อมูลในยุคดิจิทัล

(ดุษฎีนิพนธ์มีจำนวนทั้งสิ้น 235 หน้า)

คำสำคัญ: บล็อกเชน, การจัดการความยินยอม, การแฝงข้อมูล, k-Anonymity, ข้อมูลส่วนบุคคล

ลายมือชื่อนักศึกษา ..... ลายมือชื่ออาจารย์ที่ปรึกษา .....
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

6504122	:	Jiraphat Lapwattanaworakul
Dissertation Title	:	Blockchain-based Auxiliary System for Pseudonymization and Consent Management
Program	:	Doctor of Philosophy in Information Technology
Dissertation Advisor	:	Assoc. Prof. Chetneti Srisa-An, Ph.D.
Dissertation Co-Advisor	:	Asst. Prof. Thannob Aribarg, Ph.D.

Abstract

In the digital era, where personal data has become a crucial resource for business operations and social analysis, protecting personal data has become increasingly important. This is particularly true with the enforcement of data protection regulations, such as the GDPR and PDPA. Businesses and organizations must develop strategies and methods to manage data in compliance with these regulations. However, traditional data protection methods, such as data anonymization or deletion, have limitations and are still vulnerable to re-identification attacks. This research introduces an innovative approach to consent management and data pseudonymization using blockchain technology as a supportive system. The objective of this study is to develop a system that integrates smart contracts on a blockchain to manage user consent efficiently and securely. Additionally, the study seeks to enhance data pseudonymization techniques that preserve data accuracy while reducing the risks of privacy breaches. The methodology begins with designing a conceptual framework based on legal requirements, followed by utilizing standard datasets and additional data for experimental purposes to evaluate the system's impact and performance. The findings indicate that the developed system significantly reduces the risk of personal data breaches, with blockchain playing a pivotal role in ensuring data security and transparency. Furthermore, the proposed system is adaptable to various legal requirements, fostering trust in data management processes in the digital age. This research serves as a foundation framework that can evolve into best practices for managing personal data in the future, contributing to the advancement of data protection standards in the digital era.

(Total 235 pages)

Keywords: Blockchain, consent management, pseudonymization, k-Anonymity, personal data

Student's Signature …..... Dissertation Advisor's Signature .....

Dissertation Co-Advisor's Signature .....

สารบัญ

		หน้า
กิตติกรรมประกาศ		**ก**
บทคัดย่อภาษาไทย		**ข**
บทคัดย่อภาษาอังกฤษ		**ค**
สารบัญ		**ง**
สารบัญตาราง		**ฉ**
สารบัญรูป		**ช**
บทที่ 1	**บทนำ**	**1**
	1.1 ความเป็นมาและความสำคัญของปัญหา	1
	1.2 วัตถุประสงค์การวิจัย	14
	1.3 สมมติฐานการวิจัย	14
	1.4 ขอบเขตการวิจัย	14
	1.5 กรอบแนวคิดการวิจัย	15
	1.6 ประโยชน์ที่ได้รับจากการวิจัย	17
	1.7 นิยามศัพท์	18
บทที่ 2	**ทบทวนวรรณกรรมที่เกี่ยวข้อง / ทฤษฎีที่เกี่ยวข้อง**	**23**
	2.1 เทคโนโลยีบล็อกเชน	23
	2.2 สัญญาอัจฉริยะ	47
	2.3 ภาษาซอลิดิตี	52
	2.4 ภาษาไพทอนและไลบรารี่ Scikit-learn	53
	2.5 การจัดการความยินยอม	58
	2.6 เทคนิคการปกป้องข้อมูลส่วนบุคคล	69
	2.7 วิธีการสำรวจวรรณกรรม	85
บทที่ 3	**ระเบียบวิธีการวิจัย**	**107**

มหาวิทยาลัยรังสิต Rangsit University

สารบัญ (ต่อ)

		หน้า
	3.1 ขั้นตอนการวิจัย	107
	3.2 แนวคิดหรือสิ่งที่นำเสนอ	110
	3.3 การตั้งค่าการทดลอง	140
	3.4 เครื่องมือที่ใช้ในการวิจัย	187
	3.5 การเก็บรวบรวมข้อมูล	192
	3.6 การวิเคราะห์ข้อมูล	193
บทที่ 4	**ผลการวิจัย**	**195**
	4.1 ผลการทดลองการวิเคราะห์เชิงเปรียบเทียบของแพลตฟอร์มบล็อกเชนสำหรับระบบจัดการความยินยอมโดยชุดคำสั่งสัญญาอัจฉริยะ	195
	4.2 ผลการทดลองการวิเคราะห์เชิงเปรียบเทียบประสิทธิภาพการใช้เทคนิคการแฝงข้อมูลโดยใช้ฟังก์ชันแฮชบนบล็อกเชน	203
บทที่ 5	**สรุปผลและข้อเสนอแนะ**	**212**
	5.1 สรุปผลการวิจัย	212
	5.2 การอภิปรายและข้อจำกัดในการวิจัย	215
	5.3 ข้อเสนอแนะและงานวิจัยในอนาคต	221
บรรณานุกรม		**225**
ประวัติผู้วิจัย		**235**

มหาวิทยาลัยรังสิต Rangsit University

สารบัญตาราง

ตารางที่		หน้า
2.1	ข้อดีข้อเสียของบล็อกเชนแบบเปิดสาธารณะ	27
2.2	ข้อดีข้อเสียของบล็อกเชนแบบปิด	28
2.3	ข้อดีข้อเสียของบล็อกเชนแบบเฉพาะกลุ่ม	29
2.4	ข้อดีข้อเสียของบล็อกเชนแบบไฮบริด	30
2.5	เปรียบเทียบลักษณะเฉพาะของเทคนิคการทำให้เป็นนิรนามและการแฝงข้อมูล	81
2.6	ภาพรวมแสดงความเสี่ยงของการป้องกันข้อมูลแต่ละเทคนิค	81
2.7	สรุปช่องว่างของการวิจัย	103
3.1	ความแตกต่างระหว่าง ระบบการจัดการความยินยอมที่บูรณาการกับสัญญาอัจฉริยะบนบล็อกเชน และ ระบบการจัดการความยินยอมแบบดั้งเดิม	133
3.2	ความแตกต่างระหว่าง การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน และ การใช้การแฝงข้อมูลแบบดั้งเดิม	138
3.3	การเปรียบเทียบประสิทธิภาพของแพลตฟอร์มบล็อกเชน	144
3.4	สรุปจุดแข็งและจุดอ่อนของแต่ละแพลตฟอร์ม	148
3.5	ผลกระทบจากกระบวนการล้างข้อมูล	153
3.6	การเปรียบเทียบความแม่นยำของแบบจำลองก่อนและหลังใช้ k-Anonymity	177
3.7	การเปรียบเทียบความถูกต้องของแบบจำลองก่อนและหลังใช้ k-Anonymity	178
3.8	การเปรียบเทียบการเรียกคืนของแบบจำลองก่อนและหลังใช้ k-Anonymity	180
3.9	การเปรียบเทียบคะแนนเอฟวันของแบบจำลองก่อนและหลังใช้ k-Anonymity	182
3.10	เปรียบเทียบ ROC-AUC Curve ก่อนและหลังใช้ k-Anonymity	185
3.11	ผลการประเมินความเสี่ยงของการระบุตัวตนซ้ำอีกครั้ง	186

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป

รูปที่		หน้า
1.1	จำนวนประชากรและจำนวนประชากรที่ใช้อินเทอร์เน็ตทั่วโลกในปี 2566	11
1.2	จำนวนประชากรและจำนวนประชากรที่ใช้อินเทอร์เน็ตของประเทศไทยในปี 2566	11
1.3	การปฏิเสธคุกกี้อย่างน้อย 1 ครั้งของแต่ละประเทศ	12
1.4	ความกังวลเกี่ยวกับข้อมูลส่วนบุคคลของแต่ละประเทศ	13
1.5	การใช้เครือข่ายส่วนตัวเสมือน (VPN) ของแต่ละประเทศ	13
1.6	ภาพรวมการใช้เครือข่ายส่วนตัวเสมือน (VPN) ของแต่ละประเทศ	14
1.7	กรอบแนวคิดการทำวิจัย	16
2.1	วิวัฒนาการของเทคโนโลยีบล็อกเชน	26
2.2	ประเภทของบล็อกเชน	26
2.3	โครงสร้างพื้นฐานของบล็อกเชน	31
2.4	วิวัฒนาการของสัญญาอัจฉริยะ	48
2.5	สิทธิของเจ้าของข้อมูลส่วนบุคคล	62
2.6	สถาปัตยกรรมของระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต	68
2.7	เทคนิคการปกป้องข้อมูลส่วนบุคคล	69
2.8	เทคนิคการทำให้เป็นนิรนาม	71
2.9	เทคนิคการเพิ่มการรบกวน	72
2.10	เทคนิคการเรียงสับเปลี่ยน	72
2.11	เทคนิคการรวมกลุ่มและการทำ k-Anonymity	73
2.12	เทคนิคการ l-Diversity	74
2.13	เทคนิคการ t-Closeness	74
2.14	เทคนิคการแฝงข้อมูล	76
2.15	ตัวอย่างการใช้ฟังก์ชันแฮช	77
2.16	ตัวอย่างการใช้ฟังก์ชันคีย์แฮชพร้อมคีย์เพิ่มเติม	77
2.17	กระบวนการทำงานของการแฝงข้อมูลและการทำให้เป็นนิรนาม	80
2.18	โพรโทคอลการสำรวจ	87

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.1	ขั้นตอนการดำเนินการวิจัย	109
3.2	แนวคิดการวิจัยที่นำเสนอ	111
3.3	IPOO Model ภาพรวมงานวิจัย	116
3.4	IPOO Model ระบบบริหารจัดการความยินยอม	119
3.5	IPOO Model ระบบการแฝงข้อมูล	123
3.6	สถาปัตยกรรมของระบบที่นำเสนอ	124
3.7	กรอบการทำงานระบบบริหารจัดการความยินยอมเข้ากับสัญญาอัจฉริยะ	126
3.8	กระบวนการการบูรณาการระบบบริหารจัดการความยินยอมร่วมกับสัญญาอัจฉริยะ	132
3.9	กระบวนการใช้เทคนิคการแฝงข้อมูลโดยทดลองร่วมกับ RSU-Data-Anonymization โดยใช้เทคนิค k-Anonymity	136
3.10	แผนผังกระบวนการทำงานของสัญญาอัจฉริยะบนบล็อกเชน	140
3.11	กระบวนการทำงานของสัญญาอัจฉริยะบนบล็อกเชน	141
3.12	ตัวอย่างชุดคำสั่งของสัญญาอัจฉริยะ	141
3.13	เปรียบเทียบค่าธรรมเนียมการทำธุรกรรมและเวลาการทำธุรกรรม	145
3.14	เปรียบเทียบระดับความต้านทานต่อการโจมตี	147
3.15	ขั้นตอนการทำงานของการทดลองที่ 2	149
3.16	ขั้นตอนการจัดการค่าที่หายไป	151
3.17	แสดงวิธีการระบุค่าผิดปกติโดยใช้วิธีช่วงระหว่างควอไทล์ (IQR)	152
3.18	แสดงการลบค่าผิดปกติออกจากชุดข้อมูล	153
3.19	แสดงการสร้างข้อมูลแฝง	155
3.20	แสดงการสร้างที่อยู่แฮช	156
3.21	แสดงกระบวนการแบ่งส่วนข้อมูล	158
3.22	กระบวนการทำให้ตัวระบุเสมือนเป็นลักษณะทั่วไปโดยใช้ k-Anonymity กับ ‘อายุ’	159
3.23	การทำให้ตัวระบุเสมือนเป็นลักษณะทั่วไปโดยใช้ k-Anonymity กับ ‘อายุ’	160

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.24	การกระจายของ ‘อายุ’ ก่อนและหลังทำให้เป็นลักษณะทั่วไป	160
3.25	การกระจายคลาสย่อยของแอตทริบิวต์ ‘คลาส’	163
3.26	การกระจายคลาสย่อยของแอตทริบิวต์ ‘การศึกษา’	164
3.27	แสดงชุดคำสั่งการจัดกลุ่มแอตทริบิวต์ตัวระบุเสมือนใหม่	165
3.28	การทำเป็นลักษณะทั่วไปโดยการแบ่งพาร์ติชันแอตทริบิวต์เสมือน	166
3.29	การเตรียมข้อมูลตั้งต้น	168
3.30	การเตรียมข้อมูลที่ผ่านการทำให้เป็นลักษณะทั่วไป	168
3.31	การฝึกและทดสอบแบบจำลองการเรียนรู้ของเครื่องก่อนใช้ k-Anonymity	169
3.32	ทดสอบและประเมินแบบจำลองการเรียนรู้ของเครื่องก่อนใช้ k-Anonymity	170
3.33	การวิเคราะห์เชิงเปรียบเทียบแบบจำลองการเรียนรู้ของเครื่องก่อนใช้ k-Anonymity	172
3.34	การฝึกและทดสอบแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity	173
3.35	ทดสอบและประเมินแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity	174
3.36	การวิเคราะห์เชิงเปรียบเทียบแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity	176
3.37	การเปรียบเทียบความแม่นยำของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้ k-Anonymity	178
3.38	การเปรียบเทียบความถูกต้องของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้ k-Anonymity	179
3.39	การเปรียบเทียบการเรียกคืนของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้ k-Anonymity	181
3.40	การเปรียบเทียบคะแนนเอฟวันของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้ k-Anonymity	183
3.41	การวิเคราะห์ ROC-AUC Curve ก่อนใช้ k-Anonymity	184
3.42	การวิเคราะห์ ROC-AUC Curve หลังใช้ k-Anonymity	185
3.43	สถาปัตยกรรมของระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต	190

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.44	แสดงตัวอย่างของเทคนิคการแฝงข้อมูล	191
4.1	แดชบอร์ดสรุปผลการทดลองที่ 1	202
4.2	แดชบอร์ดสรุปผลการทดลองที่ 2	211

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคดิจิทัลร่วมสมัยปัจจุบัน ธุรกิจต่าง ๆ มักมีส่วนร่วมในการสร้าง การจัดเก็บ และการประมวลผลข้อมูลส่วนบุคคลจำนวนมหาศาล ข้อมูลนี้ครอบคลุมข้อมูลส่วนบุคคลที่หลากหลาย ตั้งแต่รายละเอียดการเดินทางที่จัดเก็บไว้ในอุปกรณ์เคลื่อนที่ (สมาร์ทโฟน) แต่ละเครื่อง ไปจนถึงข้อมูลประชากรและพฤติกรรมที่ฝังอยู่ในแพลตฟอร์มสื่อสังคมออนไลน์ (โซเชียลมีเดีย) ต่าง ๆ การโต้ตอบและธุรกรรมในแต่ละวันส่งผลให้เกิดการเผยแพร่ข้อมูลส่วนบุคคล รวมถึงคุณลักษณะต่าง ๆ เช่น เพศ อายุ ความสนใจ และระดับรายได้ ผ่านเครือข่ายมือถือที่เชื่อมต่ออินเทอร์เน็ต การไหลของข้อมูลอย่างต่อเนื่องนี้ไม่ได้เป็นเพียงเรื่องบังเอิญเท่านั้น มันเป็นลักษณะพื้นฐานของการค้าและการโต้ตอบดิจิทัลสมัยใหม่ โดยเฉพาะยิ่ง บริษัทโทรคมนาคม พบว่าตัวเองเป็นศูนย์กลางของการแลกเปลี่ยนข้อมูลนี้ พวกเขามีความสามารถทางเทคโนโลยีในการติดตามและบันทึกการเคลื่อนไหวและพฤติกรรมของลูกค้าโดยละเอียด ข้อมูลเช่น ใครเดินทางไปที่ไหนและในเวลาใดที่หน่วยงานเหล่านี้บันทึกเป็นประจำ ข้อมูลอันมากมายนี้สร้างภาระความรับผิดชอบอันใหญ่หลวงให้กับบริษัทเหล่านี้ พวกเขาไม่ได้เป็นเพียงผู้ให้บริการแต่ยังเป็นผู้พิทักษ์ความเป็นส่วนตัวของข้อมูลของลูกค้าด้วย วิธีที่บริษัทเหล่านี้จัดการกับข้อมูลที่ละเอียดอ่อนนี้ส่งผลโดยตรงต่อชื่อเสียงและความน่าเชื่อถือในสายตาของลูกค้าและสาธารณชนโดยรวม

ความสำคัญของความเป็นส่วนตัวของข้อมูลยังได้รับการตอกย้ำโดยการเกิดขึ้นและการบังคับใช้กฎหมายและกฎระเบียบด้านความเป็นส่วนตัวที่เข้มงวด เช่น จีดีพีอาร์ในสหภาพยุโรปและพีดีพีเอในประเทศไทย กรอบทางกฎหมายเหล่านี้ไม่ได้เป็นเพียงแนวทางเท่านั้น แต่ยังเป็นข้อบังคับที่บังคับใช้ได้ซึ่งทำให้บริษัทต่าง ๆ ต้องรับผิดชอบในการปกป้องข้อมูลส่วนบุคคล การไม่ปฏิบัติตามอาจส่งผลให้เกิดผลกระทบและทางกฎหมายและทางการเงินอย่างมีนัยสำคัญ โดยเน้นถึงลักษณะที่สำคัญของความเป็นส่วนตัวของข้อมูลในการกำกับดูแลกิจการในปัจจุบัน

มหาวิทยาลัยรังสิต Rangsit University

เพื่อตอบสนองต่อความท้าทายที่หลากหลายเหล่านี้ อุตสาหกรรมที่ขับเคลื่อนด้วยข้อมูลหันมาใช้โซลูชันทางเทคโนโลยีที่เป็นนวัตกรรมมากขึ้น เทคโนโลยีเสริมความเป็นส่วนตัว (Privacy Enhancing Technologies – PETs) แสดงถึงความก้าวหน้าครั้งสำคัญในสาขานี้ เทคโนโลยีเหล่านี้ไม่ได้เป็นเพียงเครื่องมือ แต่ยังเป็นปัจจัยสนับสนุนเชิงกลยุทธ์ ซึ่งได้รับการออกแบบมาเพื่อเป้าหมายที่ชัดเจนในการปกป้องความเป็นส่วนตัวและการรักษาความลับของข้อมูลส่วนบุคคล เทคโนโลยีเสริมความเป็นส่วนตัวทำงานในหลายระดับ เช่น ให้อำนาจแก่บุคคลให้การควบคุมและความมั่นใจในข้อมูลส่วนบุคคลของตนมากขึ้น ช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเฝ้าระวังและการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตและสนับสนุนโครงสร้างพื้นฐานด้านความปลอดภัยโดยรวมปกป้องข้อมูลที่ละเอียดอ่อนจากการละเมิดที่อาจเกิดขึ้นและการแสวงหาประโยชน์โดยไม่ได้รับอนุญาต (Information Commissioner's Office, 2022, pp.1-39)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ พีดีพีเอ (Personal Data Protection Act B.E. 2019 – PDPA) เป็นกฎหมายฉบับแรกของประเทศไทย มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 โดยมีวัตถุประสงค์เพื่อดูแลและคุ้มครองข้อมูลส่วนบุคคลในประเทศ ซึ่ง พีดีพีเอ มีเป้าหมายหลักคือ บังคับให้บริษัท องค์กร หรือหน่วยงานที่ถือครองข้อมูลส่วนบุคคล (ซึ่งในกฎหมายมีฐานะเป็นผู้ควบคุมข้อมูล – Data Controller) จะต้องปกป้องข้อมูลไม่ให้ถูกละเมิด เก็บข้อมูลให้ปลอดภัย ประมวลผลใช้งานเท่าที่จำเป็น และไม่แชร์ให้บุคคลที่สามตามอำเภอใจ ที่สำคัญต้องได้รับความยินยอมจากเจ้าของข้อมูล ก่อนการเก็บรวบรวม การใช้ การแบ่งปัน หรือการเปิดเผยข้อมูลส่วนบุคคล ระบบการจัดการความยินยอมเป็นระบบสำหรับผู้ควบคุมข้อมูลเพื่อควบคุมการใช้ข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อน (Zemler, 2019, pp.1-12) ไม่ถูกควบคุมโดยผู้อื่นหากไม่ได้รับอนุญาต เนื่องจากอาจถูกโจมตีและนำไปใช้ในทางที่ผิดได้ การละเมิดข้อมูลเป็นปัญหาร้ายแรงสำหรับทุกบริษัทที่ถือครองข้อมูลส่วนบุคคล แต่การจัดการเรื่องพีดีพีเอ ยังมีข้อจำกัดในการจัดการทางเทคโนโลยีหลายประการเช่น ในด้านความปลอดภัย ประสิทธิภาพ และความเสถียรภาพของข้อมูล เนื่องด้วยความเจริญก้าวหน้าทางด้านเทคโนโลยีสารสนเทศที่พัฒนาไปอย่างรวดเร็ว ส่งผลให้การเข้าถึงและการใช้งานสื่อสังคมออนไลน์ได้อย่างแพร่หลายในปัจจุบัน เทคโนโลยีบล็อกเชนเป็นเทคโนโลยีที่เกิดขึ้นใหม่และได้รับการกล่าวถึงอย่างมากและได้รับความสนใจจากหลากหลายด้าน เทคโนโลยีบล็อกเชนกำลังปฏิวัติโลกดิจิทัล ปฏิวัติภาคธุรกิจและเปลี่ยนแปลงด้านเศรษฐกิจและสังคมโดยนำมุมมองใหม่มาสู่ความปลอดภัย ประสิทธิภาพ และความเสถียรของระบบและข้อมูล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ จีดีพีอาร์ (General Data Protection Regulation - GDPR) ได้ประกาศใช้กับประเทศในเครือสหภาพยุโรปในปี 2561 จีดีพีอาร์เมื่อมีการบังคับใช้แล้ว ถือเป็นการประกาศยุคแห่งการเปลี่ยนแปลงในด้านความเป็นส่วนตัวและการปกป้องข้อมูล โดยเฉพาะอย่างยิ่งภายในสหภาพยุโรป กรอบการกำกับดูแลที่แข็งแกร่งนี้ได้รับการออกแบบมาเพื่อตอบสนองความท้าทายที่ซับซ้อนของความเป็นส่วนตัวของบุคคลในยุคดิจิทัล เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของแต่ละบุคคลได้รับการจัดการด้วยมาตรฐานสูงสุดด้านความปลอดภัยและการรักษาความลับ ผลกระทบดังกล่าวมีวงกว้างโดยไม่เพียงส่งผลกระทบต่อหน่วยงานในยุโรปเท่านั้น แต่ยังรวมถึงองค์กรและแพลตฟอร์มระดับโลกที่เกี่ยวข้องกับข้อมูลพลเมืองสหภาพยุโรปด้วย เช่น UCI Machine Learning Repository และ Kaggle แพลตฟอร์มเหล่านี้ซึ่งเป็นที่รู้จักในเรื่องชุดข้อมูลขนาดใหญ่ที่ใช้สำหรับการวิจัยและการวิเคราะห์ในด้านต่าง ๆ จะต้องปรับให้เข้ากับกฎระเบียบใหม่เหล่านี้ โดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับชุดข้อมูลที่มีข้อมูลส่วนบุคคล

ในอดีต ชุดข้อมูลเหล่านี้ใช้มาตรการรักษาความเป็นส่วนตัวบางอย่าง เช่น การยกเว้นตัวระบุโดยตรง เช่น ชื่อและนามสกุล แนวทางปฏิบัตินี้หรือที่เรียกกันทั่วไปว่าการลบการระบุตัวตน มีวัตถุประสงค์เพื่อรักษาความเป็นส่วนตัวของบุคคลในขณะเดียวกันก็ช่วยให้สำรวจและวิเคราะห์ข้อมูลเชิงลึกอันมีค่าที่มีอยู่ในข้อมูลได้ อย่างไรก็ตามการเกิดขึ้นของการโจมตีเพื่อระบุตัวตนซ้ำอีกครั้งซึ่งข้อมูลที่ไม่เปิดเผยตัวตนถูกดัดแปลงเพื่อระบุตัวบุคคลอีกครั้ง ทำให้เกิดช่องโหว่ในแนวทางนี้ เหตุการณ์ดังกล่าวได้รับการบันทึกไว้ตั้งแต่ปี 2552 โดยเน้นย้ำถึงลักษณะการพัฒนาของภัยคุกคามต่อความเป็นส่วนตัวของข้อมูลและความจำเป็นสำหรับมาตรการป้องกันที่ซับซ้อนมากขึ้น แสดงให้เห็นถึงวิธีที่ซับซ้อนที่สามารถนำไปใช้ในการทำวิศวกรรมย้อนกลับรอยข้อมูลที่ไม่เปิดเผยตัวตน และด้วยเหตุนี้จึงเปิดเผยตัวตนส่วนบุคคล เหตุการณ์ดังกล่าวเพิ่มความกังวลเกี่ยวกับความเพียงพอของมาตรการความเป็นส่วนตัวแบบดั้งเดิมและเน้นย้ำถึงความเสี่ยงที่เกี่ยวข้องกับการเผยแพร่ข้อมูลที่ละเอียดอ่อนบนอินเทอร์เน็ต (Hensriksen-Bulmer & Jeary, 2016, pp. 1184-1192)

เพื่อตอบสนองต่อช่องโหว่เหล่านี้และมาตรฐานความเป็นส่วนตัวที่เข้มงวดซึ่งกำหนดโดยจีดีพีอาร์ในสหภาพยุโรป ผู้เผยแพร่ข้อมูลได้เพิ่มความระมัดระวังอย่างมาก ได้เปลี่ยนไปสู่การเสริมความแข็งแกร่งให้กับชุดข้อมูลต่อความเสี่ยงของการโจมตีเพื่อระบุตัวตนซ้ำอีกครั้ง ซึ่งเป็นความพยายามที่นอกเหนือไปจากเทคนิคการลบการระบุตัวตนขั้นพื้นฐาน ในสภาพแวดล้อมการรักษาความปลอดภัยที่เพิ่มขึ้นนี้ กระบวนการทำให้ข้อมูลไม่เปิดเผยตัวตนได้รับความสำคัญอย่างยิ่ง ด้วยความตระหนักถึงบทบาทของการไม่เปิดเผยข้อมูลในการปกป้องความเป็นส่วนตัว หน่วยงานของรัฐจึง

เริ่มออกคำสั่งให้บริษัทมือถือและหน่วยงานจัดการข้อมูลอื่น ๆ ใช้กระบวนการลบข้อมูลระบุตัวตนอย่างเข้มงวด ก่อนที่จะส่งข้อมูลส่วนบุคคลผ่านเครือข่ายของพวกเขา ข้อกำหนดบ่งบอกถึงแนวทางเชิงรุกต่อความเป็นส่วนตัวของข้อมูล โดยยอมรับถึงความจำเป็นในการปกป้องข้อมูลส่วนบุคคลในเชิงรุกในยุคที่การละเมิดข้อมูลและข้อกังวลด้านความเป็นส่วนตัวแพร่หลายมากขึ้น สำหรับบริษัทมือถือและสำหรับองค์กรทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคล การใช้เทคนิคการลบข้อมูลระบุตัวตนอย่างมีประสิทธิภาพได้กลายเป็นส่วนสำคัญของระเบียบปฏิบัติในการดำเนินงานของบริษัท ไม่ใช่แค่การปฏิบัติตามมาตรฐานทางกฎหมายเท่านั้น แต่เป็นการสร้างและรักษาความไว้วางใจกับผู้ใช้ ลูกค้า และสาธารณชนโดยรวม ในขณะที่ภาพรวมทางดิจิทัลยังคงพัฒนาต่อไป ความสำคัญของแนวทางปฏิบัติในการจัดการข้อมูลที่แข็งแกร่ง สร้างสรรค์ และมีความรับผิดชอบตามหลักจริยธรรม รวมถึงการไม่เปิดเผยชื่ออย่างมีประสิทธิภาพ จะยังคงเป็นรากฐานสำคัญของการดูแลข้อมูลที่มีความรับผิดชอบในยุคข้อมูลข่าวสาร

ในปี 2566 ภาพรวมของการบังคับใช้จีดีพีอาร์ของสหภาพยุโรป มีพัฒนาการที่สำคัญ โดยมีการปรับจำนวนมากที่ไม่เคยมีมาก่อนซึ่งเน้นย้ำถึงแนวทางที่เข้มงวดและความร้ายแรงในการปกป้องข้อมูลในสหภาพยุโรป ประเด็นสำคัญจากรายการค่าปรับจีดีพีอาร์ที่ใหญ่ที่สุด 20 อันดับ (Data Privacy Manager, 2024, p.1) ได้แก่

1) ค่าปรับของเมต้า (Meta's Record Fine): เมต้าซึ่งก่อนหน้านี้รู้จักกันในชื่อของเฟซบุ๊ก (Facebook) ได้ถูกปรับจำนวน 1.2 พันล้านยูโรจากคณะกรรมการคุ้มครองข้อมูลของไอร์แลนด์ เนื่องจากการถ่ายโอนข้อมูลของผู้ใช้ในสหภาพยุโรปไปยังสหรัฐอเมริกาอย่างไม่เหมาะสมและผิดกฎหมายโดยไม่มีการป้องกันที่เพียงพอ ค่าปรับนี้เป็นค่าปรับจีดีพีอาร์ที่ใหญ่ที่สุดในปัจจุบันและถือเป็นส่วนสำคัญของค่าปรับจีดีพีอาร์ทั้งหมดตั้งแต่ออกบังคับใช้

2) บทลงโทษที่สำคัญของแอมะซอน: แอมะซอน (Amazon) ถูกปรับ 746 ล้านยูโร โดยหน่วยงานคุ้มครองข้อมูลของลักเซมเบิร์ก สำหรับปัญหาที่เกี่ยวข้องกับการได้รับความยินยอมที่ไม่เหมาะสมในระบบกำหนดเป้าหมายการโฆษณา ซึ่งแสดงให้เห็นถึงความสำคัญของความยินยอมของผู้ใช้ในกิจกรรมประมวลผลข้อมูล

3) ค่าปรับเพิ่มเติมเกี่ยวกับเมต้า: เมต้าต้องเผชิญกับค่าปรับอื่น ๆ หลายประการ มูลค่ารวมถึง 405 ยูโรสำหรับการประมวลผลข้อมูลส่วนบุคคลของเด็กอย่างไม่เหมาะสมบนอินสตาแกรม (Instagram) และค่าปรับ 390 ล้านยูโรที่เกี่ยวข้องกับการเปลี่ยนแปลงในข้อกำหนดในการให้บริการของเฟซบุ๊กและอินสตาแกรม

4) การละเมิดจีดีพีอาร์ของติ๊กต็อก: ติ๊กต็อก (TikTok) ถูกปรับ 345 ล้านยูโรสำหรับการละเมิดจีดีพีอาร์ที่เกี่ยวข้องกับการจัดการบัญชีเด็กรวมถึงปัญหาเกี่ยวกับการตั้งค่าแพลตฟอร์มและแนวทางปฏิบัติในการประมวลผลข้อมูล โดยเน้นให้เห็นถึงความกังวลที่เพิ่มขึ้นเกี่ยวกับการปกป้องข้อมูลของผู้เยาว์

5) การรั่วไหลของข้อมูลและมาตราการรักษาความปลอดภัยที่ไม่เพียงพอ: เมต้ายังถูกปรับ 265 ล้านยูโรเนื่องจากการละเมิดข้อมูลที่ส่งผลกระทบต่อผู้ใช้หลายล้านคน กรณีนี้เน้นย้ำถึงความจำเป็นที่สำคัญสำหรับมาตรการรักษาความปลอดภัยข้อมูลที่แข็งแกร่งเพื่อปกป้องข้อมูลส่วนบุคคล

6) ปัญหาความโปร่งใสของวอตส์แอปป์: วอตส์แอปป์ (WhatsApp) ซึ่งเป็นเจ้าของโดยเมต้าถูกปรับ 225 ล้านยูโร เนื่องจากขาดความโปร่งใสในการประมวลผลข้อมูล โดยเน้นย้ำถึงความสำคัญของการสื่อสารที่ชัดเจนกับผู้ใช้เกี่ยวกับการใช้ข้อมูล

7) กฎระเบียบด้านความยินยอมและการใช้คุกกี้: กูเกิล แอลแอลซี (Google LLC) และกูเกิลไอร์แลนด์ (Google Ireland) ต้องเผชิญกับค่าปรับ (90 ล้านยูโร และ 60 ล้านยูโร ตามลำดับ) จากหน่วยงานคุ้มครองข้อมูลส่วนบุคคลฝรั่งเศส ฐานไม่ปฏิบัติตามกฎระเบียบในการยินยอมให้ใช้คุกกี้ และในทำนองเดียวกันเฟซบุ๊กไอร์แลนด์ (Facebook Ireland) ถูกปรับ 60 ล้านยูโร เนื่องจากไม่สามารถให้กลไกการปฏิเสธคุกกี้ที่ตรงไปตรงมา ซึ่งชี้ให้เห็นถึงการตรวจสอบกลไกการติดตามและการยินยอมทางออนไลน์ที่เพิ่มมากขึ้น

8) การละเมิดที่หลากหลาย: รายการประกอบด้วยการละเมิดจีดีพีอาร์ที่หลากหลาย ตั้งแต่การละเมิดข้อมูลและมาตรการรักษาความปลอดภัยที่ไม่เพียงพอ (ดังที่เห็นในกรณีของบริษัท British Airways และ Marriott International) ไปจนถึงการใช้ข้อมูลส่วนบุคคลในทางที่ผิดเพื่อวัตถุประสงค์ทางการตลาด (เช่น ค่าปรับสำหรับ TIM และ Wind Tre S.p.A.)

9) ค่าปรับหลายรายการของเคลียร์วิว เอไอ: เคลียร์วิว เอไอ (Clearview AI) ต้องเผชิญกับค่าปรับ 20 ล้านยูโรในฝรั่งเศส กรีซ และอิตาลี จากการละเมิดที่เกี่ยวข้องกับเทคโนโลยีการจดจำใบหน้าและแนวทางปฏิบัติในการประมวลผลข้อมูล

10) ค่าปรับที่สำคัญอื่น ๆ: รายการนี้ยังรวมถึงค่าปรับจำนวนมากต่อบริษัทต่าง ๆ เช่น CRITEO และ H&M) สำหรับการละเมิดจีดีพีอาร์ต่าง ๆ ตั้งแต่มาตรการปกป้องข้อมูลไม่เพียงพอไปจนถึงแนวทางปฏิบัติในการยินยอมที่ไม่เหมาะสม

โดยรวมแล้ว ค่าปรับเหล่านี้เน้นให้เห็นถึงแนวโน้มที่เพิ่มขึ้นของการบังคับใช้จีดีพีอาร์ที่เข้มงวด โดยหน่วยงานต่าง ๆ มุ่งเน้นไปที่ประเด็นต่าง ๆ เช่น การถ่ายโอนข้อมูลระหว่างประเทศ กลไกการยินยอม ความปลอดภัยของข้อมูลของเด็ก โดยเน้นไปที่บริษัทข้ามชาติและยักษ์ใหญ่ด้าน

เทคโนโลยีเป็นพิเศษ ลักษณะที่สำคัญของค่าปรับเหล่านี้ทำหน้าที่เป็นเครื่องเตือนใจที่เข้มงวดแก่องค์กรต่าง ๆ เกี่ยวกับความสำคัญของการปฏิบัติตามจีดีพีอาร์สำหรับธุรกิจที่ดำเนินงานในสหภาพยุโรป และผลกระทบทางการเงินที่อาจเกิดขึ้นจากการไม่ปฏิบัติตาม

การโจมตีเพื่อระบุตัวตนซ้ำอีกครั้งกลายเป็นภัยคุกคามที่สำคัญในขอบเขตของความเป็นส่วนตัวของข้อมูล โดยที่ชุดข้อมูลที่ไม่เปิดเผยตัวตนถูกดัดแปลงเพื่อเปิดเผยตัวตนของแต่ละบุคคล สิ่งนี้นำไปสู่การละเมิดข้อมูลจำนวนมากและมีการฟ้องร้องที่โด่งดังหลายคดี ซึ่งมักส่งผลให้เกิดผลกระทบทางกฎหมายและสร้างความเสียหายอย่างมากต่อชื่อเสียงขององค์กร โดยเน้นย้ำถึงความท้าทายและความซับซ้อนที่เกี่ยวข้องกับการรับรองความเป็นส่วนตัวของข้อมูล ดังตัวอย่างที่จะหยิบยกเป็นกรณีศึกษาที่เกิดเหตุการณ์จริงที่เกี่ยวข้องกับการใช้แหล่งข้อมูลเสริมในการโจมตีข้อมูลที่ละเอียดอ่อนแบบกำหนดเป้าหมาย ซึ่งเป็นตัวอย่างของบริบทที่หลากหลายซึ่งการละเมิดเหล่านี้สามารถเกิดขึ้นได้ และผลที่มาตามในวงกว้าง

ตัวอย่างที่ 1: AOL (ข้อมูลการค้นหาทางอินเทอร์เน็ตที่ไม่ระบุชื่อ)

ในปี 2549 AOL ได้เผยแพร่ชุดข้อมูลขนาดใหญ่ของคำค้นหาที่ไม่ระบุชื่อเพื่อวัตถุประสงค์ในการวิจัยทางวิชาการ อย่างไรก็ตาม ข้อมูล “ที่ไม่ระบุชื่อ” ยังคงมีหมายเลขประจำตัวของผู้ใช้ที่ไม่ซ้ำกัน และผู้สื่อข่าวจากเดอะนิวยอร์กไทม์สสามารถระบุตัวบุคคลได้อีกครั้งตามคำค้นหาของพวกเขา การละเมิดนี้นำไปสู่การโวยวายของสาธารณชนเกี่ยวกับการละเมิดความเป็นส่วนตัวและส่งผลให้เกิดการฟ้องร้องดำเนินคดีในชั้นศาลกับ AOL กรณีนี้เน้นย้ำถึงช่องโหว่ของข้อมูลที่ “ไม่เปิดเผยตัวตน” และความสะดวกในการระบุตัวบุคคลผ่านข้อมูลที่ดูเหมือนไม่ละเอียดอ่อน

ตัวอย่างที่ 2: รัฐอิลลินอยส์ตอนใต้และหน่วยงานสาธารณสุข

หนังสือพิมพ์ของรัฐอิลลินอยส์ตอนใต้ร่วมกับหน่วยงานสาธารณสุขได้ตีพิมพ์ชุดข้อมูลที่ไม่ระบุชื่อเกี่ยวกับผู้ป่วยโรคติดเชื้อ อย่างไรก็ตาม ข้อมูลที่เหลือก็เพียงพอสำหรับการระบุตัวบุคคล ซึ่งนำไปสู่การละเมิดความเป็นส่วนตัวและปัญหาทางกฎหมายและจริยธรรมที่ตามมา เป็นการย้ำเตือนถึงความซับซ้อนที่เกี่ยวข้องกับการลบข้อมูลด้านสุขภาพ ข้อมูลดังกล่าวแสดงให้เห็นถึงความสำคัญอย่างยิ่งยวดของเทคนิคการทำให้ข้ออมูลเป็นนิรนามที่เข้มงวด โดยเฉพาะอย่างยิ่งเมื่อต้องจัดการกับข้อมูลสุขภาพที่ละเอียดอ่อน

ตัวอย่างที่ 3: ฐานข้อมูลการฆาตกรรมในชิคาโก

มหาวิทยาลัยรังสิต Rangsit University

ฐานข้อมูลนี้สร้างขึ้นเพื่อให้ข้อมูลเชิงลึกเกี่ยวกับการฆาตกรรมในชิคาโกเพื่อการวิจัยและการพัฒนานโยบาย อย่างไรก็ตาม ความล้มเหลวในการปกปิดข้อมูลอย่างเพียงพอนำไปสู่การระบุตัวเหยื่ออีกครั้ง ละเมิดความเป็นส่วนตัวและอาจส่งผลกระทบต่อการสอบสวนทางกฎหมายที่กำลังดำเนินอยู่และความเป็นอยู่ที่ดีของครอบครัวของเหยื่อ กรณีนี้เน้นย้ำถึงความจำเป็นในการพิจารณาอย่างรอบคอบและการลบข้อมูลระบุตัวตนที่เข้มงวด โดยเฉพาะอย่างยิ่งเมื่อต้องจัดการกับข้อมูลที่ละเอียดอ่อนและอาจกระทบกระเทือนจิตใจ

ตัวอย่างที่ 4: การประกวดรางวัลของเน็ตฟลิกซ์

ในปี 2549 เน็ตฟลิกซ์ได้เผยแพร่ชุดข้อมูลการจัดอันดับภาพยนตร์ของผู้ใช้สำหรับการแข่งขันเพื่อปรับปรุงอัลกอริทึมการแนะนำขึ้น แม้ว่าข้อมูลไม่เปิดเผยตัวตนแต่นักวิจัยจากมหาวิทยาลัยเท็กซัสได้แสดงให้เห็นว่าข้อมูลดังกล่าวก็สามารถลบข้อมูลระบุตัวบุคคลได้อีกครั้งโดยเชื่อมโยงข้อมูลที่ไม่เปิดเผยตัวตนกับข้อมูลที่เปิดเผยต่อสาธารณะ ซึ่งนำไปสู่การฟ้องร้องที่กล่าวหาว่าละเมิดกฎหมายความเป็นส่วนตัว และก่อให้เกิดความกังวลอย่างมากเกี่ยวกับความเป็นส่วนตัวในชุดข้อมูลที่ใช้สำหรับการเรียนรู้ของเครื่องและการวิเคราะห์ข้อมูล กรณีนี้เป็นเครื่องเตือนใจที่ชัดเจนถึงความเป็นไปได้ที่ข้อมูล “ที่ไม่เปิดเผยตัวตน” ยังคงมีข้อมูลเพียงพอที่จะระบุตัวบุคคล โดยเฉพาะอย่างยิ่งเมื่อมีการอ้างอิงโยงกับแหล่งข้อมูลอื่น

ตัวอย่างที่ 5: สถาบันสุขภาพแห่งชาติ (NIH)

NIH อยู่ในระดับแนวหน้าในการจัดทำข้อมูลทางพันธุกรรมและสุขภาพต่าง ๆ สำหรับการวิจัย อย่างไรก็ตามการศึกษาพบว่าบางครั้งสามารถระบุตัวบุคคลได้อีกครั้งจากชุดข้อมูลเหล่านี้โดยการเชื่อมโยงข้อมูลทางพันธุกรรมกับแหล่งข้อมูลอื่น ศักยภาพในการระบุตัวตนซ้ำอีกครั้งนี้ทำให้เกิดความท้าทายอย่างต่อเนื่องในการรักษาความเป็นส่วนตัวไปพร้อม ๆ กับการส่งเสริมการวิจัย ซึ่งเป็นประเด็นสำคัญของความตึงเครียดระหว่างการวิจัยทางวิทยาศาสตร์ที่ก้าวหน้าและการปกป้องความเป็นส่วนตัวของแต่ละบุคคล กรณีนี้เน้นถึงความสมดุลที่ละเอียดอ่อนซึ่งจำเป็นในการแบ่งปันข้อมูลเพื่อการวิจัย ในขณะเดียวกันก็รับประกันความเป็นส่วนและการรักษาความลับของบุคคลที่ปรากฏในข้อมูล

ตัวอย่างที่ 6: การระบุตัวตนซ้ำของเวชระเบียนของผู้ว่าการรัฐแมสซาชูเซตส์

เหตุการณ์นี้ เวชระเบียนของผู้ว่าการรัฐแมสซาชูเซตส์ได้รับการระบุตัวตนซ้ำอีกครั้งจากข้อมูลด้านสุขภาพที่ไม่ระบุชื่อ ซึ่งเผยแพร่โดย Group Insurance Commission นักวิจัยสามารถ

เชื่อมโยงข้อมูลการเยี่ยมโรงพยาบาลที่ไม่ระบุชื่อกับรายงานข่าวเกี่ยวกับการเข้ารับการรักษาในโรงพยาบาลของผู้ว่าการรัฐ จึงสามารถระบุบันทึกทางการแพทย์ของเขาได้ โดยเฉพาะอย่างยิ่งการเชื่อมโยงข้อมูลดังกล่าวกับผู้ว่าการรัฐ มันแสดงให้เห็นถึงศักยภาพของการโจมตีเพื่อระบุตัวตนซ้ำอีกครั้งแบบกำหนดเป้าหมายและผลกระทบที่ลึกซึ้งต่อความเป็นส่วนตัว กรณีนี้ทำหน้าที่เป็นสัญญาเตือนที่สำคัญเกี่ยวกับช่องโหว่ในกระบวนการลบข้อมูลระบุตัวตน และความจำเป็นในการป้องกันที่แข็งแกร่งต่อการระบุตนซ้ำ โดยเฉพาะอย่างยิ่งสำหรับบุคคลที่มีชื่อเสียงซึ่งข้อมูลอาจเป็นที่สนใจเป็นพิเศษ

จากกรณีตัวอย่างเหล่านี้ร่วมกันแสดงให้เห็นถึงความเสี่ยงและความท้าทายที่แพร่หลายที่เกี่ยวข้องกับการลบข้อมูลระบุตัวตนและการระบุตัวตนซ้ำอีกครั้ง โดยเน้นย้ำถึงความจำเป็นในการเฝ้าระวังอย่างต่อเนื่อง เทคนิคการปกป้องความเป็นส่วนตัวที่ซับซ้อน และความเข้าใจที่ครอบคลุมเกี่ยวกับแนวทางที่เป็นไปได้ที่ข้อมูลที่ไม่เปิดเผยตัวตนอาจถูกบุกรุกได้ เนื่องจากข้อมูลยังคงมีบทบาทสำคัญในภาคส่วนต่าง ๆ บทเรียนจากเหตุการณ์เหล่านี้ยังคงมีความสำคัญสำหรับการแจ้งนโยบาย แนวปฏิบัติ และโซลูชันทางเทคโนโลยีที่มุ่งปกป้องความเป็นส่วนตัวในยุคดิจิทัล

จีดีพีอาร์ได้แนะนำข้อกำหนดที่เข้มงวดในการจัดการข้อมูลส่วนบุคคลโดยเน้นที่การจัดการความยินยอมเป็นอย่างมาก ภายใต้จีดีพีอาร์ แนวคิดของการจัดการความยินยอมมีความสำคัญและมีหลายแง่มุมซึ่งไม่เพียงแต่เกี่ยวข้องกับการได้รับความยินยอมในเบื้องต้นจากเจ้าของข้อมูลเท่านั้น แต่ยังรวมถึงการจัดการความยินยอมอย่างต่อเนื่องด้วย ซึ่งรวมถึงการแก้ไข การถอน หรือการปรับปรุงให้เป็นปัจจุบัน และตรวจสอบให้แน่ใจว่าการจัดการข้อมูลส่วนบุคคลใด ๆ กระทำภายใต้การตั้งค่าและสิทธิ์ของแต่ละบุคคล เพื่อตอบสนองความท้าทายนี้เทคโนโลยีบล็อกเชนจึงกลายเป็นผู้เปลี่ยนเกมที่มีศักยภาพ เป็นที่รู้จักจากลักษณะเฉพาะของการเปลี่ยนแปลงไม่ได้ ความโปร่งใส และความปลอดภัย บล็อกเชนได้นำเสนอโซลูชันที่น่าสนใจเป็นนวัตกรรมสำหรับการจัดการความยินยอมภายใต้จีดีพีอาร์ ข้อเสนอก็คือ บล็อกเชนสามารถใช้เป็นที่เก็บบันทึกสาธารณะ โดยบันทึกทุกธุรกรรมการยินยอมอย่างถาวร (การอนุมัติ การถอน การปรับปรุง) ระหว่างเจ้าของข้อมูลและผู้ควบคุม สิ่งนี้จะสร้างเส้นทางการตรวจสอบที่ไม่เปลี่ยนแปลงและโปร่งใส เพื่อให้แน่ใจว่าได้รับบันทึกและจัดการความยินยอมตามข้อกำหนดจีดีพีอาร์ อย่างไรก็ตาม การใช้บล็อกเชนสาธารณะในการจัดการความยินยอมอาจจะไม่ใช่วิธีที่มีประสิทธิภาพหรือคุ้มค่าที่สุด เนื่องจากอาจมีต้นทุนการทำธุรกรรมที่สูงและข้อกังวลด้านความสามารถในการขยายขนาด เพื่อหลีกเลี่ยงปัญหาเหล่านี้องค์กรต่าง ๆ กำลังหันมาใช้บล็อกเชนส่วนตัวหรือแบบกลุ่ม ซึ่งสามารถสร้างสมดุลระหว่างประสิทธิภาพ

ความโปร่งใส และความปลอดภัยได้ วิธีการที่เป็นนวัตกรรมนี้ไม่เพียงแต่ช่วยลดความซับซ้อนที่เกี่ยวข้องกับการจัดการความยินยอมเท่านั้น แต่ยังรับประกันการปฏิบัติตามข้อกำหนดที่เข้มงวดของจีดีพีอาร์ ซึ่งส่งเสริมความไว้วางใจและความโปร่งใสในการจัดการข้อมูลส่วนบุคคล

มีคำถามต่าง ๆ ตามมาว่ากฎระเบียบและความก้าวหน้าของเทคโนโลยีจะสามารถก้าวไปด้วยกันได้หรือไม่โดยเฉพาะเทคโนโลยีบล็อกเชนที่กล่าวกันว่า บล็อกเชนมีการออกแบบระบบอยู่บนพื้นฐานที่ไม่ใช่แค่การเปลี่ยนแปลงข้อมูลไม่ได้แต่ข้อมูลเหล่านั้นจะมีการบันทึกอย่างถาวร ในรายงานของ European Parliament (2019) ระบุไว้ว่า เทคโนโลยีบล็อกเชนและข้อกำหนดของจีดีพีอาร์มีความขัดแย้งกันสองประการ กล่าวคือ

1) ประการแรก: จีดีพีอาร์ตั้งอยู่บนฐานความคิดที่ว่าในความสัมพันธ์ของข้อมูลส่วนบุคคล เป็นความสัมพันธ์ระหว่างบุคคลธรรมดาหรือนิติบุคคลอย่างน้อยหนึ่งคน ในฐานะ “ผู้ควบคุมข้อมูล” และ “เจ้าของข้อมูล” ซึ่งเจ้าของข้อมูลสามารถใช้สิทธิ์ของตนภายใต้ข้อกำหนดจีดีพีอาร์ในการแก้ไข เปลี่ยนแปลง หรือลบข้อมูลของตนได้ ผู้ควบคุมข้อมูลเหล่านั้นมีความรับผิดชอบต่อสิทธิ์เจ้าของข้อมูลตามจีดีพีอาร์ ในขณะที่บล็อกเชนเป็นฐานข้อมูลแบบกระจายศูนย์ ด้วยวัตถุประสงค์การกระจายอำนาจทำให้มีบุคคลหรือนิติบุคคลหลายคนขาดความเห็นเป็นเอกฉันท์ จึงไม่สามารถระบุได้ว่าใครมีอำนาจกระทำการหรือมีความรับผิดชอบตามข้อกำหนดจีดีพีอาร์

2) ประการที่สอง: จีดีพีอาร์ตั้งอยู่บนสมมติฐานที่ว่าข้อกำหนดสามารถแก้ไขหรือลบได้เมื่อจำเป็น เพื่อปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น มาตรา 16 และ 17 ขณะที่บล็อกเชนทำให้การแก้ไขข้อมูลทำได้ยากหรือแทบเป็นไปไม่ได้เลย จะมีเพียงการเพิ่มข้อมูลเข้าไปเพื่อเสริมความสมบูรณ์และความน่าเชื่อมั่นของเครือข่ายบล็อกเชนเท่านั้น

อย่างไรก็ตาม ในรายงานฉบับดังกล่าว นอกจากจะช่วยสำรวจความขัดแย้งและอุปสรรคของจีดีพีอาร์และบล็อกเชนแล้ว ยังคงเน้นย้ำถึงความจริงที่ว่าบล็อกเชนอาจช่วยส่งเสริมวัตถุประสงค์บางประการของจีดีพีอาร์ในการช่วยลดขนาดข้อมูลและการจำกัดวัตถุประสงค์ในการเก็บข้อมูลที่มักมีการนำไปใช้งานในเศรษฐกิจดิจิทัลหรือเศรษฐกิจข้อมูลในปัจจุบัน ถึงแม้ว่ารายงานฉบับนี้ได้ถูกเขียนขึ้นตั้งแต่ปี 2561 แต่ประเด็นปัญหาและแนวทางแก้ไขนับว่าร่วมสมัย เพราะพีดีพีเอของประเทศไทยเพิ่งจะประกาศใช้ ประกอบกับแนวโน้มการใช้เทคโนโลยีใหม่ ๆ ขององค์กรอย่างบล็อกเชน อาจนำมาซึ่งคำถามลักษณะเดียวกันว่า เทคโนโลยีบล็อกเชนจะขัดแย้งหรือช่วยส่งเสริมกับหลักการคุ้มครองข้อมูลส่วนบุคคล

ความตึงเครียดระหว่างเทคโนโลยีบล็อกเชนและข้อกำหนดความเป็นส่วนตัวของข้อมูลทั่วไป (Shah, Forester, Berberich, & Raspe, 2019, pp.1-20) ผู้ออกกฎหมายดูเหมือนจะไม่ให้ความสำคัญกับเทคโนโลยีบล็อกเชนและคุณลักษณะเฉพาะ เมื่อร่างกฎหมายและกรอบความเป็นส่วนตัวของข้อมูลล่าสุด คุณสมบัติบางประการของเทคโนโลยีบล็อกเชนสามารถช่วยลดหรือตอบสนองข้อกังวลด้านความเป็นส่วนตัว เช่น การใช้การเข้ารหัสและการตรวจสอบข้อมูลความซื่อสัตย์ อย่างไรก็ตาม สถาปัตยกรรมเครือข่ายแบบเพียร์ทูเพียร์แบบกระจายของเทคโนโลยีบล็อกเชนมักจะทำให้ขัดแย้งกับแนวคิดดั้งเดิมของการประมวลผลข้อมูลโดยใช้ตัวควบคุมจากส่วนกลางของจีดีพีอาร์ของสหภาพยุโรป และซีซีพีเอของแคลิฟอร์เนีย ความตึงเครียดที่สำคัญบางประการที่ต้องพิจารณา ได้แก่

1) มุมมองที่แตกต่างกันเกี่ยวกับการไม่เปิดเผยตัวตนและการใช้ข้อมูลแฝง และวิธีที่สิ่งเหล่านี้ส่งผลต่อการบังคับใช้การปกป้องข้อมูลต่าง ๆ และกฎหมายความเป็นส่วนตัว

2) วิธีระบุผู้ควบคุมข้อมูลและผู้ประมวลข้อมูลในการใช้งานเทคโนโลยีบล็อกเชนรูปแบบต่าง ๆ

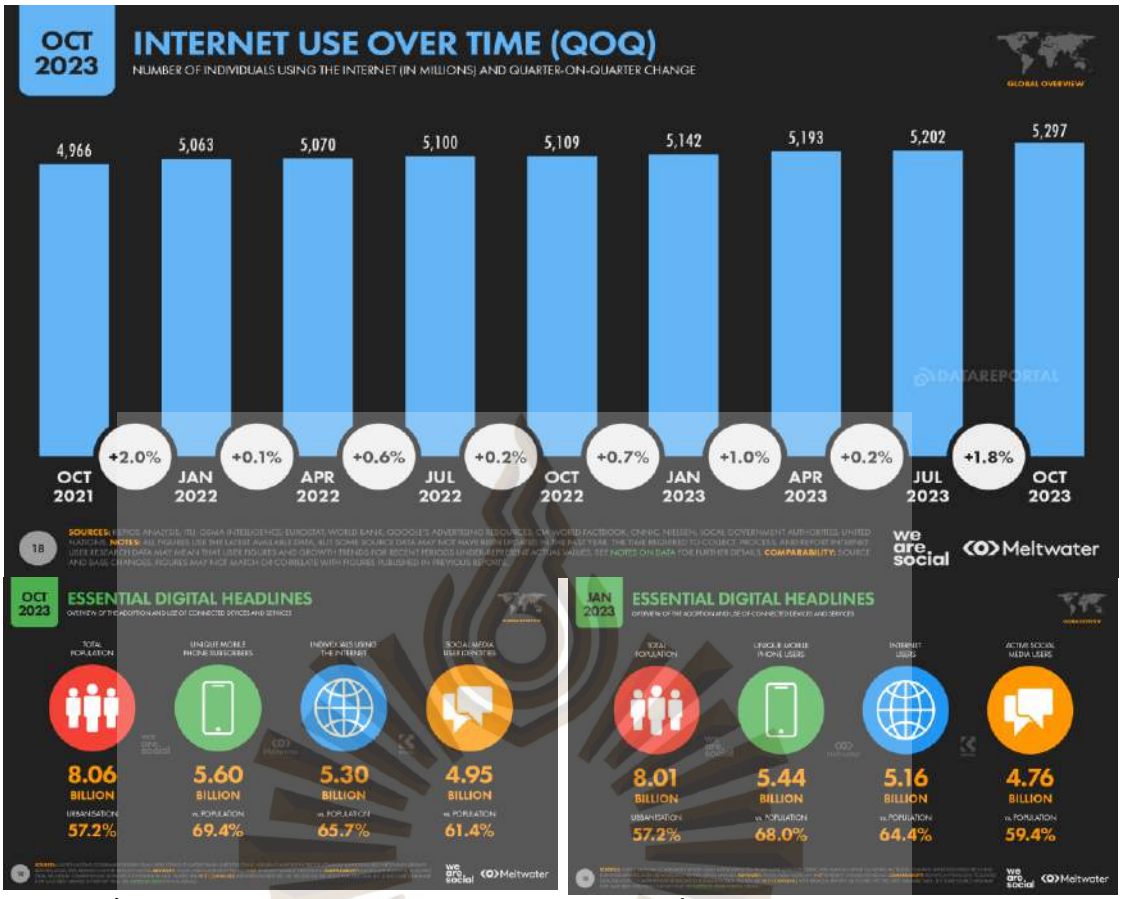
3) ผลกระทบด้านอาณาเขตสำหรับเครือข่ายบล็อกเชนแบบกระจายศูนย์

4) เมื่อเกิดการถ่ายโอนข้อมูลข้ามพรมแดนและข้อจำกัดที่อาจเกิดขึ้น

5) การใช้เกณฑ์สำหรับเหตุผลที่ชอบด้วยกฎหมายในการประมวลผลส่วนบุคคลต่อกรณีการใช้งานบล็อกเชน

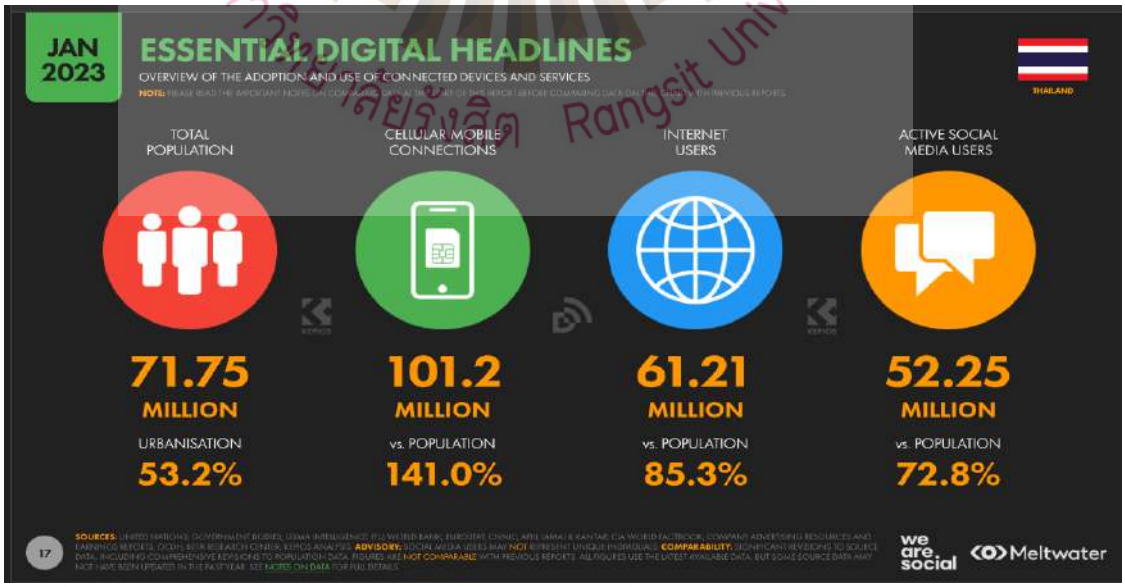
6) การกระทบยอดการทำธุรกรรมที่ไม่เปลี่ยนแปลงและการเก็บรักษาข้อมูลในแอปพลิเคชันบล็อกเชนด้วยสิทธิ์ส่วนบุคคล

จากรายงานของ Digital 2023 Global Overview Report พบว่า ในไตรมาสที่ 4 มีจำนวนประชากรที่ใช้อินเทอร์เน็ตทั่วโลกถึง 5.30 พันล้านคน คิดเป็น 65.7% ของประชากรทั่วโลก (8.06 พันล้านคน) มีจำนวนผู้ใช้อินเทอร์เน็ตที่เพิ่มขึ้น 1.9% และ 1.3% เมื่อเทียบกับปีที่แล้วในช่วงเวลาเดียวกันและต้นปี 2566 เป็นข้อมูล ณ เดือนตุลาคม 2566 ดังแสดงในรูปที่ 1.1 ซึ่งแสดงให้เห็นว่าผู้ใช้อินเทอร์เน็ตยังคงเติบโตเช่นกัน โดยข้อมูลล่าสุดระบุว่า จำนวนผู้ใช้ที่เชื่อมต่อกันทั่วโลกเพิ่มขึ้น 189 ล้านคนในช่วง 12 เดือนถึงเดือนตุลาคม 2566 ในขณะที่จำนวนประชากรที่ใช้อินเทอร์เน็ตของประเทศไทยมีถึง 61.21 ล้านคน คิดเป็น 85.3% ของประชากรทั้งประเทศ (71.75 ล้านคน) มีจำนวนผู้ใช้อินเทอร์เน็ตที่เพิ่มขึ้น 0.2% เมื่อเทียบกับปีที่แล้วในช่วงเวลาเดียวกัน เป็นข้อมูล ณ เดือนมกราคม 2566 ดังแสดงในรูปที่ 1.2 เนื่องด้วยการเจริญทางด้านดิจิทัลและสามารถเข้าถึงการใช้งานอินเทอร์เน็ตได้ง่าย พบว่าในปี 2566 ประเทศไทยมีสัดส่วนประชากรที่เข้าถึงอินเทอร์เน็ตได้สูงถึง 85.3% นั้นหมายความว่า แทบจะทุกคนในประเทศล้วนเข้าถึงโลกออนไลน์กันหมดแล้ว



รูปที่ 1.1 แสดงจำนวนประชากรและจำนวนประชากรที่ใช้อินเทอร์เน็ตทั่วโลกในปี 2566

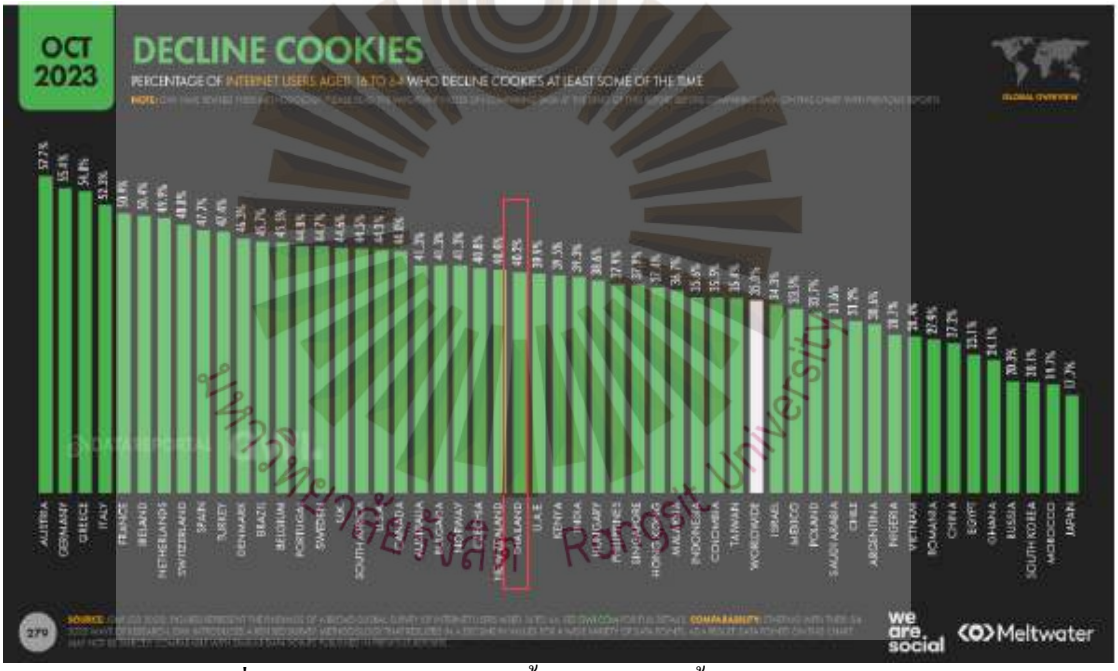
ที่มา: DataReportal.com, 2023



รูปที่ 1.2 แสดงจำนวนประชากรและจำนวนประชากรที่ใช้อินเทอร์เน็ตของประเทศไทยในปี 2566

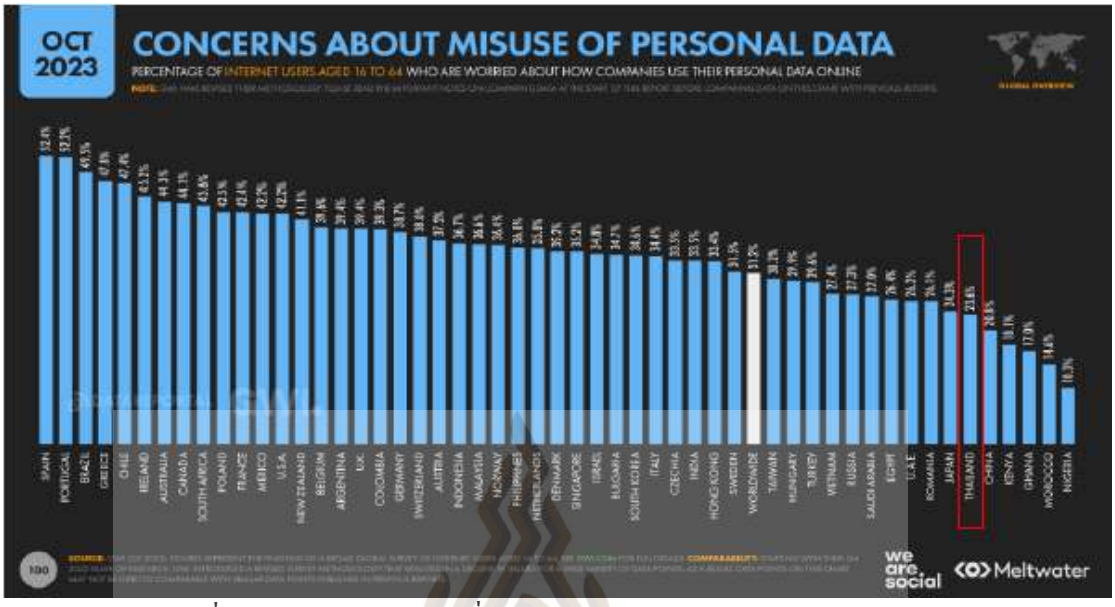
ที่มา: DataReportal.com, 2023

เมื่อกล่าวถึงความกังวลเรื่องข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล จากรูปที่ 1.3 จะเห็นได้ว่าผู้ใช้งานอินเทอร์เน็ตที่มีช่วงอายุ 16 – 64 ปี จะมีการปฏิเสธคุกกี้อย่างน้อย 1 ครั้ง คิดเป็นค่าเฉลี่ยทั่วอยู่โลกที่ 35.0% ในสหภาพยุโรปส่วนแบ่งของผู้ใช้อินเทอร์เน็ตที่ปฏิเสธคุกกี้เพิ่มขึ้นเป็นเกือบ 48% ซึ่งเพิ่มขึ้นมากกว่าหนึ่งในสามเมื่อเทียบกับค่าเฉลี่ยทั่วโลก ในขณะที่ประเทศไทยมีการปฏิเสธคุกกี้อย่างน้อย 1 ครั้ง คิดเป็น 40.2% ซึ่งสูงกว่าค่าเฉลี่ยทั่วโลกถึง 5.2% สำหรับความกังวลในเรื่องข้อมูลส่วนบุคคล จากรูปที่ 1.4 แสดงให้เห็นว่าค่าเฉลี่ยทั่วโลกอยู่ที่ 31.2% แต่ผู้ใช้อินเทอร์เน็ตในสหภาพยุโรปส่วนใหญ่กังวลเกี่ยวกับวิธีที่รัฐบาลติดตามพวกเขาทางออนไลน์ ซึ่งสูงกว่าเฉลี่ยทั่วโลกที่ 19.3% ในขณะที่ประเทศไทยมีความกังวลเพียง 23.6% เท่านั้น ซึ่งต่ำกว่าค่าเฉลี่ยทั่วโลกที่ถึง 7.6% นั้นก็หมายความว่าหน่วยงานภาครัฐและภาคเอกชนต้องให้ความรู้เรื่องข้อมูลส่วนบุคคลกับประชาชนให้มากขึ้น เพราะไม่อย่างนั้นเราคงได้เห็นข่าวข้อมูลรั่วไหลกันยังไม่รู้จบ



รูปที่ 1.3 แสดงการปฏิเสธคุกกี้อย่างน้อย 1 ครั้งของแต่ละประเทศ

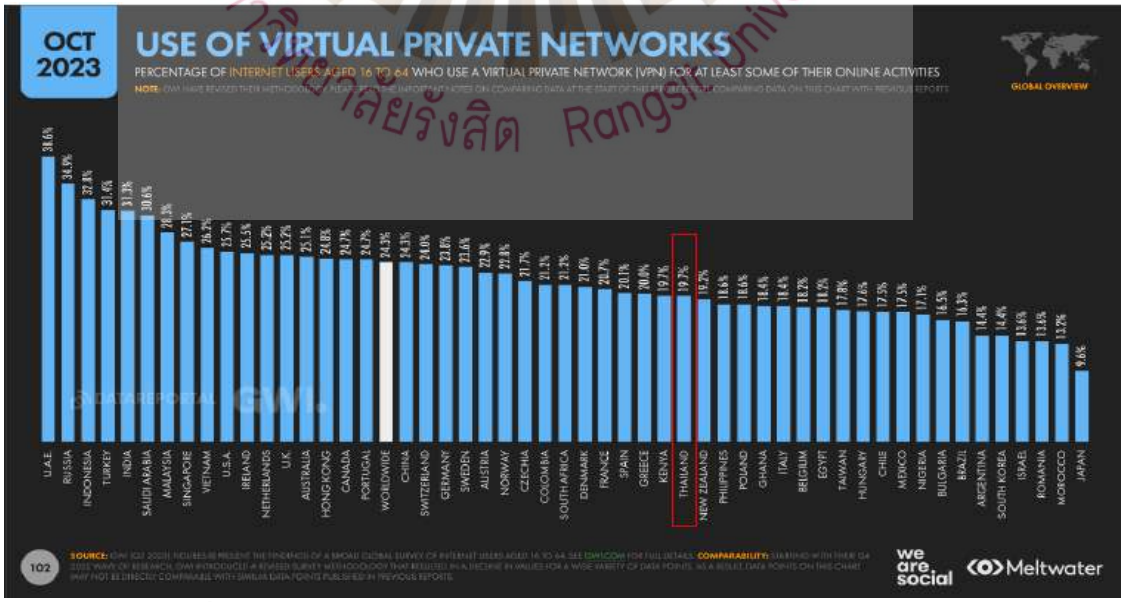
ที่มา: DataReportal.com, 2023



รูปที่ 1.4 แสดงความกังวลเกี่ยวกับข้อมูลส่วนบุคคลของแต่ละประเทศ

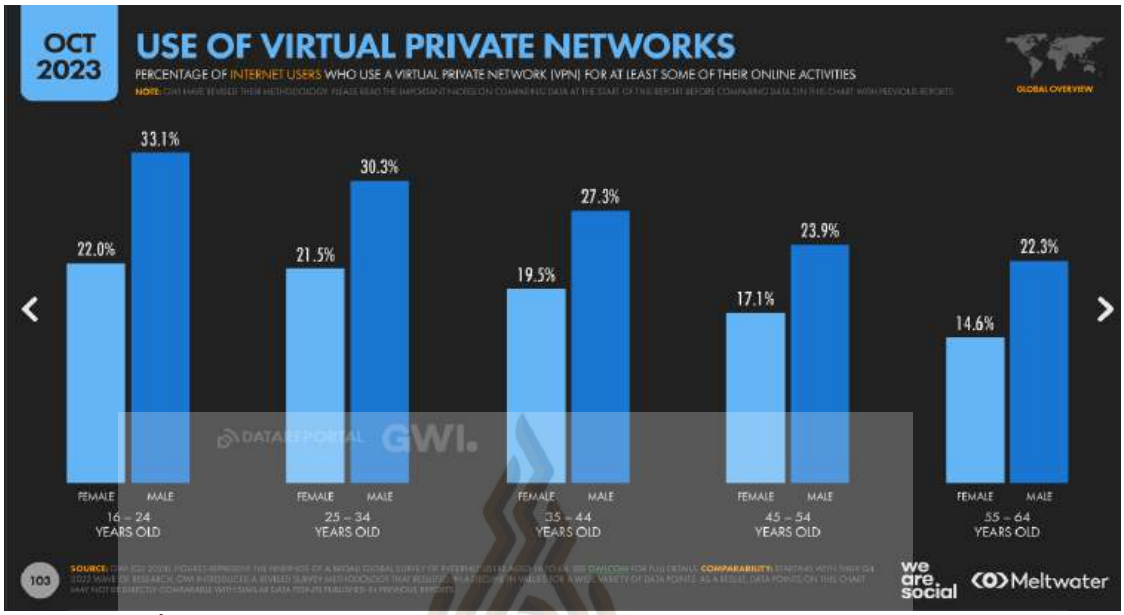
ที่มา: DataReportal.com, 2023

สำหรับการไม่เปิดเผยตัวตนบนโลกออนไลน์โดยการเชื่อมต่อกับเครือข่ายส่วนตัวเสมือน จากรูปที่ 1.5 พบว่าผู้ใช้งานในประเทศไทยมีการใช้งานเครือข่ายส่วนตัวเสมือน 19.7% สำหรับกิจกรรมออนไลน์ ซึ่งมีค่าต่ำกว่าค่าเฉลี่ยทั่วโลกถึง 4.6% และรูปที่ 1.6 แสดงให้เห็นว่ามีผู้หญิงจำนวนน้อยเมื่อเทียบกับผู้ชายและการใช้งานมีแนวโน้มลดลงตามอายุ มีการใช้งานมากสุดในช่วง 16-24 ปี



รูปที่ 1.5 แสดงการใช้เครือข่ายส่วนตัวเสมือน (VPN) ของแต่ละประเทศ

ที่มา: DataReportal.com, 2023



รูปที่ 1.6 แสดงภาพรวมการใช้เครือข่ายส่วนตัวเสมือน (VPN) ของแต่ละประเทศ

ที่มา: DataReportal.com, 2023

1.2 วัตถุประสงค์การวิจัย

งานวิจัยฉบับนี้เสนอเทคนิคใหม่ในการใช้ระบบบริหารจัดการความยินยอมและการแฝงข้อมูลโดยใช้เทคโนโลยีบล็อกเชนเป็นระบบช่วยเหลือ โดยมีวัตถุประสงค์หลักดังนี้

1.2.1 เพื่อให้ระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS) ที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชน ทำงานได้อย่างมีประสิทธิภาพ

1.2.2 เพื่อใช้เทคนิคการแฝงข้อมูลแบบใหม่รักษาความเป็นต้นฉบับของข้อมูลและยังสามารถปฏิบัติตามกฎหมายที่กำหนด

1.3 สมมติฐานการวิจัย

การประยุกต์ใช้เทคโนโลยีบล็อกเชนในการแก้ปัญหา การละเมิดข้อมูลส่วนบุคคล ดีกว่าวิธีอื่น ๆ อย่างมีประสิทธิภาพต่อ วิธีการให้ความยินยอม (Consent) และ วิธีการทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Non-identifiability)

1.4 ขอบเขตการวิจัย

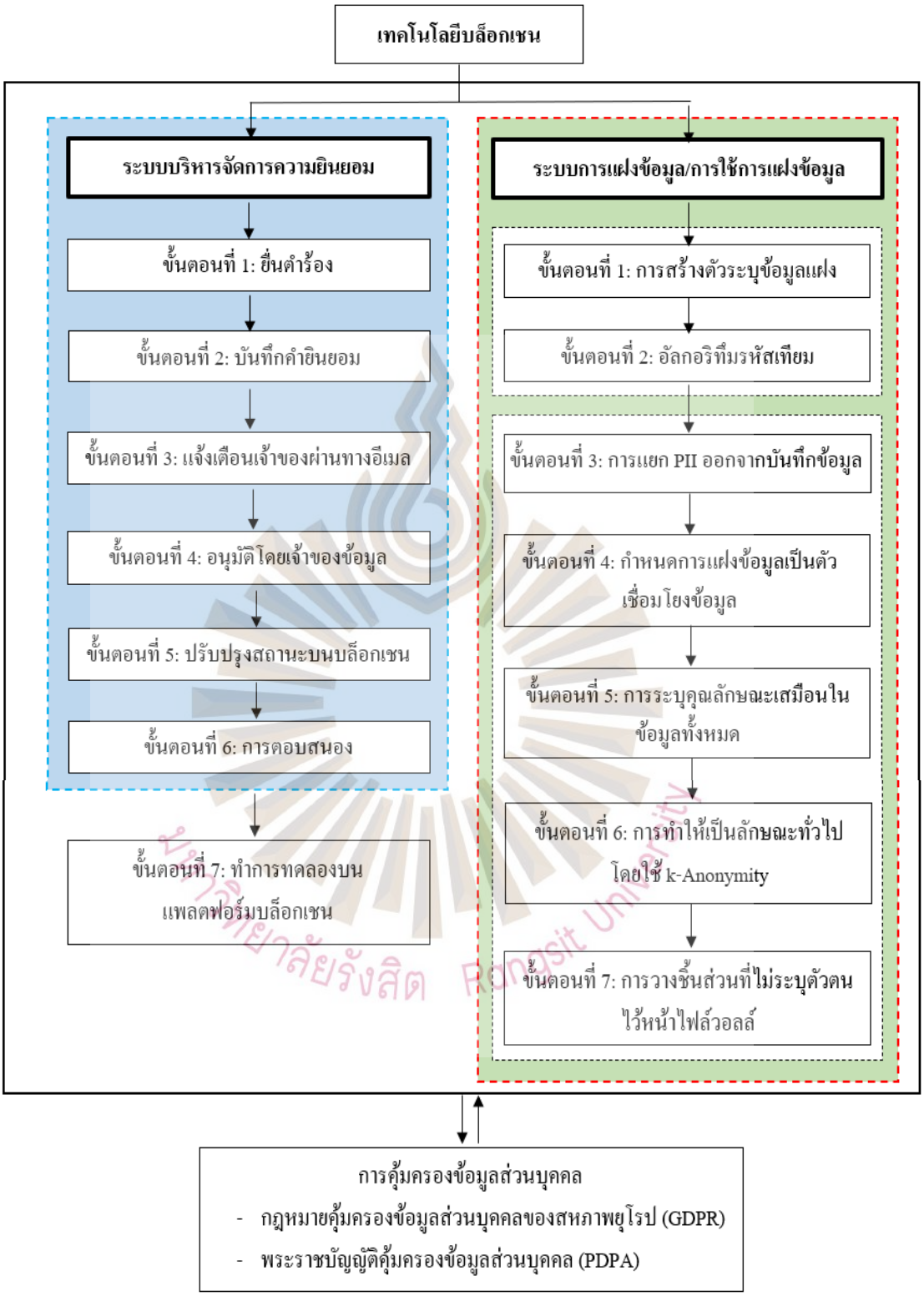
งานวิจัยนี้มุ่งเน้นการนำเอาคุณสมบัติเฉพาะของเทคโนโลยีบล็อกเชนมาเป็นเครื่องมือและตัวช่วยในการเก็บรวบรวม ปกป้อง และคุ้มครองข้อส่วนบุคคล โดยผ่านกระบวนการจัดการความยินยอมและการปกปิดข้อมูลด้วยเทคนิคการแฝงข้อมูล ให้เป็นไปตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ พีดีพีเอ (Personal Data Protection Act B.E. 2019 – PDPA) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ จีดีพีอาร์ (General Data Protection Regulation - GDPR)

1.5 กรอบแนวคิดการวิจัย

งานวิจัยฉบับนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ซึ่งผู้วิจัยได้ทำการศึกษาเกี่ยวกับข้อกำหนดของกรอบกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยและสหภาพยุโรป มีการใช้เครื่องมือและเทคโนโลยีอื่น ๆ ที่เกี่ยวข้องกับในการเก็บรวบรวมข้อมูล การปกป้องข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องและมีคุณภาพและประสิทธิภาพที่ดี

จากการทบทวนวรรณกรรมจำนวนมากพบว่า มีการศึกษาและการประยุกต์ใช้บล็อกเชนในแนวปฏิบัติของพีดีพีเอมีจำนวนน้อยมาก การศึกษาเกี่ยวข้องกับการทบทวนวรรณกรรมและเอกสาร ซึ่งเครื่องมือการวิจัยเหล่านี้ช่วยให้สามารถรวบรวมข้อมูลเพื่อให้แน่ใจว่ามีการจัดระเบียบที่ดีและเหมาะสมของแหล่งที่มาซึ่งใช้ในการวิจัย จากการทบทวนวรรณกรรมที่เกี่ยวข้องสามารถนำมาพัฒนากรอบแนวคิดที่ใช้สำหรับงานวิจัยฉบับนี้ได้ดังรูปที่ 1.7 เพื่อแสดงถึงขอบเขตกระบวนการดำเนินงานวิจัยด้วยการใช้เทคโนโลยีบล็อกเชนให้เป็นระบบช่วยเหลือเพื่อบรรลุวัตถุประสงค์ของงานวิจัย กล่าวคือ มีกระบวนการในการดำเนินการวิจัยอยู่ 2 กระบวนการคือ การใช้ทฤษฎีการจัดการความยินยอม และทฤษฎีการการแฝงข้อมูล

จากกรอบแนวคิดในงานวิจัยในการศึกษาเบื้องต้น ดังรูปที่ 1.7 ผู้วิจัยใช้ชุดข้อมูลชื่อ “Adult.csv” ซึ่งเป็นข้อมูลการสำรวจประชากรของประเทศสหรัฐอเมริกาในปี 2537 จาก UCI Machine Learning Repository ซึ่งชุดข้อมูลนี้เป็น De Facto Standard problem และนิยมถูกใช้เพื่อเป็นเกณฑ์มาตรฐานในการปกปิดข้อมูล ในการทำการทดลองงานวิจัย ซึ่งในชุดข้อมูลนี้ประกอบไปด้วยข้อมูลของ เพศ อายุ เชื้อชาติ สถานภาพการสมรส ระดับการศึกษา อาชีพ รายได้ เป็นต้น จากนั้นทำการนำข้อมูลของ หมายเลขบัตรประชาชน ชื่อ นามสกุล และที่อยู่ มารวมเข้ากับชุดข้อมูล “adult.csv” และได้เรียกชุดข้อมูลนี้ว่า “Full-Adult-database.csv”



รูปที่ 1.7 กรอบแนวคิดการทำวิจัยระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล

1.6 ประโยชน์ที่ได้รับจากการวิจัย

งานวิจัยเรื่อง “ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล” มุ่งเน้นการแก้ปัญหาการละเมิดสิทธิ์ การขออนุญาต และการขอสิทธิ์ โดยใช้วิธีใหม่ที่ยังไม่เคยมีใครนำเสนอมาก่อน กล่าวคือ การนำเอาเทคโนโลยีบล็อกเชนเข้ามาช่วยบริหารจัดการสิทธิ์ในการขอใช้และการปกปิดข้อมูลด้วยเทคนิคการแฝงข้อมูล โดยรวมเอาจุดเด่นของหลากหลายเทคนิควิธีมาประมวลเป็นวิธีใหม่แนวคิดใหม่ที่ตอบโจทย์ปัญหาการละเมิดสิทธิ์ส่วนบุคคล ไม่เพียงแต่ผลักดันขอบเขตทางเทคโนโลยีเท่านั้น แต่ยังมีโอกาสที่จะปรับเปลี่ยนแนวทางปฏิบัติและนโยบายในการจัดการข้อมูลและการปกป้องความเป็นส่วนตัวอีกด้วย เป็นงานวิจัยที่ที่มีองค์ประกอบทางวิชาการที่หลากหลาย นวัตกรรมทางเทคโนโลยี และการกำหนดนโยบาย ซึ่งสะท้อนให้เห็นถึงความสำคัญที่เพิ่มขึ้นของความเป็นส่วนตัวของข้อมูลในยุคดิจิทัล ดังนั้น ประโยชน์ที่คาดว่าจะได้รับจากการวิจัยฉบับนี้มีดังนี้

1) กรอบการบริหารจัดการความยินยอมที่เป็นนวัตกรรม:

เสนอกรอบการทำงานใหม่สำหรับการบริหารจัดการความยินยอมของผู้ใช้ โดยเฉพาะอย่างยิ่งในสถานการณ์ที่เกี่ยวข้องกับข้อมูลที่ละเอียดอ่อนหรือข้อมูลส่วนบุคคล การวิจัยเจาะลึกว่าบล็อกเชนสามารถรับประกันได้อย่างไรว่าความยินยอมจะถูกบันทึกอย่างไม่เปลี่ยนแปลงโดยให้เส้นทางความยินยอมที่โปร่งใสและตรวจสอบได้

2) แอปพลิเคชันและระบบอัตโนมัติด้วยสัญญาอัจฉริยะ:

ตรวจสอบการใช้สัญญาอัจฉริยะในกระบวนการบริหารจัดการความยินยอมโดยอัตโนมัติ เพื่อให้มั่นใจว่าการตั้งค่าของผู้ใช้จะถูกบังคับใช้อย่างสม่ำเสมอและไม่มีอคติ ระบบอัตโนมัตินี้สามารถปรับปรุงความคล่องตัวในการปฏิบัติตามข้อกำหนดและกระบวนการจัดการข้อมูลทำให้มีประสิทธิภาพมากขึ้นและเสี่ยงต่อข้อผิดพลาดน้อยลง

3) การปฏิบัติตามกฎหมาย กฎระเบียบ และการปรับตัว:

ตอบสนองความต้องการที่สำคัญสำหรับองค์กรในการปฏิบัติตามกฎหมายและกฎระเบียบการปกป้องข้อมูลที่เข้มงวด เช่น จีดีพีอาร์ในยุโรป และ พีดีพีเอในประเทศไทย การวิจัยสำรวจว่าระบบที่ใช้บล็อกเชนสามารถช่วยในการตอบสนองข้อกำหนดเหล่านี้ได้อย่างไร ซึ่งอาจกำหนดมาตรฐานใหม่สำหรับการปฏิบัติตามกฎระเบียบในการจัดการข้อมูล

4) การปรับปรุงเทคนิคความเป็นส่วนตัวของข้อมูล:

พัฒนาและปรับปรุงวิธีการสำหรับการใช้การแฝงข้อมูล ซึ่งเป็นกระบวนการที่

แทนที่ตัวระบุส่วนบุคคลในชุดข้อมูลด้วยตัวระบุหรือข้อมูลแฝงหรือนามแฝง การบูรณาการร่วมกับฟังก์ชันแฮชบนบล็อกเชนทำให้เกิดความปลอดภัยและความรับผิดชอบอีกชั้นหนึ่ง ซึ่งมีส่วนช่วยในการพัฒนาแนวปฏิบัติและวิธีการด้านความเป็นส่วนตัวของข้อมูล

5) การบูรณาการการใช้การแฝงข้อมูลร่วมกับเทคโนโลยีบล็อกเชน:

สำรวจการทำงานร่วมกันระหว่างเทคโนโลยีบล็อกเชนและเทคนิคการแฝงข้อมูล ซึ่งรวมถึงการศึกษาผลกระทบของลักษณะที่ไม่เปลี่ยนรูปและโปร่งใสของบล็อกเชนต่อประสิทธิภาพและความน่าเชื่อถือของการใช้การแฝงข้อมูลในการปกป้องความเป็นส่วนตัวของผู้ใช้

1.7 นิยามศัพท์

Anonymization หรือ การทำให้เป็นนิรนาม หมายถึง กระบวนการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนของบุคคลได้ เพื่อวัตถุประสงค์ด้านการคุ้มครองข้อมูลส่วนบุคคล โดยการนำข้อมูลที่ใช้ระบุตัวตนของบุคคลได้ในชุดข้อมูลมาเข้ารหัส ลบ หรือทำลาย ตามกฎหมายที่ได้ระบุไว้ ด้วยว่าการทำให้เป็นนิรนามอย่างแท้จริง ข้อมูลดังกล่าวควรจะไม่สามารถกู้กลับคืนมาเป็นลักษณะดั้งเดิมที่สามารถระบุตัวตนของบุคคลได้อีก

Blockchain หรือ บล็อกเชน หมายถึง วิธีการเก็บข้อมูลรายการเปลี่ยนแปลงตามหลักการทางบัญชี โดยการเข้ารหัสและจัดเรียงข้อมูลเหล่านี้ต่อกันตามลำดับเวลาที่ข้อมูลเข้ามา กลุ่มข้อมูลดังกล่าวจะเผยแพร่ไปให้ผู้ใช้ในเครือข่ายที่กำหนดได้ทราบทั่วกัน ทั้งนี้ผู้ใช้ทุกคนจะทราบการแก้ไขเพิ่มเติมรายการเปลี่ยนแปลงในบล็อกเชนทุกรายการตลอดเวลา

Consensus หรือ ฉันทามติ หมายถึง การกำหนดข้อตกลงและความเห็นชอบร่วมกันระหว่างสมาชิกในเครือข่ายบล็อกเชน โดยสมาชิกต้องยอมรับกฎระเบียบร่วมกัน ด้วยกลไกในการควบคุมความถูกต้องของข้อมูลในทุกโหนดผ่านอัลกอริทึมต่าง ๆ เพื่อให้ข้อมูลมีความถูกต้อง เที่ยงตรง และเป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน

Consensus Algorithm หรือ กลไกฉันทามติ หมายถึง มาตรการหรือกลไกที่เครือข่ายบล็อกเชนใช้ในการยืนยันความน่าเชื่อถือของธุรกรรม โดยผู้ที่จะมายืนยันความเชื่อถือของธุรกรรมต้องมีการ “เดิมพัน” ด้วยอะไรบางอย่าง เครือข่ายถึงจะสามารถยอมรับการตัดสินนั้น ๆ ได้

Consent หรือ ความยินยอม หมายถึง การแสดงเจตนาของเจ้าของข้อมูลส่วนบุคคล หรือผู้มีอำนาจกระทำการแทนเจ้าของข้อมูลส่วนบุคคล อนุญาตให้ผู้อื่นเก็บรวบรวมข้อมูล ใช้ข้อมูล หรือเผยแพร่ข้อมูลส่วนบุคคลผ่านเอกสารหรือผ่านระบบอิเล็กทรอนิกส์ โดยการกระทำข้างต้นจะถือว่าไม่เป็นการละเมิด ไม่ถือว่าเป็นความเสียหาย บุคคลจึงไม่มีสิทธิ์เรียกค่าเสียหายอันเกิดจากการกระทำที่ตนให้ความยินยอม

Consent Management หรือ การจัดการความยินยอม หมายถึง กระบวนการขอความยินยอมจากผู้ใช้และอนุญาตให้ผู้ใช้จัดการข้อมูลที่แชร์และวัตถุประสงค์ของการแชร์ การจัดการความยินยอมมีทั้งนโยบายที่นำมาใช้ในการจัดการความยินยอมของผู้ใช้ และการใช้งานทางเทคนิคที่ช่วยให้ผู้ใช้ตัดสินใจเกี่ยวกับวิธีการรวบรวมหรือใช้ข้อมูลของตน

Cryptocurrency หรือ เงินตราเข้ารหัสลับ, คริปโทเคอร์เรนซี หมายถึง สินทรัพย์ดิจิทัลที่เป็นสื่อกลางในการทำธุรกรรม ซึ่งใช้วิทยาการเข้ารหัสลับสำหรับรับประกันความถูกต้องของธุรกรรมนั้น เพื่อควบคุมการสร้างหน่วยเงินดิจิทัลเพิ่ม และ เพื่อยืนยันความถูกต้องของการโอนสินทรัพย์ เป็นเงินดิจิทัลรูปแบบหนึ่งที่ควบคุมโดยกระจายศูนย์ผ่านบล็อกเชน

Data Controllers หรือ ผู้ควบคุมข้อมูล หมายถึง บุคคลหรือนิติบุคคลที่มีอำนาจที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล

Data Processors หรือ ผู้ประมวลผลข้อมูล หมายถึง บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

Data Subject หรือ เจ้าของข้อมูล หมายถึง ลักษณะเป็นบุคคลที่ข้อมูลนั้นบ่งชี้ไปถึง ไม่เป็นเจ้าของในลักษณะทรัพยสิทธิ หรือเป็นคนสร้างข้อมูลนั้นขึ้นมา

Data Subject Rights หรือ สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล หมายถึง การให้ความคุ้มครองตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เจ้าของข้อมูลส่วนบุคคลสามารถขอใช้สิทธิ์กับผู้ควบคุมข้อมูลส่วนบุคคลได้หากเจ้าของข้อมูลมีความประสงค์

De-identification หรือ การปิดบังตัวตน หมายถึง กระบวนการขจัดข้อมูลส่วนที่ใช้ระบุตัวตนได้โดยทั้งทางตรงและทางอ้อมออกจากตัวข้อมูล รวมถึงการแฝงข้อมูล และการทำข้อมูลให้เป็นนิรนาม

Encryption หรือ การเข้ารหัสข้อมูล หมายถึง รูปแบบการจัดการข้อมูลอย่างหนึ่ง เพื่อวัตถุประสงค์ด้านการคุ้มครองข้อมูลส่วนบุคคล โดยกระบวนการนำข้อมูลส่วนบุคคลมาเข้ารหัสที่คนทั่วไปไม่สามารถเข้าใจได้ โดยเฉพาะผู้ที่ได้รับอนุญาตหรือมีกุญแจเท่านั้นที่จะสามารถถอดรหัสกลับคืนมาเป็นข้อมูลธรรมดาที่สามารถอ่านเข้าใจได้อีกครั้งหนึ่ง

GDPR หรือ จีดีพีดาร์ ย่อมาจาก General Data Protection Regulation หมายถึง กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

Hash หรือ **Hash function** หมายถึง กลไกในการแปลงข้อมูล โดยการนำเอาข้อมูลต่าง ๆ มาทำการเข้ารหัสและผ่านกระบวนการทางคณิตศาสตร์ซึ่งเรียกว่า Hash เพื่อให้เกิดข้อมูลที่มีลักษณะเฉพาะ ซึ่งในที่นี้เรียกว่า “ค่าแฮช (Hash value)”

IPOO ย่อมาจาก **Input, Process, Output, Outcome** หมายถึง กรอบแนวคิดที่ใช้ในการวิเคราะห์และอธิบายการดำเนินงานของระบบหรือโครงสร้าง โดยเน้นการเชื่อมโยงระหว่างทรัพยากรนำเข้า กระบวนการทำงาน ผลลัพธ์ที่เกิดขึ้น และผลกระทบในระยะยาว

k-Anonymity หมายถึง แบบจำลองที่จะการันตีว่าทุกลักษณะของข้อมูลจะมีอย่างน้อย k-1 รายการ ซึ่งจะทำให้ผู้ที่ต้องการจะโจมตีไม่สามารถทำการระบุตัวตนของข้อมูลได้

PDPA หรือ พีดีพีเอ ย่อมาจาก Personal Data Protection Act หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล

Personal Data หรือ ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรมไปแล้ว

Personal Data Privacy or Information Privacy หรือ ความเป็นส่วนตัวของข้อมูลส่วน

บุคคล หมายถึง การให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและบริหารจัดการข้อมูลส่วนบุคคล ที่บุคคลอื่นห้ามเก็บรวบรวม ใช้ หรือเผยแพร่โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคล

Personal Data Protection หรือ การคุ้มครองข้อมูลส่วนบุคคลโดยกฎหมาย ซึ่งเป็นการจำกัดสิทธิและเสรีภาพบางประการของบุคคลที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น เพื่อให้เกิดการคุ้มครองข้อมูลส่วนบุคคลและมาตรการเยียวยาเจ้าของข้อมูลที่มีประสิทธิภาพ

Privacy Policy หมายถึง นโยบายคุ้มครองข้อมูลส่วนบุคคล เป็นนโยบายที่เกี่ยวกับแนวทางการจัดเก็บรวบรวม และใช้งานข้อมูลส่วนบุคคลภายในองค์กร/หน่วยงาน ซึ่งจะเกี่ยวข้องโดยตรงกับพนักงานที่ใช้ข้อมูลส่วนบุคคลไม่ว่าจะเก็บ หรือใช้ ก็ตาม ดังนั้นพนักงานต้องเข้าใจ และทำตามนโยบายที่องค์กรกำหนดมาอย่างเคร่งครัด

Pseudonymization หรือ การแฝงข้อมูล หมายถึง รูปแบบการจัดการข้อมูลอย่างหนึ่ง เพื่อวัตถุประสงค์ด้านการคุ้มครองข้อมูลส่วนบุคคลโดยการทดแทนข้อมูลบางส่วนที่สามารถระบุตัวตนของบุคคลในชุดข้อมูลด้วยข้อมูลแฝงหรือนามแฝงซึ่งประดิษฐ์ขึ้น การใช้ข้อมูลแฝงหรือนามแฝงจะช่วยให้สามารถระบุตัวตนของบุคคลได้ยากขึ้นขณะการโอนเคลื่อนย้ายข้อมูลหรือเมื่อถูกจารกรรม แต่ยังเป็นรูปแบบข้อมูลที่สามารถนำมาแปลงกลับมาเพื่อระบุตัวตนซ้ำอีกครั้ง เมื่อมีข้อมูลประกอบเพิ่มเติม

Quasi-identifiers หมายถึง กลุ่มของแอตทริบิวต์ที่มีความสามารถเพียงพอที่จะระบุตัวตนซ้ำได้เมื่อนำมารวมกับข้อมูลสาธารณะ

Re-identification หรือ การระบุตัวตนซ้ำ หมายถึง กระบวนการที่ข้อมูลส่วนบุคคลที่ไม่ระบุชื่อถูกจับคู่กับเจ้าของที่แท้จริง เพื่อปกป้องผลประโยชน์ความเป็นส่วนตัวของเจ้าของข้อมูล

Request for Consent หรือ การขอความยินยอม หมายถึง การที่ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อาจกระทำผ่านเอกสารหรือผ่านระบบอิเล็กทรอนิกส์อย่างชัดเจน

มหาวิทยาลัยรังสิต Rangsit University

RSU-CMS หมายถึง ระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (Rangsit University Consent Management System)

Sensitive Personal Data หรือ ข้อมูลละเอียดอ่อน หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อน และ สุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ

Smart Contract หรือ สัญญาอัจฉริยะ หมายถึง โปรแกรมคอมพิวเตอร์ที่มีการดำเนินงานอัตโนมัติ ตามสัญญาหรือข้อกำหนดที่ระบุไว้ โดยเป้าหมายของสัญญาอัจฉริยะคือการลดการมีคนกลางของสัญญา ลดค่าใช้จ่ายของคนกลาง เพิ่มความโปร่งใส และลดความผิดพลาดที่เกิดขึ้นโดยการทำงานผ่านบล็อกเชน

VPN ย่อมาจาก Virtual Private Network หมายถึง เครือข่ายส่วนตัวเสมือน เป็นการสร้างการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่าง ๆ ผ่านอินเทอร์เน็ต

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

2.1 เทคโนโลยีบล็อกเชน (Blockchain)

บล็อกเชน เป็นเทคโนโลยีการเก็บข้อมูลแบบกระจายศูนย์ (Decentralize) ที่ใช้สำหรับจัดการและเก็บข้อมูลโดยไม่มีการตรวจสอบจากบุคคลกลาง (Central Authority) เช่น ธนาคารหรือรัฐบาล โดยสามารถเก็บข้อมูลได้เพียงแต่บันทึกข้อมูลลงในบล็อก (Block) แล้วนำบล็อกที่บันทึกแล้วมาเชื่อมต่อเข้าด้วยกันเป็นเชน (Chain) โดยแต่ละบล็อกจะมีข้อมูลที่ถูกเข้ารหัส (Encrypted) และเชื่อมโยงกับบล็อกก่อนหน้านั้น ๆ ด้วยการระบุค่าทางคณิตศาสตร์ที่เรียกว่าแฮช (Hash) ซึ่งทำให้ข้อมูลที่ถูกบันทึกไว้ในบล็อกไม่สามารถแก้ไขหรือเปลี่ยนแปลงบล็อกทั้งหมดในเชนนั้น ๆ โดยบล็อกเชนมีการใช้งานอย่างแพร่หลายในการเก็บข้อมูลสินทรัพย์ดิจิทัล เช่น สกุลเงินดิจิทัล (Cryptocurrency) หรือการเก็บข้อมูลส่วนบุคคลที่มีความปลอดภัยสูง เนื่องจากบล็อกเชนมีการใช้เทคโนโลยีเข้ารหัสที่มีความซับซ้อนและต้องการความยืดหยุ่นต่อการเข้าถึงข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต จึงทำให้สามารถใช้งานบล็อกเชนเพื่อให้การเก็บข้อมูลและการทำธุรกรรมออนไลน์เป็นไปอย่างปลอดภัยและเชื่อถือได้มากยิ่งขึ้น

เทคโนโลยีบล็อกเชนได้รับการเปิดเผยเป็นครั้งแรกในปีพ.ศ. 2551 โดย Satoshi Nakamoto ในบทความเรื่อง “Bitcoin: A Peer-to-Peer Electronic Cash System” ซึ่งเป็นเทคโนโลยีที่เงินตราเข้ารหัสลับบิตคอยน์ (Bitcoin Cryptocurrency) ทำงานบนบล็อกเชน บล็อกเชนเป็นรายการบันทึกที่ป้องกันการดัดแปลงที่นำไปใช้ในรูปแบบของบัญชีแยกประเภทแบบกระจายศูนย์ (Nakamoto, 2008, pp.1-9)

เทคโนโลยีบล็อกเชนคาดว่าจะปฏิวัติอุตสาหกรรมและการพาณิชย์และขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมในระดับโลกในยุคดิจิทัล ซึ่งเพราะเป็นสิ่งที่เปลี่ยนแปลงไม่ได้ โปร่งใส และนิยามใหม่ของความไว้วางใจ ทำให้เกิดโซลูชันที่ปลอดภัย รวดเร็ว เชื่อถือได้ และโปร่งใส ด้วยเหตุนี้ทำให้เทคโนโลยีบล็อกเชนได้รับความสนใจและทำการศึกษากันอย่างกว้างขวางทั้งในประเทศและต่างประเทศ นอกจากนั้นยังมีบทบาทในการยกระดับการบริหารงานและการบริการประชาชน

ภาครัฐเพื่อเข้าสู่การเป็นรัฐบาลดิจิทัล (Digital Government) รวมถึง การเข้าไปเปลี่ยนวิถีชีวิตของภาคประชาชนไปสู่ความสะดวกสบายมากขึ้น (สำนักงานพัฒนารัฐบาลดิจิทัล (องค์กรมหาชน), 2564)

2.1.1 วิวัฒนาการของเทคโนโลยีบล็อกเชน (Lin, Zhang, Li, Ji, & Sun, 2022, pp. 635-690)

2.1.1.1 ยุคริเริ่ม (2534 – 2551)

บล็อกเชนได้รับการจินตนาการโดย Stuart Haber และ W. Scott Stornetta ในปี พ.ศ. 2534 พวกเขาเริ่มต้นด้วยการทำงานบนเชนของบล็อกที่มีการรักษาความปลอดภัยโดยการเข้ารหัส ไม่สามารถแก้ไขการประทับเวลาของเอกสารได้ วิธี Merkle Tree ได้ถูกรวมเข้ากับระบบในปีพ.ศ. 2535 สิ่งนี้ช่วยให้ระบบมีประสิทธิภาพมากขึ้นและตอนนี้สามารถใส่เอกสารได้มากขึ้นในบล็อกเดียว แต่บล็อกเชนเริ่มมีบทบาทในปีพ.ศ. 2551 เพราะ Nakamoto มักถูกเรียกว่ามันสมองที่อยู่เบื้องหลังเทคโนโลยีนี้ Nakamoto ยังคงเป็นปริศนาจนถึงปัจจุบัน Nakamoto ได้รับเครดิตจากการวางแนวคิดของเทคโนโลยีบล็อกเชนครั้งแรกในปีพ.ศ. 2551 ตั้งแต่นั้นเป็นต้นมาเทคโนโลยีก็พัฒนาอย่างต่อเนื่องและหาทางนำไปใช้ในแอปพลิเคชันอื่นที่ไม่ใช่สกุลเงินดิจิทัลอีกด้วย

2.1.1.2 ยุคบล็อกเชน 1.0 หรือยุคธุรกรรม (2551 – 2556)

บิตคอยน์ (Bitcoin) ถือกำเนิดขึ้นในปีพ.ศ. 2551 โดยเป็นแอปพลิเคชันแรกในประวัติศาสตร์ของเทคโนโลยีบล็อกเชน เนื่องจากเป็นช่วงที่บล็อกเชนบิตคอยน์เริ่มได้รับความนิยมผู้คนจำนวนมากจึงสับสนว่าบิตคอยน์และบล็อกเชนเป็นสิ่งเดียวกัน ในปีพ.ศ. 2551 Nakamoto ได้เปิดตัวเอกสารบทความฉบับแรกเกี่ยวกับเทคโนโลยีบล็อกเชน ในบทความนี้พวกเขาอธิบายว่าบล็อกเชนเป็นระบบอิเล็กทรอนิกส์แบบเพียร์ทูเพียร์ (Peer-to-Peer) Nakamoto ได้สร้างบล็อกแรกหรือบล็อกเจเนซิส ซึ่งทำให้บล็อกอื่น ๆ ถูกขุดขึ้นมา บล็อกเหล่านี้เชื่อมต่อกันก่อตัวเป็นบล็อกที่ใหญ่ที่สุดกลุ่มหนึ่งที่มีข้อมูลที่แตกต่างกัน เมื่อบิตคอยน์เริ่มได้รับความนิยมแอปพลิเคชันอื่น ๆ จำนวนมากก็เกิดขึ้นพร้อมกับวิวัฒนาการของเทคโนโลยีบล็อกเชน

2.1.1.3 ยุคบล็อกเชน 2.0 หรือยุคสัญญา (2556 – 2558)

นักพัฒนาชื่อ Vitalik Buterin มีความกังวลเกี่ยวกับข้อจำกัดของบิตคอยน์ที่มาก

เกินไป ตามที่เขากล่าวว่า บิตคอยน์ไม่สามารถใช้ประโยชน์จากเทคโนโลยีบล็อกเชนได้อย่างเหมาะสม ดังนั้นเขาจึงเริ่มทำงานกับบล็อกเชนที่ไม่จำกัดเพียงแค่เทคโนโลยีแบบเพียร์ทูเพียร์เท่านั้น อีเธอเรียม (Ethereum) จึงได้รับการพัฒนาเป็นบล็อกเชนสาธารณะขึ้นใหม่ในปีพ.ศ. 2556 โดยได้เพิ่มฟังก์ชันการทำงานต่าง ๆ Buterin ทำให้อีเธอเรียมแตกต่างไปจากบิตคอยน์โดยการเพิ่มฟังก์ชันอื่นที่ไม่เหมือนใคร ซึ่งช่วยให้ผู้ใช้สามารถบันทึกทรัพย์สินต่าง ๆ เช่น สโลแกน ตอนนี้อีเธอเรียมยังสามารถเป็นแพลตฟอร์มสำหรับการพัฒนาแอปพลิเคชันแบบกระจายศูนย์แทนที่จะเป็นเพียงสกุลเงินดิจิทัล สิ่งนี้พิสูจน์แล้วว่าเป็นก้าวสำคัญในประวัติศาสตร์ของเทคโนโลยีบล็อกเชน อีเธอเรียม เปิดตัวอย่างเป็นทางการในปีพ.ศ. 2558 และตั้งแต่นั้นเป็นต้นมาก็กลายเป็นหนึ่งในแอปพลิเคชันที่ใหญ่ที่สุดในเทคโนโลยีบล็อกเชนที่สามารถอ้างความสามารถในการจัดการธุรกรรมจำนวนมากที่สุดในหนึ่งวัน เนื่องจากความสามารถในการรองรับทั้งแอปพลิเคชันที่กระจายศูนย์และสัญญาอัจฉริยะ

2.1.1.4 ยุคบล็อกเชน 3.0 หรือยุคแอปพลิเคชัน (2561 – อนาคต)

ในช่วงไม่กี่ปีที่ผ่านมามีการดำเนินการหลายอย่างที่เกี่ยวกับเทคโนโลยีบล็อกเชน มีโครงการใหม่ ๆ เกิดขึ้นมากมายโดยมีวัตถุประสงค์เพื่อใช้ประโยชน์จากเทคโนโลยีนี้ นีโอ (NEO) เป็นแพลตฟอร์มโอเพ่นซอร์สแบบกระจายศูนย์ตัวแรกที่เปิดตัวในประเทศจีน ประเทศจีนได้ปิดกั้นสกุลเงินดิจิทัลแต่ก็ยังลงทุนอย่างแข็งขันในการพัฒนาเทคโนโลยีบล็อกเชน นีโอได้รับการขนานนามว่าเป็นอีเธอเรียมของจีน นักพัฒนาบางคนใช้เทคโนโลยีบล็อกเชนเพื่อช่วยในการพัฒนาอินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things - IoT) โดยสิ่งนี้นำไปสู่การเปิดตัวโปรแกรมประยุกต์ด้วยอินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things Application - IoTA) ซึ่งเป็นแพลตฟอร์มสกุลเงินดิจิทัลที่ออกแบบมาเป็นพิเศษสำหรับระบบนิเวศของอินเทอร์เน็ตทุกสรรพสิ่ง ไม่มีค่าธรรมเนียมการทำธุรกรรมและใช้กระบวนการเฉพาะสำหรับการตรวจสอบ แพลตฟอร์มบล็อกเชนรุ่นที่สองอย่าง Monero Zcash และ Dash ได้ช่วยแก้ไขปัญหาด้านความปลอดภัยและความสามารถในการปรับขนาดที่สำคัญในแอปพลิเคชันบล็อกเชนรุ่นเก่า เนื่องจากเทคโนโลยีบล็อกเชนได้พัฒนาไปตามกาลเวลา จึงเปลี่ยนจากเครือข่ายสาธารณะเป็นเครือข่ายส่วนตัว หลายบริษัทเริ่มนำเทคโนโลยีบล็อกเชนมาใช้เพื่อเพิ่มประสิทธิภาพที่ดีขึ้น

รูปที่ 2.1 วิวัฒนาการของเทคโนโลยีบล็อกเชน

ที่มา: Lin et al., 2022

2.1.2 ประเภทของบล็อกเชน

บล็อกเชนสามารถแบ่งออกได้เป็น 4 ประเภท (GeekforGeeks, 2024, p.1) ดังรูปที่ 2.2 โดยพิจารณาจากเข้าร่วมในเครือข่าย โดยมีรายละเอียดดังนี้

รูปที่ 2.2 ประเภทของบล็อกเชน

ที่มา: Techskill Brew, 2022

2.1.2.1 บล็อกเชนแบบเปิดสาธารณะ (Public Blockchain)

หรือรู้จักกันในอีกชื่อ คือ บล็อกเชนแบบไม่จำเป็นต้องขออนุญาตเข้าเครือข่าย (Permissionless Blockchain) คือ บล็อกเชนสาธารณะที่ระบบโครงข่ายเปิดเสรีที่ใครต้องการเชื่อมต่อก็สามารถทำได้เพื่อทำธุรกรรมหรือดูธุรกรรมต่าง ๆ ที่เคยเกิดขึ้นบนโครงข่ายบล็อกเชนแบบเปิดสาธารณะที่เชื่อมต่ออยู่ได้อย่างอิสระ โดยไม่จำเป็นต้องขออนุญาต โดยทุกคนในเครือข่ายสามารถเห็นข้อมูลรายการธุรกรรมได้ ซึ่งรายการธุรกรรมที่เกิดขึ้นใหม่จะต้องผ่านกระบวนการทำฉันทามติ (Consensus) จากสมาชิกในเครือข่ายเสียก่อน ตัวอย่างของบล็อกเชนประเภทนี้ ได้แก่ บิตคอยน์ (Bitcoin) และ อีเธอเรียม (Ethereum) เป็นต้น สำหรับในประเทศไทยบล็อกเชนประเภทนี้ได้แก่ เอ็กซ์เชน (xCHAIN) และ เรอิเชน (REI Chin) เป็นต้น

ตารางที่ 2.1 ข้อดีข้อเสียของบล็อกเชนแบบเปิดสาธารณะ

ข้อดี	ข้อเสีย
1. เชื่อถือได้ (Trustable) มีอัลกอลิทึมในการตรวจจับว่าไม่มีการฉ้อโกง ผู้เข้าร่วมไม่จำเป็นต้องกังวลเกี่ยวกับโหนดอื่น ๆ ในเครือข่าย	1. การประมวลผล (Processing) อัตราของการดำเนินธุรกรรมช้ามาก เนื่องจากมีขนาดใหญ่ การยืนยันแต่ละโหนดเป็นกระบวนการที่ใช้เวลานาน
2. ปลอดภัย (Secure) บล็อกเชนนี้มีขนาดใหญ่เมื่อเปิดให้ประชาชนทั่วไป มีการกระจายข้อมูลได้มากขึ้น	2. การใช้พลังงาน (Energy Consumption) การพิสูจน์การทำงานใช้พลังงานสูง ต้องใช้เครื่องคอมพิวเตอร์ที่ดีในการเข้าร่วมในเครือข่าย
3. ลักษณะนิรนาม (Anonymous Nature) เป็นแพลตฟอร์มที่ปลอดภัยในการทำธุรกรรมอย่างถูกต้อง ในขณะเดียวกันไม่จำเป็นต้องเปิดเผยชื่อและตัวตนเพื่อเข้าร่วม	3. การยอมรับ (Acceptance) ไม่มีหน่วยงานกลาง ดังนั้นรัฐบาลจึงประสบปัญหาในการใช้เทคโนโลยีเร็วขึ้น
4. การกระจายศูนย์ (Decentralized) ไม่มีแพลตฟอร์มเดียวที่ดูแลเครือข่าย แต่ผู้ใช้ทุกคนมีสำเนาของบัญชีแยกประเภท	

ที่มา: GeeksforGeek, 2024

2.1.2.2 บล็อกเชนแบบปิด (Private Blockchain)

คือ บล็อกเชนส่วนตัวที่ใช้ภายในองค์กรหรือบริษัทที่ร่วมด้วยเท่านั้น ทำให้คนในองค์กรหรือผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถทำธุรกรรมต่าง ๆ ในระบบบล็อกเชนได้ โดยข้อมูลหรือประวัติการทำธุรกรรมต่าง ๆ ที่เกิดขึ้นก็จะถูกจำกัดอยู่เฉพาะภายในเครือข่าย ซึ่งมีแต่สมาชิกที่ได้รับอนุญาตเท่านั้นจะสามารถเข้าถึงข้อมูลได้ ดังนั้นบล็อกเชนแบบปิดจึงเหมาะกับองค์กรหรือบริษัทที่ต้องการรักษาความปลอดภัยข้อมูลในระดับสูง ตัวอย่างของบล็อกเชนประเภทนี้ได้แก่ Hyperledger, Corda และ Tendermint เป็นต้น

ตารางที่ 2.2 ข้อดีข้อเสียของบล็อกเชนแบบปิด

ข้อดี	ข้อเสีย
1. ความเร็ว (Speed) อัตราการทำธุรกรรมสูง เนื่องจากมีขนาดเล็ก การยืนยันแต่ละโหนดใช้เวลาน้อยลง	1. ความปลอดภัย (Security) จำนวนโหนดประเภทนี้มีจำกัด ดังนั้นโอกาสในการจัดการจึงมีอยู่ บล็อกเชนเหล่านี้มีความเสี่ยงมากกว่า
2. การปรับขนาด (Scalability) สามารถปรับเปลี่ยนความสามารถในการปรับขนาดได้ ขนาดของเครือข่ายสามารถตัดสินใจได้ด้วยตนเอง	2. การรวมศูนย์ (Centralized) การสร้างความน่าเชื่อถือเป็นหนึ่งในข้อเสียหลักเนื่องจากมีลักษณะเป็นศูนย์กลาง องค์กรสามารถใช้สิ่งนี้เพื่อการทุจริตได้
3. ความเป็นส่วนตัว (Privacy) เพิ่มระดับความเป็นส่วนตัวด้วยเหตุผลด้านการรักษาความลับตามที่ธุรกิจต้องการ	3. การนับ (Count) เนื่องจากมีโหนดน้อย หากโหนดออฟไลน์ ระบบบล็อกเชนทั้งหมดอาจได้รับอันตราย
4. สมดุล (Balanced) มีความสมดุลมากขึ้นเนื่องจากมีเพียงผู้ใช้บางรายเท่านั้นที่สามารถเข้าถึงธุรกรรมซึ่งช่วยปรับปรุงประสิทธิภาพของเครือข่าย	

ที่มา: GeeksforGeek, 2024

2.1.2.3 บล็อกเชนแบบเฉพาะกลุ่ม (Consortium Blockchain)

คือ บล็อกเชนประเภทนี้จะเป็นลักษณะการรวมบล็อกเชนแบบเปิดสาธารณะกับบล็อกเชนแบบปิดเข้าด้วยกัน โดยผู้ที่สามารถเชื่อมต่อหรือทำธุรกรรมได้ต้องอยู่ในกลุ่มเครือข่ายที่เกี่ยวข้องหรือผู้ที่ได้รับอนุญาตเท่านั้น โดยข้อมูลต่าง ๆ หรือธุรกรรมที่เคยเกิดขึ้นก็จะอยู่

ในกลุ่มตัวเองท่านั้น โดยปกติแล้วบล็อกเชนแบบเฉพาะกลุ่มจะถูกใช้โดยองค์กรต่าง ๆ ที่มีลักษณะธุรกิจเหมือนกันต้องการจะแลกเปลี่ยนข้อมูลกัน เพื่อผลประโยชน์ต่าง ๆ ขององค์กรเอง เช่น การแลกเปลี่ยนข้อมูลการทำธุรกรรมต่าง ๆ หรือแลกเปลี่ยนสินทรัพย์ภายในกลุ่มของธนาคาร เป็นต้น

ตารางที่ 2.3 ข้อดีข้อเสียของบล็อกเชนแบบเฉพาะกลุ่ม

ข้อดี	ข้อเสีย
1.ความเร็ว (Speed) ผู้ใช้จำนวนจำกัดทำให้การยืนยันรวดเร็ว ความเร็วสูงทำให้ใช้งานได้มากขึ้นสำหรับองค์กร	1. การอนุมัติ (Approval) สมาชิกทุกคนเห็นด้วยกับที่ว่าโพรโทตอลทำให้มีความยืดหยุ่นน้อยลงเนื่องจากมีองค์กรที่เกี่ยวข้องตั้งแต่หนึ่งองค์กรขึ้นไป วิสัยทัศน์ที่น่าสนใจมีความแตกต่างกัน
2.อำนาจ (Authority) หลายองค์กรสามารถมีส่วนร่วมและทำให้กระจายศูนย์ในทุกระดับการกระจายศูนย์ทำให้มีความปลอดภัยมากขึ้น	2. ความโปร่งใส (Transparency) สามารถโจมตีได้หากองค์กรเสียหาย องค์กรอาจซ่อนข้อมูลจากผู้ใช้ได้
3.ความเป็นส่วนตัว (Privacy) ข้อมูลของบล็อกที่ถูกตรวจสอบไม่เป็นที่รู้จักในมุมสาธารณะ แต่สมาชิกที่อยู่ในบล็อกเชนสามารถเข้าถึงได้	3. ช่องโหว่ (Vulnerability) หากมีบางโหนดถูกบุกรุก มีโอกาสเกิดช่องโหว่ในบล็อกเชนนี้มากขึ้น
4.ความยืดหยุ่น (Flexible) ความยืดหยุ่นของบล็อกเชนมีความหลากหลายมาก เนื่องจากเป็นการตัดสินใจที่ไม่ใหญ่มากสามารถดำเนินการได้เร็วขึ้น	

ที่มา: GeeksforGeek, 2024

2.1.2.4 บล็อกเชนแบบไฮบริด (Hybrid Blockchain)

คือ บล็อกเชนที่รวมองค์ประกอบต่าง ๆ จากทั้งเครือข่ายบล็อกเชนแบบปิดและแบบเปิดสาธารณะ บริษัทต่าง ๆ สามารถตั้งค่าระบบแบบปิดที่ใช้สิทธิ์การได้รับอนุญาตควบคู่ไปกับระบบแบบเปิดได้ ด้วยวิธีนี้พวกเขาจึงควบคุมการเข้าถึงข้อมูลเฉพาะที่จัดเก็บไว้ในบล็อกเชนได้ ในขณะที่ยังคงให้สาธารณะสามารถเข้าถึงข้อมูลที่เหลือได้ โดยพวกเขาใช้สัญญาอัจฉริยะเพื่อให้สมาชิกสาธารณะตรวจสอบว่าธุรกรรมส่วนตัวเสร็จสมบูรณ์แล้วหรือไม่ ตัวอย่างเช่น บล็อกเชนแบบไฮบริดสามารถใช้สิทธิ์ในการเข้าถึงสกุลเงินดิจิทัลแก่สาธารณะได้ในขณะที่ยังคงควบคุมสกุลเงินที่

ธนาคารเป็นเจ้าของให้เป็นส่วนตัวได้

ตารางที่ 2.4 ข้อดีข้อเสียของบล็อกเชนแบบไฮบริด

ข้อดี	ข้อเสีย
1. ระบบนิเวศ (Ecosystem) สิ่งที่ได้เปรียบที่สุดเกี่ยวกับบล็อกเชนนี้คือธรรมชาติแบบผสมผสาน ไม่สามารถโจมดีได้เนื่องจากมีผู้ใช้ถึง 51% ไม่สามารถเข้าถึงเครือข่ายได้	1. ประสิทธิภาพ (Efficiency) ไม่ใช่ทุกคนที่อยู่ในฐานะที่จะใช้บล็อกเชนแบบไฮบริดได้ องค์กรยังประสบปัญหาบางประการในแง่ของประสิทธิภาพในการบำรุงรักษาระบบ
2. ค่าใช้จ่าย (Cost) การทำธุรกรรมมีราคาถูกเนื่องจากมีเพียงไม่กี่โหนดเท่านั้นที่ตรวจสอบการทำธุรกรรม โหนดทั้งหมดไม่มีการตรวจสอบดังนั้นค่าใช้จ่ายในการคำนวณจึงน้อยลง	2. ความโปร่งใส (Transparency) มีความเป็นไปได้ที่บางคนสามารถซ่อนข้อมูลจากผู้ใช้ได้ หากมีคนต้องการเข้าถึงบล็อกเชนแบบไฮบริดนั้นขึ้นอยู่กับองค์กรว่าจะให้สิทธิ์หรือไม่
3. สถาปัตยกรรม (Architecture) สามารถปรับแต่งได้สูงและยังคงไว้ซึ่งความสมบูรณ์ ปลอดภัย และโปร่งใส	3. ระบบนิเวศ (Ecosystem) เนื่องจากเป็นระบบนิเวศแบบปิด บล็อกเชนนี้จึงขาดสิ่งจูงใจสำหรับการมีส่วนร่วมของเครือข่าย
4. การดำเนินการ (Operation) สามารถเลือกผู้เข้าร่วมในบล็อกเชน และตัดสินใจว่าธุรกรรมใดที่สามารถเปิดเผยต่อสาธารณะได้	

ที่มา: GeeksforGeek, 2024

มหาวิทยาลัยรังสิต Rangsit University

2.1.3 คุณลักษณะที่สำคัญของเทคโนโลยีบล็อกเชน

บล็อกเชนมีคุณลักษณะการเป็นเทคโนโลยีที่มีวัตถุประสงค์ทั่วไป (General Purpose Technology) เนื่องจากสามารถนำไปประยุกต์ใช้กับรูปแบบธุรกิจได้หลากหลาย มีการพัฒนาของเทคโนโลยีอย่างต่อเนื่องและสามารถสร้างนวัตกรรมต่อยอดรูปแบบธุรกิจเดิมได้มากมายเช่นกัน บล็อกเชนจึงได้เติบโตและได้รับความนิยม นอกจากนี้มีโอกาสที่สร้างประโยชน์แก่ระบบเศรษฐกิจรวมถึงการเปลี่ยนแปลงต่อสังคม เทคโนโลยีบล็อกเชนมีคุณลักษณะที่สำคัญ 5 ประการ (ธนาคารแห่งประเทศไทย, 2564, น. 7) ดังนี้

2.1.3.1 ฐานข้อมูลแบบกระจายศูนย์ (Distributed Database) โดยสมาชิกในเครือข่าย

บล็อกเชนจะมีข้อมูลชุดเดียวกัน โดยอาศัยกระบวนการฉันทามติ

2.1.3.2 การสื่อสารระหว่างกันโดยตรงระหว่างสมาชิก (Peer-to-Peer Transmission) โดยสมาชิกในเครือข่ายบล็อกเชนจะแลกเปลี่ยนข้อมูลกันโดยตรงด้วยรูปแบบการแลกเปลี่ยนข้อมูล (Protocol)

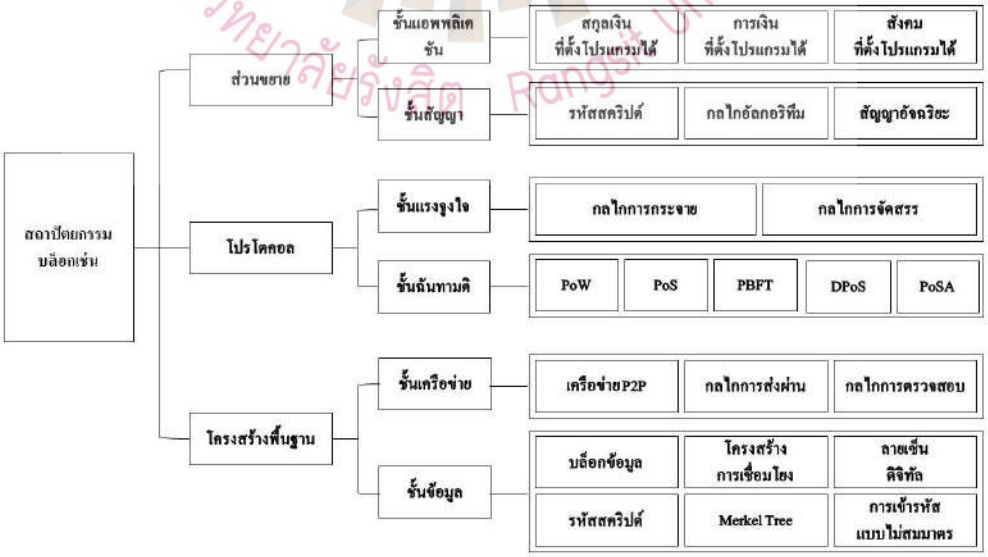
2.1.3.3 ข้อมูลธุรกรรมมีความโปร่งใส (Transparency) โดยสมาชิกในเครือข่ายบล็อกเชนจะสามารถเข้าถึงข้อมูลชุดเดียวกันจากโหนดใด ๆ ได้ ซึ่งยากต่อการปลอมแปลงข้อมูล

2.1.3.4 ข้อมูลย้อนกลับไปแก้ไขไม่ได้ (Immutability) โดยชุดข้อมูลในแต่ละบล็อกจะมีการระบุค่าทางคณิตศาสตร์ (Hash) ของบล็อกก่อนหน้าเชื่อมโยงกัน ทำให้การแก้ไขข้อมูลในบล็อกใด ๆ จะส่งผลกระทบต่อข้อมูลของบล็อกที่เชื่อมโยงในภายหลังตลอดทั้งชุดข้อมูล

2.1.3.5 สามารถตั้งโปรแกรมให้ทวนสอบอัตโนมัติ (Computational Logic) โดยนักพัฒนาระบบสามารถเขียนโปรแกรมเพื่อเพิ่มข้อมูลในระบบบล็อกเชน เช่น สัญญาอัจฉริยะ ซึ่งข้อมูลในบล็อกเชนจะดำเนินการตามเงื่อนไขที่กำหนดไว้ในโปรแกรม

2.1.4 โครงสร้างพื้นฐานของบล็อกเชน (Infrastructure of Blockchain)

ตามหน้าที่หลักของโครงสร้างพื้นฐานของบล็อกเชน สามารถแบ่งออกเป็น 3 ส่วนหลักที่สร้างให้เกิดสถาปัตยกรรม จากล่างขึ้นบน: โครงสร้างพื้นฐาน โปรโตคอล และส่วนขยาย ดังแสดงในรูปที่ 2.3 โดยมีรายละเอียดดังนี้



รูปที่ 2.3 โครงสร้างพื้นฐานของบล็อกเชน

ที่มา: Lin et al., 2022

2.1.4.1 ส่วนโครงสร้างพื้นฐาน (Infrastructure)

ส่วนโครงสร้างพื้นฐานประกอบด้วยชั้นข้อมูล (Data Layer) และชั้นเครือข่าย (Network Layer)

1) ชั้นข้อมูล (Data Layer)

ชั้นข้อมูลเป็นโครงสร้างข้อมูลระดับต่ำสุดของเทคโนโลยีบล็อกเชนทั้งหมด โดยประกอบด้วย โครงสร้างของเชน (Chain Structure / Linked Structure) ของบล็อกข้อมูล (Data Block) พื้นฐาน ตลอดจนเทคโนโลยีที่เกี่ยวข้อง เช่น ลายเซ็นดิจิทัล (Digital Signature) กุญแจส่วนตัวสาธารณะแบบอสมมาตรการเข้ารหัสข้อมูล (Asymmetric Encryption) และการประทับเวลา (Time Stamp) นอกจากนี้หน้าที่หลักคือการจัดเก็บข้อมูลและบัญชีตามหลัก Merkle tree เช่นเดียวกับการใช้งานและความปลอดภัยของการทำธุรกรรม

2) ชั้นเครือข่าย (Network Layer)

สาระสำคัญของบล็อกเชนคือเครือข่ายแบบเพียร์ทูเพียร์ (Peer-to-Peer Network) ที่เป็นโหนดรักษาการสื่อสาร โดยการบำรุงรักษาบล็อกเชนทั่วไป อย่างไรก็ตามจุดประสงค์หลักของชั้นเครือข่ายคือ การบรรลุปฏิสัมพันธ์ของข้อมูลระหว่างโหนดในเครือข่ายบล็อกเชน ซึ่งรวมถึงกลไกเครือข่ายแบบเพียร์ทูเพียร์ (P2P) กลไลการส่งผ่านข้อมูล (Transmission Mechanism) และกลไกการตรวจสอบข้อมูล (Verification Mechanism)

2.1.4.2 ส่วนโพรโทตอล (Protocol)

ส่วนโพรโทคอลประกอบด้วยชั้นฉันทามติ (Consensus Layer) และชั้นสิ่งจูงใจ (Incentive Layer)

1) ชั้นฉันทามติ (Consensus Layer)

ฉันทามติเป็นพื้นฐานและเป็นหนึ่งในเทคโนโลยีหลักของบล็อกเชนและกลไกธรรมาภิบาลของชุมชนบล็อกเชนที่จะทำให้โหนดที่มีการกระจายสูง สามารถเข้าถึงฉันทามติในเครือข่ายบล็อกเชนแบบกระจายผ่านกลไกฉันทามติ ตัวอย่างเช่น PoW, pBFT, PoS, DPoS, PoB, PoC, PoET, PoA, PoSA ซึ่งกลไกฉันทามติเหล่านี้จะได้กล่าวในส่วนถัดไป

2) ชั้นสิ่งจูงใจ (Incentive Layer)

ชั้นสิ่งจูงใจส่วนใหญ่ ประกอบด้วย กลไกการจัดสรร (Allocation

Mechanism) และกลไกการกระจาย (Distribution Mechanism) ของสิ่งจูงใจทางศรษฐกิจ ฟังก์ชันของมันคือการจัดให้มีมาตรการจูงใจ ซึ่งกระตุ้นให้โหนดที่จะเข้าร่วมในการตรวจสอบความปลอดภัยของบล็อกเชน เพื่อให้แน่ใจว่าการทำงานที่ปลอดภัยของเครือข่ายทั้งหมดและส่วนใหญ่ใช้บล็อกเชนแบบเปิดสาธารณะ

2.1.4.3 ส่วนขยาย (Expansion)

ส่วนขยายประกอบด้วยชั้นสัญญา (Contract Layer) และชั้นแอปพลิเคชัน (Application Layer) ซึ่งส่วนใหญ่ให้บริการที่หลากหลาย เข้าถึงได้โดยเรียกส่วนประกอบการทำงานของส่วนโปรโตคอล

1) ชั้นสัญญา (Contract Layer)

ชั้นสัญญาจะห่อหุ้มสคริปต์ทุกชนิด (Script Code) กลไกอัลกอริทึม (Algorithmic Mechanism) และสัญญาอัจฉริยะ (Smart Contract) ซึ่งเป็นพื้นฐานของคุณลักษณะที่ตั้งโปรแกรมได้ของบล็อกเชน ยิ่งไปกว่านั้นสัญญาอัจฉริยะคือชุดคำสั่งโปรแกรมบางส่วนที่ประมวลผลบนบล็อกเชนที่สามารถดำเนินการได้โดยอัตโนมัติโดยไม่มีการแทรกแซง ส่วนใหญ่ใช้การพัฒนาด้วยอัลกอริทึมและตรรกะที่กำหนดขึ้นเอง

2) ชั้นแอปพลิเคชัน (Application Layer)

อย่างที่เราทราบกันดีว่าบล็อกเชนจะอยู่ที่ชั้นแอปพลิเคชัน เป็นชั้นที่สรุปสถานการณ์การใช้งานและกรณีต่าง ๆ ของบล็อกเชน เช่น สกุลเงิน (Programmable Currency) การเงิน (Programmable Finance) และสังคมที่ตั้งโปรแกรมได้ (Programmable Society) เนื้อหาหลักของธุรกรรมรวมถึงการก่อตัวของบล็อกเชนโดยการซื้อขายแพ็คเกจของนักขุดและการตรวจสอบบล็อกที่ขุดได้จากการขุดและการออกอากาศของนักขุด เพื่อความปลอดภัยและความสมบูรณ์ของการทำธุรกรรมในระบบการสร้างที่อยู่ การทำธุรกรรมยังใช้การเข้ารหัสทางคณิตศาสตร์หลากหลาย

2.1.5 แฮชบล็อกเชน (Blockchain Hash) (Parrots, 2024, p.1)

โลกแห่งการตรวจสอบและการจัดเก็บข้อมูลกำลังเติบโตอย่างรวดเร็วอย่างที่ไม่เคยมีมาก่อน โดยได้รับแรงหนุนจากความต้องการเกี่ยวกับวิธีที่มีประสิทธิภาพ ปลอดภัย และเชื่อถือได้มากขึ้นในการจัดเก็บ การประมวลผลและการตรวจสอบปริมาณข้อมูลที่เพิ่มขึ้นเรื่อย ๆ แอปพลิเคชันและโซลูชันที่ใช้เทคโนโลยีบล็อกเชนยังคงได้รับแรงผลักดันเนื่องจากเทคโนโลยีบล็อกเชนอยู่ใน

ระดับแนวหน้าของการปฏิวัติครั้งนี้ โดยนำเสนอวิธีใหม่ในการจัดการความสมบูรณ์และความน่าเชื่อถือของข้อมูล ในขณะที่ฐานข้อมูลที่เป็นกรรมสิทธิ์อื่น ๆ ก็ได้รับการพัฒนาและเปิดตัวสู่สาธารณะทุกวัน การพัฒนาฐานข้อมูลที่เป็นกรรมสิทธิ์อื่น ๆ บ่งชี้ถึงเส้นทางคู่ขนานของนวัตกรรมที่ตอบสนองความต้องการข้อมูลเฉพาะและข้อมูลเฉพาะทาง เราทุกคนเคยได้ยินเกี่ยวกับรหัสแฮชและความสำคัญในวิทยาการคอมพิวเตอร์ ซึ่งบทบาทของรหัสแฮชบนแพลตฟอร์มเหล่านี้บ่งบอกถึงส่วนสำคัญในการเล่าเรื่องที่กว้างขึ้นเกี่ยวกับวิทยาศาสตร์ข้อมูลและความปลอดภัยทางไซเบอร์

รหัสแฮช (Hash Code) คือ ลายนิ้วมือดิจิทัลของชุดข้อมูลอินพุต โดยรหัสจะใช้เพื่อตรวจสอบหรือระบุความสมบูรณ์และความถูกต้องของข้อมูลต้นฉบับในอนาคต ค่าแฮชมักจะถูกสร้างขึ้นโดยการใช้ฟังก์ชันแฮชกับชุดข้อมูล รหัสแฮชมีบทบาทสำคัญในด้านต่าง ๆ เช่น การรักษาความปลอดภัยของข้อมูล การเข้ารหัส การจัดการข้อมูลและการจัดการในทางการใช้งานทางเทคโนโลยีต่าง ๆ

แฮชเป็นฟังก์ชันทางคณิตศาสตร์ที่แปลงอินพุตที่มีความยาวตามใจชอบให้เป็นเอาต์พุตที่เข้ารหัสซึ่งมีความยาวคงที่ ดังนั้นไม่ว่าปริมาณข้อมูลหรือขนาดไฟล์เดิมจะเป็นอย่างไร แฮชเฉพาะของมันจะมีขนาดเท่ากันเสมอ นอกจากนี้แฮชไม่สามารถใช้เพื่อ “วิศวกรรมย้อนกลับ” อินพุตจากเอาต์พุตที่แฮชได้ เนื่องจากฟังก์ชันแฮชเป็นแบบ “ทางเดียว” อย่างไรก็ตามหากคุณใช้ฟังก์ชันดังกล่าวกับข้อมูลเดียวกัน แฮชของฟังก์ชันนั้นจะเหมือนกัน ดังนั้นคุณจึงสามารถตรวจสอบได้ว่าข้อมูลเหมือนกันหากคุณทราบแฮชของฟังก์ชันนั้นแล้ว

แฮชบล็อกเชน (Blockchain Hash) เป็นแนวคิดหลักในเทคโนโลยีบล็อกเชนโดยใช้ฟังก์ชันแฮชที่เข้ารหัส เพื่อรับรองความสมบูรณ์และความปลอดภัยของเครือข่ายบล็อกเชน สามารถอธิบายถึงบทบาท ลักษณะ และความสำคัญของแฮชในเทคโนโลยีบล็อกเชนได้ดังนี้

1) ฟังก์ชันแฮชที่เข้ารหัสในบล็อกเชน: แฮชบล็อกเชนถูกสร้างขึ้นโดยใช้ฟังก์ชันแฮชที่เข้ารหัส ฟังก์ชันนี้รับข้อมูลอินพุตหรือข้อความใด ๆ (ซึ่งอาจมีขนาดแตกต่างกันไป) และสร้างสตริงอักขระที่มีขนาดคงที่เรียกว่า “แฮช” แฮชนี้เป็นลักษณะเฉพาะของข้อมูลที่ป้อน แม้แต่การเปลี่ยนแปลงเล็กน้อยก็ส่งผลให้เกิดแฮชที่แตกต่างไปจากเดิมอย่างสิ้นเชิง คุณลักษณะสำคัญของฟังก์ชันแฮชเหล่านี้ได้แก่ ความเร็ว (การคำนวณอย่างรวดเร็ว) การกำหนด (เอาต์พุตที่สอดคล้องกัน

สำหรับอินพุตเดียวกัน) ความต้านทานการชนกัน (ความยากในการค้นหาอินพุตที่แตกต่างกันสองตัวที่สร้างเอาต์พุตเดียวกัน) และฟังก์ชันทางเดียว (ความเป็นไปไม่ได้ในการอนุมานอินพุตจากแฮช)

2) การระบุบล็อกที่ไม่ซ้ำกัน: ในบล็อกเชนแต่ละบล็อกประกอบด้วยชุดธุรกรรมหรือข้อมูลอื่น ๆ การใช้ฟังก์ชันแฮชกับข้อมูลนี้จะสร้างค่าแฮชเฉพาะสำหรับบล็อกนั้น แฮชนี้ทำหน้าที่เหมือนลายเซ็นดิจิทัลหรือลายนิ้วมือสำหรับบล็อก โดยสรุปเนื้อหาในลักษณะที่ปลอดภัยและตรวจสอบได้

3) การรักษาความปลอดภัยบล็อกเชนผ่านแฮช: ความปลอดภัยของบล็อกเชนอาศัยแฮชเหล่านี้อย่างมาก แต่ละบล็อกในบล็อกเชนประกอบด้วย แฮชของบล็อกก่อนหน้า ทำให้เกิดเชนของบล็อก การเชื่อมโยงนี้หมายความว่าความพยายามใด ๆ ในการเปลี่ยนแปลงข้อมูลในบล็อกก่อนหน้าไม่เพียงแต่จะเปลี่ยนแฮชของบล็อกนั้นเท่านั้น แต่ยังต้องมีการคำนวณแฮชใหม่สำหรับบล็อกที่ตามมาทั้งหมดอีกด้วย ซึ่งเป็นสิ่งต้องห้ามในการคำนวณ สิ่งนี้ทำให้เกิดบล็อกเชนที่มีความปลอดภัยสูงและป้องกันการงัดแงะ

4) การรักษาความสมบูรณ์ของข้อมูล: การใช้แฮชในบล็อกเชนทำให้มั่นใจในความสมบูรณ์ของข้อมูล เนื่องจากค่าแฮชเปลี่ยนแปลงแม้การเปลี่ยนข้อมูลของบล็อกเพียงเล็กน้อย จึงสามารถตรวจจับการปลอมแปลงได้อย่างง่ายดาย คุณลักษณะนี้จำเป็นสำหรับแอปพลิเคชันที่ความยาวสมบูรณ์ของข้อมูลเป็นสิ่งสำคัญ เช่น ธุรกรรมทางการเงิน สัญญาทางกฎหมาย และการจัดการห่วงโซ่อุปทาน

5) บทบาทในกลไกฉันทามติของบล็อกเชน: ในบล็อกเชนที่ใช้การพิสูจน์ด้วยการทำงาน (Proof of Work – PoW) การสร้างแฮชที่ถูกต้องเป็นส่วนสำคัญในกระบวนการเพิ่มบล็อกใหม่ให้กับเชน นักขุดจะต้องค้นหาแฮชที่ตรงตามเงื่อนไขที่กำหนดไว้ล่วงหน้า ซึ่งโดยทั่วไปเกี่ยวข้องกับแฮชที่น้อยกว่าค่าเป้าหมายเฉพาะ กระบวนการนี้เรียกว่าการขุด ต้องใช้ความพยายามในการคำนวณอย่างมาก เพื่อรักษาความปลอดภัยเครือข่ายจากกิจกรรมฉ้อโกง

6) การอำนวยความสะดวกในการตรวจสอบที่มีประสิทธิภาพ: แฮชเนื่องจากขนาดที่คงที่และค่อนข้างเล็ก ช่วยให้การตรวจสอบบล็อกเชนมีประสิทธิภาพ การตรวจสอบความสมบูรณ์ของบล็อกข้อมูลทั้งหมดสามารถทำได้อย่างมีประสิทธิภาพโดยเพียงแค่ตรวจสอบค่าแฮชของบล็อกแทนที่จะเปรียบเทียบข้อมูลทั้งหมดภายใน

7) การเก็บบันทึกที่ไม่เปลี่ยนรูป: การใช้แฮชในบล็อกเชนช่วยให้การเก็บบันทึกที่ไม่เปลี่ยนรูปเกิดขึ้นได้ เมื่อป้อนข้อมูลลงในบล็อกเชนแล้วจะไม่สามารถเปลี่ยนแปลงได้หากไม่มีการตรวจจับ ทำให้บล็อกเชนเป็นโซลูชันในอุดมคติสำหรับแอปพลิเคชันที่ต้องการบันทึกประวัติที่ไม่สามารถเปลี่ยนแปลงได้

8) ความท้าทายและข้อความพิจารณา: แม้ว่าแฮชบล็อกเชนจะให้ความปลอดภัยที่แข็งแกร่ง แต่เทคโนโลยีก็ไม่ได้ปราศจากความท้าทายความแข็งแกร่งของความปลอดภัยของบล็อกเชน ส่วนหนึ่งขึ้นอยู่กับความแข็งแกร่งของฟังก์ชันแฮชที่ใช้เมื่อพลังการคำนวณเพิ่มขึ้น ฟังก์ชันแฮชบางอย่างอาจมีช่องโหว่ ทำให้จำเป็นต้องปรับปรุงอัลกอริทึมที่ปลอดภัยยิ่งขึ้น

2.1.5.1 แฮชบล็อกเชนทำงานอย่างไร

แฮชบล็อกเชนใช้เพื่อตรวจสอบว่าข้อมูลในเอกสารหรือข้อความถูกแทรกแซงหรือไม่ แฮชบล็อกเชนถูกสร้างขึ้นเมื่อมีการเพิ่มบล็อกข้อมูลใหม่ลงในเชน ข้อมูลที่อยู่ในบล็อกจะถูกแฮช จากนั้นค่าแฮชจะถูกเพิ่มเข้าไปที่ส่วนท้ายของเชน เมื่อใดก็ตามที่ข้อมูลที่อยู่ในบล็อกมีการเปลี่ยนแปลงหรือเปลี่ยนแปลงในทางใดทางหนึ่ง ค่าแฮชก็จะเปลี่ยนไปเช่นกัน หากค่าแฮชไม่ตรงกับข้อมูลต้นฉบับ แสดงว่าข้อมูลถูกแก้ไข หากค่าแฮชตรงกับข้อมูลต้นฉบับ จะได้รับการยืนยันว่าข้อมูลไม่มีการเปลี่ยนแปลงหรือแก้ไข บล็อกเชนคือกลุ่มของบล็อกข้อมูลที่ได้รับการยืนยันและเชื่อมโยงเข้าด้วยกันตามลำดับเวลาโดยใช้ค่าแฮชแต่ละบล็อกจะคล้ายกับหน้าในหนังสือ และแต่ละหน้าจะได้รับการตรวจสอบโดยใช้ค่าแฮช

2.1.5.2 ประเภทของแฮชบล็อกเชน

มีอัลกอริทึมการแฮชที่แตกต่างกันมากมายที่ใช้ในการสร้างค่าแฮช นี่คือตัวอย่างบางส่วนของแฮชและวิธีการนำไปใช้ในเทคโนโลยีบล็อกเชน

1) SHA-256:

คำอธิบาย: SHA-256 ซึ่งย่อมาจาก Secure Hash Algorithm 256-bit หรืออัลกอริทึมแฮชที่ปลอดภัย 256 บิต เป็นฟังก์ชันแฮชการเข้ารหัสที่ใช้กันอย่างแพร่หลาย เป็นฟังก์ชันแฮชที่ใช้ในการตรวจสอบความถูกต้องของไฟล์และป้องกันการปลอมแปลง ได้รับการออกแบบในปีพ.ศ. 2540 โดยสำนักงานความมั่นคงแห่งชาติ (the National Security Agency – NSA)

การใช้ในบล็อกเชน: ในเทคโนโลยีบล็อกเชน SHA-156 ใช้เพื่อรับรองความสมบูรณ์ของข้อมูลเป็นหลัก จะตรวจสอบว่าข้อมูลภายในบล็อกเชนมีการเปลี่ยนแปลงหรือไม่ อัลกอริทึมนี้มีความสำคัญอย่างยิ่งในกระบวนการขุดสกุลเงินดิจิทัล เช่น บิตคอยน์ ซึ่งใช้ในการแฮชข้อมูลของบล็อกเพื่อสร้างหลักฐานการทำงาน SHA-256 ยังเป็นเครื่องมือในการสร้างคู่กุญแจส่วนตัวและกุญแจสาธารณะ ซึ่งจำเป็นสำหรับการักษาความปลอดภัยธุรกรรมบนบล็อกเชน ปัจจุบัน

นิยมใช้ในอุตสาหกรรมและภาคส่วนต่าง ๆ รวมถึงการเงินและการดูแลสุขภาพ

2) MD5:

คำอธิบาย: MD5 ย่อมาจาก Message Digest Algorithm 5 หรืออัลกอริทึมการแยกข้อความ5 สร้างค่าแฮช 128 บิต ซึ่งโดยทั่วไปจะแสดงเป็นเลขฐานสิบหก 32 อักขระ

การใช้ในบล็อกเชนและข้อจำกัด: ใช้สำหรับตรวจสอบความสมบูรณ์ของไฟล์หรือชุดข้อมูล ซึ่งมักจะทำหน้าที่เป็นผลรวมตรวจสอบเพื่อรับรองความสมบูรณ์ของข้อมูล ในบริบทของบล็อกเชน สามารถใช้ MD5 กับแอปพลิเคชันที่มีความสำคัญด้านความปลอดภัยน้อยกว่าได้ อย่างไรก็ตาม MD5 ไม่ถือว่าปลอดภัยจากการชนกันของแฮชอีกต่อไป ทำให้ไม่เหมาะสมสำหรับแอปพลิเคชันที่ต้องการความปลอดภัยสูง

3) RIPEMD-160:

คำอธิบาย: RIPEMD-160 ย่อมาจาก RACE Integrity Primitives Evaluation Message Digest 160 bit) RIPEMD-160 สร้างค่าแฮช 160 บิต ซึ่งสั้นกว่า SHA-256

การใช้ในบล็อกเชน: ใช้ในบล็อกเชนเพื่อวัตถุประสงค์ที่คล้ายกันเช่นเดียวกับ SHA-256 เช่น การตรวจสอบความสมบูรณ์ของข้อมูลในบล็อก และในการสร้างคู่กุญแจส่วนตัวและกุญแจสาธารณะ RIPMED-160 ได้รับการกล่าวถึงเป็นพิเศษสำหรับการใช้งานในบิตคอยน์เพื่อสร้างที่อยู่กระเป๋าเงิน

4) CRC32:

คำอธิบาย: CRC32 ย่อมาจาก Cyclic Redundancy Check 32 bit และโดยหลักแล้วเป็นชุดคำสั่งตรวจจับข้อผิดพลาด แทนที่จะเป็นฟังก์ชันแฮชการเข้ารหัส

การใช้ในบล็อกเชน: มักใช้เพื่อตรวจจับการเปลี่ยนแปลงข้อมูลโดยไม่ตั้งใจในแอปพลิเคชันบล็อกเชนหรือที่จัดเก็บข้อมูลบางตัว สามารถใช้ CRC32 สำหรับการตรวจสอบความสมบูรณ์ของไฟล์ขั้นพื้นฐานได้ เนื่องจาก CRC32 จะสร้างเอาต์พุตเดียวกันสำหรับอินพุตเดียวกันอย่างสม่ำเสมอ อย่างไรก็ตามอรรถประโยชน์ในบล็อกเชนนั้นมีจำกัดเนื่องจากขาดคุณสมบัติความปลอดภัยในการเข้ารหัส

5) Tiger Algorithm:

คำอธิบาย: Tiger Algorithm ขึ้นชื่อในด้านความเร็วและประสิทธิภาพโดย เฉพาะบนแพลตฟอร์ม 64 บิต มันสร้างแฮช 192 บิตและมีเวอร์ชันที่เรียกว่า Tiger2 ซึ่งนำเสนอคุณสมบัติแบบไดนามิกมากขึ้น

การออกแบบและฟังก์ชันการทำงาน: พัฒนาขึ้นจากโครงสร้าง Merkle-Damgard โดย Wiger ดำเนินการโดยใช้คำ 64 บิตและรวมชุด 24 รอบที่เกี่ยวข้องกับการ

ดำเนินการต่าง ๆ เช่น XOR การบวก/การลบ การหมุน และการค้นหา S-box อัลกอริทึมยังมีกลไกการตั้งเวลากุญแจที่ซับซ้อนอีกด้วย แม้ว่าจะไม่ได้ใช้กันทั่วไปเหมือนกับ SHA-256 ในบล็อกเชน แต่ Tiger ก็เหมาะสมอย่างยิ่งสำหรับระบบสมัยใหม่ที่ต้องการความสามารถในการแฮชที่รวดเร็วและมีประสิทธิภาพ

6) SHA-1:

คำอธิบาย: SHA-1 หรือ Secure Hash Algorithm 1 เป็นฟังก์ชันแฮชสำหรับการเข้ารหัสที่สร้างค่าแฮช 160 บิต (20 ไบต์) มีการใช้กันอย่างแพร่หลายในการรักษาความปลอดภัยแอปพลิเคชันลายเซ็นดิจิทัล และในใบรับรอง SSL/TLS อย่างไรก็ตามขณะนี้ SHA-1 ถือว่าไม่ปลอดภัยต่อผู้โจมตีที่ได้รับทุนสนับสนุนเพียงพอ เนื่องจากมีความเสี่ยงต่อการโจมตีแบบชนกัน (อินพุตสองรายการที่สร้างแฮชเดียวกัน)

การใช้ในบล็อกเชน: การใช้ SHA-1 ในเทคโนโลยีบล็อกเชนสมัยใหม่ไม่สนับสนุนเนื่องจากช่องโหว่ด้านความปลอดภัย บล็อกเชนต้องการฟังก์ชันแฮชที่แข็งแกร่งเพื่อรับรองความสมบูรณ์และความปลอดภัยของข้อมูล และความไวต่อการโจมตีการชนกันของ SHA-1 ทำให้ไม่เหมาะสม มีทางเลือกที่ปลอดภัยกว่าเช่น SHA-256 หรือ SHA-3 เป็นที่ต้องการในแอปพลิเคชันบล็อกเชน

7) SHA-3:

คำอธิบาย: SAH-3 ย่อมาจาก Secure Hash Algorithm 3 เป็นสมาชิกล่าสุดของตระกูล Secure Hash Algorithm ต่างจาก SHA-1 และ SHA-2 ตรงที่ SHA-3 ใช้อัลกอริทึม Keccak มีขนาดเอาต์พุตแฮชที่หลากหลาย (เช่น 256 บิต และ 512 บิต) ให้ความยืดหยุ่นและความปลอดภัยสูง SHA-3 ได้รับการออกแบบมาให้ทนทานต่อเทคนิคการโจมตีด้วยการเข้ารหัสที่อาจคุกคามอัลกอริทึม SHA อื่นๆ

การใช้ในบล็อกเชน: SHA-3 ให้การรักษาความปลอดภัยระดับสูงและเหมาะสำหรับการใช้ในเทคโนโลยีบล็อกเชน โดยเฉพาะอย่างยิ่งในสถานการณ์ที่ต้องการความสมบูรณ์และความปลอดภัยของข้อมูลระดับสูง การต้านทานต่อการโจมตีด้วยการเข้ารหัสทำให้เป็นตัวเลือกที่แข็งแกร่งสำหรับแอปพลิเคชันที่ความปลอดภัยของข้อมูลเป็นข้อกังวลหลัก รวมถึงการตรวจสอบธุรกรรม ลายเซ็นดิจิทัล และในกระบวนการขุดหาบล็อกเชนที่พิสูจน์การทำงาน

เทคนิคการแฮช (Hashing Technique) เป็นคำทั่วไปที่อ้างถึงกระบวนการใช้ฟังก์ชันแฮชเพื่อแปลงข้อมูลให้เป็นสตริงอักขระที่มีขนาดคงที่ เทคนิคการแฮชมีการใช้งานกันอย่างแพร่หลายในด้านต่าง ๆ ของการประมวลผล รวมถึงการเรียกข้อมูล การเข้ารหัส และการ

ตรวจสอบความสมบูรณ์ของข้อมูล แนวคิดหลักเบื้องหลังการแฮชคือ การรับอินพุต (หรือข้อความ) และส่งกลับสตริงที่มีขนาดคงที่ ซึ่งโดยทั่วไปจะปรากฏแบบสุ่ม ผลลัพธ์เรียกว่าค่าแฮช รหัสแฮช หรือเพียงแค่แฮช

ฟังก์ชันแฮช (Hash Function): ฟังก์ชันแฮชเป็นอัลกอริทึมเฉพาะที่ใช้ในเทคนิคการแฮช เป็นฟังก์ชันทางคณิตศาสตร์ที่แปลงอินพุต (หรือข้อความ) ให้เป็นสตริงไบต์ขนาดคงที่ โดยทั่วไปเอาต์พุตที่เรียกว่าแฮชจะเป็นตัวเลขที่สร้างจากสตริงข้อความ คุณสมบัติที่สำคัญของฟังก์ชันแฮชที่ดี ได้แก่

1) ความมุ่งมั่น: อินพุตเดียวกันจะสร้างเอาต์พุตเดียวกันเสมอ (แฮช)

2) การคำนวณที่รวดเร็ว: แฮชสามารถคำนวณได้อย่างรวดเร็วสำหรับอินพุตที่กำหนด

3) ไม่สามารถกลับด้านได้: การสร้างอินพุตดั้งเดิมจากค่าแฮชของมันควรจะเป็นไปไม่ได้ทางคอมพิวเตอร์ (ซึ่งมักจะเรียกว่าคุณสมบัติทางเดียว)

4) ความต้านทานการชนกัน: อินพุตสองตัวที่แตกต่างกันไม่ควรสร้างค่าแฮชเดียวกัน (แม้ว่าไม่น่าจะเป็นไปได้ทางสถิติ แต่ก็เป็นไปไม่ได้)

ที่อยู่แฮช (Hash Address): ในบริบทของตารางแฮชหรือการจัดเก็บข้อมูล ที่อยู่แฮชหมาย ถึงตำแหน่งในหน่วยความจำที่จัดเก็บข้อมูล (ที่เกี่ยวข้องกับแฮชเฉพาะ) เมื่อใช้ฟังก์ชันแฮชกับกุญแจหรือตัวระบุเพื่อจัดเก็บหรือดึงข้อมูล ค่าแฮชที่ได้จะถูกนำมาใช้เป็นดัชนีเพื่อกำหนดตำแหน่งพื้นที่เก็บข้อมูลที่แน่นอน ซึ่งเรียกว่าที่อยู่แฮช ซึ่งช่วยให้ดึงข้อมูลได้อย่างมีประสิทธิภาพ เนื่องจากฟังก์ชันแฮชให้เส้นทางโดยตรงไปยังตำแหน่งของข้อมูล โดยไม่ต้องค้นหาตามลำดับผ่านรายการ

2.1.5.3 กรณีการใช้งานบล็อกเชนแฮชชิ่ง

บล็อกเชนแฮชชิ่ง (Blockchain Hashing) ซึ่งเป็นลักษณะพื้นฐานของเทคโนโลยีบล็อกเชน มีการใช้งานที่หลากหลายในภาคส่วนต่าง ๆ ต่อไปนี้เป็นกรณีการใช้งานที่สำคัญบางส่วน

1) ธุรกรรมสกุลเงินดิจิทัล: ในสกุลเงินดิจิทัลที่ใช้บล็อกเชน เช่น บิตคอยน์ การแฮชจะใช้เพื่อความปลอดภัยและตรวจสอบธุรกรรม แต่ละธุรกรรมจะถูกแฮช และแฮชเหล่านี้จะ

ถูกรวบรวมเป็นบล็อก การเปลี่ยนแปลงส่วนใดส่วนหนึ่งของธุรกรรมจะเปลี่ยนแฮชของมัน ดังนั้นจึงส่งสัญญาณถึงความไม่สอดคล้องกันในบล็อกเชน ซึ่งช่วยป้องกันการฉ้อโกงและการใช้จ่ายซ้ำซ้อน

2) การขุดและความปลอดภัยเครือข่าย: ในสกุลเงินดิจิทัลที่พิสูจน์การทำงาน การขุด เกี่ยวข้องกับการไขปริศนาการเข้ารหัสที่ซับซ้อน ซึ่งโดยพื้นฐานแล้วหมายถึงการค้นหาค่าแฮชที่เฉพาะเจาะจง กระบวนการนี้รักษาความปลอดภัยเครือข่ายบล็อกเชนด้วยการทำให้มีราคาแพงในการคำนวณและใช้เวลานานในการเพิ่มบล็อกใหม่ ดังนั้นจึงขัดขวางการโจมตีที่เป็นอันตราย

3) ความสมบูรณ์ของข้อมูลในห่วงโซ่อุปทาน: การแฮชของบล็อกเชนสามารถใช้เพื่อติดตามสินค้าในห่วงโซ่อุปทาน แต่ละขั้นตอนของการเดินทางของผลิตภัณฑ์สามารถบันทึกและแฮชบนบล็อกเชนได้ ทำให้เกิดเส้นทางที่ไม่เปลี่ยนรูปและโปร่งใส สิ่งนี้มีประโยชน์อย่างยิ่งในการตรวจสอบความถูกต้องของผลิตภัณฑ์และรับรองว่าผลิตภัณฑ์จะไม่ถูกดัดแปลง

4) การเก็บบันทึกที่ปลอดภัยในการดูแลสุขภาพ: ในอุตสาหกรรมการดูแลสุขภาพ สามารถใช้การแฮชบล็อกเชนเพื่อจัดเก็บบันทึกผู้ป่วยได้อย่างปลอดภัย ด้วยการแฮชข้อมูลที่ละเอียดอ่อนและจัดเก็บแฮชเหล่านี้ไว้ในบล็อกเชน ผู้ให้บริการด้านการแพทย์สามารถรับประกันความสมบูรณ์และการรักษาความลับของข้อมูลผู้ป่วยได้

5) การยืนยันตัวตนดิจิทัล: การแฮชบล็อกเชนสามารถใช้เพื่อสร้างข้อมูลประจำ ตัวดิจิทัลที่ปลอดภัยและไม่เปลี่ยนรูป การแฮชข้อมูลส่วนบุคคลและจัดเก็บไว้ในบล็อกเชนทำให้บุคคลสามารถควบคุมและยืนยันตัวตนของตนได้โดยไม่ต้องเปิดเผยข้อมูลที่ละเอียดอ่อน

6) สัญญาอัจฉริยะ: ในแพลตฟอร์มบล็อกเชนที่รองรับสัญญาอัจฉริยะ เช่น อีเธอเรียม การแฮชถูกใช้เพื่อเข้ารหัส กฎและเงื่อนไขของสัญญา เมื่อปรับใช้แล้วแฮชของสัญญาอัจฉริยะช่วยให้แน่ใจว่าเงื่อนไขไม่สามารถเปลี่ยนแปลงได้

7) การคุ้มครองทรัพย์สินทางปัญญาและลิขสิทธิ์: การแฮชบล็อกเชนสามารถใช้สำหรับการประทับเวลาการสร้างสรรค์ดิจิทัล เช่น งานศิลปะ ดนตรี หรือ วรรณกรรม เพื่อพิสูจน์การมีอยู่ ณ เวลาใดเวลาหนึ่งโดยเฉพาะ สิ่งนี้มีประโยชน์ในการปกป้องสิทธิ์ในทรัพย์สินทางปัญญา

8) ระบบการลงคะแนน: สำหรับระบบการลงคะแนนแบบบล็อกเชน การแฮชทำให้แน่ใจได้ถึงความสมบูรณ์และการไม่เปิดเผยชื่อของการลงคะแนน ช่วยให้สามารถนับคะแนนเสียงได้อย่างโปร่งใสและป้องกันการงัดแงะ ซึ่งอาจลดความเสี่ยงของการฉ้อโกงในการเลือกตั้ง

9) สำนักทะเบียนอสังหาริมทรัพย์และที่ดิน: ในการจัดการบันทึกที่ดิน

และธุรกรรมด้านอสังหาริมทรัพย์ การใช้บล็อกเชนสามารถใช้เพื่อสร้างบันทึกการเป็นเจ้าของธุรกรรมและประวัติของทรัพย์สินอย่างถาวรและไม่สามารถเปลี่ยนแปลงได้

10) การจัดการไฟล์แบบกระจายอำนาจ: ในระบบการจัดเก็บไฟล์แบบกระจายอำนาจที่สร้างขึ้นบนบล็อกเชน การแฮชจะใช้เพื่อตรวจสอบความสมบูรณ์ของไฟล์ที่จัดเก็บและดึงข้อมูลผ่านเครือข่ายแบบกระจาย เพื่อให้มั่นใจว่าข้อมูลยังคงไม่เปลี่ยนแปลงและปลอดภัย

2.1.5.4 การแฮชมีประโยชน์อย่างไร

การแฮชซึ่งเป็นแนวคิดพื้นฐานในด้านวิทยาการคอมพิวเตอร์และความปลอดภัยของข้อมูล ทำให้มีประโยชน์ที่สำคัญหลายประการ เช่น

1) การตรวจสอบความสมบูรณ์ของข้อมูล: การแฮชถือเป็นสิ่งสำคัญในการรับรองความสมบูรณ์ของข้อมูล ด้วยการสร้างค่าแฮชที่ไม่ซ้ำกันสำหรับชุดข้อมูลที่กำหนด การเปลี่ยนแปลงใด ๆ ของข้อมูลแม้แต่การเปลี่ยนแปลงเล็กน้อยก็จะส่งผลให้ได้ค่าแฮชที่แตกต่างกัน คุณลักษณะนี้ใช้กันอย่างแพร่หลายเพื่อตรวจสอบว่าข้อมูลไม่ได้รับการเปลี่ยนแปลง เสียหาย หรือดัดแปลง

2) การดึงข้อมูลอย่างมีประสิทธิภาพ: การแฮชใช้เพื่อเพิ่มประสิทธิภาพกระบวนการดึงข้อมูลโดยเฉพาะในตารางแฮช ซึ่งเป็นโครงสร้างข้อมูลทั่วไป ด้วยการแปลงกุญแจให้เป็นดัชนีของอาร์เรย์โดยใช้ฟังก์ชันแฮช การแฮชทำให้สามารถเข้าถึงข้อมูลและดำเนินการค้นหาได้อย่างรวดเร็ว

3) การปรับปรุงความปลอดภัย: ในขอบเขตของความปลอดภัยทางไซเบอร์ การแฮชช่วยเพิ่มความปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับการจัดเก็บข้อมูลที่ละเอียดอ่อน เช่น รหัสผ่าน รหัสผ่านที่ถูกแฮชช่วยให้มั่นใจได้ว่าแม้ว่าที่เก็บข้อมูลจะถูกบุกรุก แต่รหัสผ่านจริงก็ไม่สามารถเรียกกลับคืนมาได้อย่างง่ายดาย

4) แอปพลิเคชันการเข้ารหัส: ฟังก์ชันการแฮชเป็นรากฐานสำคัญของโพรโทคอลการเข้ารหัสจำนวนมาก ใช้ในการสร้างลายเซ็นดิจิทัล ซึ่งจำเป็นสำหรับการตรวจสอบตัวตนของผู้ใช้และความสมบูรณ์ของข้อมูลหรือเอกสาร

5) การลดขนาดข้อมูล: ฟังก์ชันแฮชสามารถรับอินพุตที่มีความยาวต่างกันและส่งกลับเอาต์พุตที่มีขนาดคงที่ได้ คุณสมบัตินี้มีประโยชน์สำหรับการสรุปข้อมูลจำนวนมากให้เป็นลายนิ้วมือที่มีขนาดเล็กลงซึ่งสามารถจัดการและวิเคราะห์ได้ง่ายขึ้น

6) บล็อกเชนและสกุลเงินดิจิทัล: ในเทคโนโลยีบล็อกเชน การแฮชจะรักษา

ความปลอดภัยของบัญชีแยกประเภทบล็อกเชน เพื่อให้แน่ใจว่าแต่ละบล็อกธุรกรรมจะไม่สามารถเปลี่ยนแปลงได้เมื่อเพิ่มแล้ว นี่เป็นสิ่งสำคัญสำหรับความไว้วางใจและการทำงานของสกุลเงินดิจิทัลและแอปพลิเคชันอื่น ๆ ที่ใช้บล็อกเชน

7) โหลดบาลานซ์: การแฮชสามารถใช้เพื่อกระจายโหลดอย่างสม่ำเสมอทั่วทั้งระบบ ตัวอย่างเช่น ในเครือข่ายแบบกระจาย การแฮชจะช่วยกระจายพื้นที่จัดเก็บข้อมูลหรือโหลดเครือข่ายอย่างสม่ำเสมอ ปรับปรุงประสิทธิภาพและความเสถียรของระบบ

8) การตรวจจับข้อผิดพลาด: ฟังก์ชันแฮชบางอย่างใช้เพื่อตรวจจับข้อผิดพลาดในการส่งหรือจัดเก็บข้อมูล Checksum ซึ่งเป็นแฮชประเภทหนึ่ง มักใช้ในการสื่อสารเครือข่ายเพื่อรับรองความสมบูรณ์ของข้อมูลระหว่างการส่งผ่าน

9) การไม่เปิดเผยตัวตน: ในบางแอปพลิเคชันการแฮชสามารถช่วยรักษาการไม่เปิดเผยตัวตนของผู้ใช้โดยการปกปิดข้อมูลต้นฉบับ ซึ่งมีความเกี่ยวข้องอย่างยิ่งในการวิเคราะห์ข้อมูลการรักษาความเป็นส่วนตัว

10) การป้องกันรายการที่ซ้ำกัน: สามารถใช้แฮชเพื่อตรวจสอบรายการหรือบันทึกที่ซ้ำกัน ด้วยการแฮชข้อมูลและเปรียบเทียบค่าแฮช ระบบสามารถระบุและป้องกันรายการที่ซ้ำกันได้อย่างมีประสิทธิภาพ

2.1.6 กลไกฉันทามติ (Consensus Algorithm)

หลักการทำงานของบล็อกเชนอยู่ภายใต้ระบบที่เรียกว่าระบบฉันทามติ (Consensus Algorithm) ซึ่งเป็นกระบวนการในวิทยาการคอมพิวเตอร์ที่ใช้เพื่อให้บรรลุข้อตกลงเกี่ยวกับค่าข้อมูลเดี่ยวระหว่างกระบวนการหรือระบบแบบกระจาย อัลกอริทึมเหล่านี้ได้รับการออกแบบมาเพื่อให้เกิดความน่า เชื่อถือในเครือข่ายที่มีผู้ใช้หลายคนหรือมีโหนดหลากหลาย และเป็นชุดของกฎที่ช่วยปกป้องเครือ ข่ายจากพฤติกรรมที่เป็นอันตรายและการโจมตีจากการแฮก การแก้ปัญหานี้หรือที่เรียกว่าปัญหาฉันทามตินั้นมีความสำคัญในระบบคอมพิวเตอร์แบบกระจายและระบบหลายตัวแทน เช่น ที่เห็นในเครือข่ายบล็อกเชนสกุลเงินดิจิทัล ระบบฉันทามตินั้นมีหลายประเภทขึ้นอยู่กับบล็อกเชนและการใช้งานที่ได้รับความนิยมในปัจจุบันมีดังนี้ (Techsauce Team, 2022, p. 1)

2.1.6.1 การพิสูจน์ด้วยการทำงาน (Proof of Work - PoW)

การพิสูจน์ด้วยการทำงาน เป็นระบบฉันทามติแบบดั้งเดิมที่เก่าแก่ที่สุดและ

เป็นที่รู้จักกันดีบนบล็อกเชน ถูกพัฒนาขึ้นโดย Satoshi Nakamoto ระบบฉันทามติแบบ PoW ใช้เพื่อเลือกนักขุด (Mining) สำหรับการสร้างบล็อกถัดไปบิตคอยน์ใช้ระบบฉันทามตินี้ แนวคิดหลักที่อยู่เบื้องหลังกลไกตัวนี้คือการไขปริศนาทางคณิตศาสตร์ที่ซับซ้อนและให้คำตอบได้อย่างง่ายดาย ปริศนาทางคณิตศาสตร์นี้ต้องใช้พลังในการคำนวณอย่างมาก ดังนั้นโหนดที่ไขปริศนาได้เร็วที่สุดจะได้ขุดบล็อกถัดไป อย่างไรก็ตาม PoW ยังคงได้รับความนิยมอย่างต่อเนื่อง เนื่องจากมีการรักษาความปลอดภัยของเครือข่ายและทนทานต่อการโจมตีทางไซเบอร์ เช่น การโจมตีแบบปฏิเสธการให้ บริการ (Distributed Denial-of-Service – DDoS) ระบบฉันทามติแบบ PoW ถูกใช้โดยสกุลเงินดิจิทัลหลายสกุล เช่น Bitcoin, Litecoin, ZCash, Primecoin, Monero และ Vertcoin เป็นต้น (ก่อนหน้านี้มีอีเธอเรียมด้วยที่ใช้กลไกนี้ แต่ปัจจุบันได้เปลี่ยนไปใช้กลไกของการพิสูจน์ด้วยการค้ำประกัน (Proof of Stake– PoS) ในแง่ของการนำไปใช้งาน PoW ไม่เพียงแต่มีอิทธิพลต่ออุตสาหกรรมการเงินเท่านั้น แต่ยังรวมถึงการดูแลสุขภาพ ธรรมาภิบาลภาครัฐ การจัดการและอื่น ๆ อย่างไรก็ตามระบบฉันทามติแบบ PoW ยังมีข้อกังวลในประเด็นการใช้พลังงานจำนวนมหาศาลที่นำไปสู่ค่าใช้จ่ายที่สูง รวมถึงปริมาณการใช้ไฟฟ้ามีผลต่อสิ่งแวดล้อม ซึ่งสิ่งนี้ทำให้หลาย ๆ โพรโทคอลบนบล็อกเชนเปลี่ยนไปใช้ระบบฉันทามติแบบอื่นที่ประหยัดพลังงานมากกว่า

2.1.6.2 ความผิดพลาดของไบแซนไทน์ (Practical Byzantine Fault Tolerance - pBFT)

ความผิดพลาดของไบแซนไทน์ เป็นอัลกอริทึมที่เปิดตัวในช่วงปลายยุค 90 โดย Barbara Liskov และ Miguel Castro ซึ่ง pBFT เป็นอัลกอริทึมบล็อกเชนขนาดเล็กที่แก้ปัญหาต่าง ๆ ที่เกี่ยวข้องกับโซลูชัน Byzantine General ได้อย่างมีประสิทธิภาพ โดยให้ผู้ใช้ยืนยันข้อความที่ส่งถึงพวกเขาด้วยการคำนวณเพื่อประเมินการตัดสินใจเกี่ยวกับความถูกต้องของข้อมูล จากนั้นก็จะประกาศการตัดสินใจไปยังโหนดอื่น ๆ ที่ดำเนินการตัดสินใจในท้ายที่สุด ด้วยวิธีนี้การตัดสินใจขั้นสุดท้ายจะขึ้นอยู่กับการตัดสินใจที่ได้รับจากโหนดอื่น ๆ ตัวอย่างเครือข่ายบล็อกเชนที่มีการใช้งานของระบบฉันทามติแบบนี้ เช่น Stellar, Ripple และ Hyperledger Fabric เป็นต้น ข้อจำกัดของระบบฉันทามติแบบนี้ คือ pBFT จะทำงานได้อย่างมีประสิทธิภาพก็ต่อเมื่อจำนวนโหนดในเครือข่ายแบบกระจายมีจำนวนน้อย เนื่องจากมีค่าใช้จ่ายในการสื่อสารสูงซึ่งเพิ่มขึ้นแบบทวีคูณกับโหนดพิเศษทุกโหนดในเครือข่าย

2.1.6.3 การพิสูจน์ด้วยการค้ำประกัน (Proof of Stake - PoS)

การพิสูจน์ด้วยการค้ำประกัน ถือเป็นทางเลือกที่มีความเป็นมิตรกับสิ่งแวดล้อมมากกว่าการพิสูจน์ด้วยการทำงาน ซึ่งมีความแตกต่างที่เห็นชัดเจนอย่างยิ่งคือ PoS ต้องการทรัพยากรฮาร์ดแวร์หรือซอฟต์แวร์พิเศษเพียงเล็กน้อยในการขุดสกุลเงินดิจิทัล เนื่องจากไม่เกี่ยวข้องกับการแก้ปัญหาการคำนวณที่ซับซ้อน แต่ตัวตรวจสอบการเข้ารหัสลับจะค้ำประกันเหรียญบางส่วนในกระเป๋าเงิน จากนั้นพวกเขาจะตรวจสอบบล็อก หากพบบล็อกที่สามารถเพิ่มลงในบล็อกเชนได้ ผู้ตรวจสอบจะได้รับรางวัลหรือเงินค้ำประกันเพิ่มขึ้นตามสัดส่วนกับการค้ำประกันตามบล็อกที่เพิ่มในบล็อกเชน เนื่องจากอัลกอริทึมอิงตามสิ่งจูงใจ จึงใช้พลังงานในการคำนวณน้อยกว่าแบบ PoW แม้จะมีข้อได้เปรียบนี้แต่อัลกอริทึม PoS ก็มีข้อเสียอย่างร้ายแรง นั้นคือความสามารถในการขุดของเครื่องมือตรวจสอบซึ่งจะขึ้นอยู่กับจำนวนของโทเค็นที่พวกเขามี ดังนั้นนักขุดที่เริ่มต้นด้วยเหรียญที่มากจะสามารถควบคุมกลไกฉันทามติได้มากขึ้น นอกจากนี้นักขุดเพียงไม่กี่คนยังสามารถซื้อเหรียญจำนวนมากได้ ทำให้กลไกเจือจางมากขึ้นและลดคุณสมบัติการกระจายของระบบลงไป โดยรวมแล้วสิ่งสนับสนุนให้แพลตฟอร์มต่าง ๆ เช่น อีเธอเรียมได้ปรับเปลี่ยนระบบฉันทามติจาก PoW เป็น PoS ในการอัปเดต Ethereum 2.0 นอกจากนี้ยังช่วยให้ระบบนิเวศของบล็อกเชนต่าง ๆ เช่น Dash, Peercoin, Decred, Reddcoin และ PivX ทำงานได้อย่างถูกต้อง ตัวอย่างเครือข่ายบล็อกเชนที่ใช้ระบบฉันทามติแบบ PoS ได้แก่ Cardano (ADA), Solana, Avalanche และ Polkadot เป็นต้น

2.1.6.4 การพิสูจน์การมีส่วนได้ส่วนเสียที่ได้รับมอบหมาย (Delegated Proof of Stake - DPoS)

การพิสูจน์การมีส่วนได้ส่วนเสียที่ได้รับมอบหมาย เป็นระบบฉันทามติอีกประเภทหนึ่งของ PoS ที่มีประสิทธิภาพและเป็นประชาธิปไตยมากกว่า DPoS ได้ถูกพัฒนาขึ้นโดย Daniel Larimer ผู้ก่อตั้ง BitShares, Steemit และ EOS ในปีพ.ศ. 2557 อัลกอริทึมนี้ขึ้นอยู่กับระบบการลงคะแนนซึ่งผู้รับมอบสิทธิ์หรือพยาน ลงคะแนนให้กับผู้ตรวจสอบความถูกต้องที่พวกเขาชื่นชอบเพื่อให้ได้ฉันทามติระหว่างการสร้างและการตรวจสอบบล็อก นอกจากการตรวจสอบธุรกรรมแล้วผู้ได้รับมอบหมายยังช่วยรักษาความสมบูรณ์ ความเชื่อถือและความโปร่งใสของเครือข่ายบล็อกเชน นอกจากนี้ DPoS เป็นกลไกที่ปรับขนาดได้มากกว่า PoW หรือ PoS เนื่องจากสามารถประมวลผลธุรกรรมต่อวินาทีได้มากขึ้นและให้เวลายืนยันที่รวดเร็วกว่า ตัวอย่างเครือข่ายบล็อกเชนที่ใช้ระบบฉันทามติแบบ DPoS ได้แก่ EOS, BitShares, Steemit, Lisk, Ark และ Tron เป็นต้น

2.1.6.5 การพิสูจน์การเผาไหม้ (Proof of Burn - PoB)

การพิสูจน์การเผาไหม้ กำลังได้รับการทดสอบว่าเป็นทางเลือกที่ใช้งานได้และยั่งยืนสำหรับระบบฉันทามติแบบ PoW และ PoS ในแง่ของการใช้พลังงาน ซึ่งระบบฉันทามติแบบ PoB จะเหมือนกับ PoW แต่จะใช้พลังงานในการคำนวณน้อยกว่า นี่เป็นเพราะกระบวนการตรวจสอบความถูกต้องของบล็อกเชนไม่ต้องการทรัพยากรหรือฮาร์ดแวร์ในการคำนวณ ในทางกลับกันนัดขุดจะ “เผา” หรือ ลงทุนเหรียญในบล็อกเชนเพื่อให้ได้ฉันทามติ เหรียญจำนวนหนึ่งจะถูกส่งไปยังบัญชีหนึ่งที่เรียกว่า “Eater Address” ซึ่งไม่สามารถเรียกคืนได้ กู้คืนหรือนำไปใช้ได้ ทำให้ไม่สามารถเข้าถึงได้และไม่มีประโยชน์ สิ่งเหล่านี้แสดงให้เห็นถึงความมุ่งมั่นของนักขุดที่มีต่อเครือข่ายและให้สิทธิ์ในการขุดเหรียญใหม่และตรวจสอบธุรกรรมใหม่บนเครือข่าย ยิ่งนัดขุดเผาเหรียญมากเท่าไหร่ พวกเขาก็ยิ่งมีพลังในการขุดมากขึ้นเท่านั้นซึ่งจะเพิ่มโอกาสในการเป็นผู้ตรวจสอบความถูกต้องของบล็อกถัดไป การเผาเหรียญใน PoB จะช่วยลดอุปทานของเหรียญและเพิ่มมูลค่าของเหรียญ นอกจากนี้ยังปรับปรุงความปลอดภัยของเครือข่ายผ่านการลงทุนเผาเหรียญ ตัวอย่างเครือข่ายบล็อกเชนที่ใช้ระบบฉันทามตินี้ ได้แก่ Slimcoin และ Factom

2.1.6.6 การพิสูจน์ด้วยความสามารถ (Proof of Capacity - PoC)

การพิสูจน์ด้วยความสามารถ เป็นระบบที่ใช้ความจุของเครื่องคอมพิวเตอร์หรือความจุของฮาร์ดไดร์ฟในการขุด เนื่องจากระบบฉันทามติแบบ PoC ไม่ต้องใช้อุปกรณ์ที่มีราคาแพงหรืออุปกรณ์พิเศษ ยิ่งมีตัวตรวจสอบความถูกต้องของพื้นที่ฮาร์ดไดร์ฟมากเท่าใดโอกาสที่จะได้รับเลือกสำหรับการขุดบล็อกถัดไปและรับรางวัลบล็อกก็จะยิ่งดีขึ้นเท่านั้น ระบบนี้จึงเปิดโอกาสให้คนทั่วไปมีส่วนร่วมในเครือข่ายได้ อย่างไรก็ตามนักพัฒนาไม่กี่รายเลือกที่จะใช้ระบบฉันทามตินี้เนื่องจากยังคงมีข้อกังวลเกี่ยวกับความอ่อนแอต่อการโจมตีของมัลแวร์ ตัวอย่างเครือข่ายบล็อกเชนที่ใช้ระบบฉันทามตินี้ ได้แก่ Burstcoin และSpaceMint

2.1.6.7 การพิสูจน์ด้วยเวลาที่ผ่านไป (Proof of Elapsed Time - PoET)

การพิสูจน์ด้วยเวลาที่ผ่านไป เป็นระบบฉันทามติที่เป็นเอกฉันท์ว่ายุติธรรมที่สุด ซึ่งเลือกจากบล็อกถัดไปโดยใช้วิธีการที่ยุติธรรมเท่านั้น มีการใช้กันอย่างแพร่หลายในเครือข่ายบล็อกเชนที่ได้รับอนุญาต (Permissioned blockchain) ในอัลกอริทึมนี้ ผู้ตรวจสอบทุกคนในเครือข่ายจะได้รับโอกาสที่ยุติธรรมในการสร้างบล็อกของตนเอง โหนดทั้งหมดทำได้โดยการรอเป็น

ระยะเวลาหนึ่งและเพิ่มหลักฐานการรอในบล็อก บล็อกที่สร้างขึ้นจะถูกส่งไปยังเครือข่ายเพื่อให้ผู้อื่นพิจารณา ผู้ชนะคือตัวตรวจสอบที่มีค่าตัวจับเวลาน้อยที่สุด ในส่วนการพิสูจน์บล็อกจากโหนดตัวตรวจสอบความถูกต้องที่ชนะจะถูกผนวกเข้ากับบล็อกเชน มีการตรวจสอบเพิ่มเติมในอัลกอริทึมเพื่อหยุดไม่ให้โหนดชนะการเลือกตั้งเสมอ และหยุดไม่ให้โหนดสร้างค่าตัวจับเวลาที่ต่ำที่สุด แม้ว่าระบบฉันทามติแบบนี้จะมีประสิทธิภาพสูงและใช้พลังงานน้อย แต่สิ่งที่ยังเป็นข้อถกเถียงคือ การที่ระบบนี้เป็นโปรแกรมของ Intel จึงอาจจะปราศจากการกระจายศูนย์ ตัวอย่างเครือข่ายบล็อกเชนที่ใช้ระบบฉันทามติแบบนี้ ได้แก่ Hyperledger Fabric และ Hyperledger Sawtooth

2.1.6.8 การพิสูจน์ด้วยการมีอำนาจ (Proof of Authority - PoA)

การพิสูจน์ด้วยการมีอำนาจ คือเวอร์ชันแก้ไขของการพิสูจน์ด้วยการค้ำประกัน ซึ่งมีตัวตนของผู้ตรวจสอบความถูกต้องในเครือข่ายเป็นเดิมพัน PoA เป็นทางเลือกที่มีประสิทธิภาพและปรับขนาดได้มากกว่าสำหรับ PoW ที่ใช้พลังงานสูงและปรับขนาดได้น้อยกว่า นอกจากนี้ใน PoA เครื่องมือตรวจสอบความถูกต้องของบล็อกจะเดิมพันชื่อเสียงและตัวตนของพวกเขามากกว่าเหรียญ ทำให้ระบบมีความปลอดภัยมากกว่า PoS โดยพื้นฐานแล้วเครือข่ายบล็อกเชนที่ใช้ PoA นั้นได้รับการรักษาความปลอดภัยโดยโหนดตรวจสอบความถูกต้องในจำนวนจำกัด โหนดเหล่านี้เป็นฝ่ายที่เชื่อถือได้ซึ่งถูกเลือกโดยพลการและได้รับการอนุมัติล่วงหน้าเพื่อการตรวจสอบบล็อกและการทำธุรกรรม ผู้เข้าร่วมเหล่านี้ทำหน้าที่เป็นผู้ดูแลระบบและช่วยสร้างกลไกที่ปรับขนาดได้มากกว่า PoW ดังนั้น PoA จึงเหมาะอย่างยิ่งสำหรับการใช้งานด้านโลจิสติกส์ เช่น ซัพพลายเชนหรือเครือข่ายการค้า ช่วยให้ผู้ใช้สามารถใช้ประโยชน์จากประโยชน์ทั้งหมดของเทคโนโลยีบล็อกเชน ในขณะที่รักษาความเป็นส่วนตัวและรักษาความปลอดภัยในการทำธุรกรรม อย่างไรก็ตาม PoA แทบไม่ต้องใช้พลังงานในการประมวลผลเลย เพราะใช้ทรัพยากรน้อยกว่าระบบฉันทามติแบบอื่น ๆ และมีต้นทุนที่ต่ำกว่า แต่ก็มีความเสี่ยงเรื่องการถูกโจมตีจากการเปิดเผยตัวตนของผู้ตรวจสอบและ PoA ตัวอย่างเครือข่ายบล็อกเชนที่ใช้ระบบฉันทามติแบบนี้ ได้แก่ VeChain, Ethereum Kovan testnet, xCHAIN และ REI chain เป็นต้น

2.1.6.9 การพิสูจน์ด้วยผู้มีอำนาจในการค้ำประกัน (Proof of Stake Authority - PoSA)

การพิสูจน์ด้วยผู้มีอำนาจในการค้ำประกัน เป็นระบบฉันทามติลูกผสมระหว่าง PoS และ PoA แบบจำลองฉันทามติของ PoSA รองรับเวลาบล็อกที่สั้นกว่าและต้นทุนต่ำกว่า

PoSA ได้นำเสนอการเปลี่ยนแปลงที่ปฏิวัติวงการโลกบล็อกเชน โดยพิจารณาไม่เพียงแค่สัดส่วนการถือหุ้นที่ตัวตรวจสอบโหนดแต่ละโหนดมีส่วนร่วมกับเครือข่าย แต่ยังรวมถึงระดับกิจกรรมของพวกเขาด้วย เป็นวิธีการใหม่ในการสร้างบล็อก และการตรวจสอบความถูกต้องจะเป็นตัวกำหนดอนาคตของเศรษฐกิจบล็อกเชน PoSA ใช้สัญญาอัจฉริยะที่ปรับใช้โดยตัวตรวจสอบความถูกต้องเพื่อประเมินการกระทำของผู้ใช้นอกเหนือจากเงินเดิมพัน ก่อนที่จะให้โอกาสในการเป็นผู้ผลิตบล็อกหรือตัวตรวจสอบความถูกต้อง สิ่งนี้ส่งผลต่อการกระจายของรางวัลบล็อกด้วย PoSA ให้ความสำคัญกับผู้เข้าร่วมเครือข่ายที่ให้ความสำคัญกับการส่งมอบคุณค่าให้กับผู้ใช้ผ่านรางวัลบล็อกที่สม่ำเสมอ ซึ่งมีฐานผู้ใช้มาก ระดับของกิจกรรมก็จะยิ่งมากขึ้นและส่วนแบ่งของรางวัลก็จะมากขึ้นเท่านั้น แนวทางระบบฉันทามติใหม่นี้มีเป้าหมายเพื่อสร้างสภาพแวดล้อมธุรกิจ web3.0 สามารถเติบโตได้ และธุรกิจ web2.0 สามารถเข้าร่วมและปรับเปลี่ยนรูปแบบสำหรับบล็อกเชนในอนาคตได้อย่างง่ายดาย ระบบฉันทามติแบบ PoSA นี้เป็นพื้นฐานของ Binance Smart Chain เมื่อเปรียบเทียบกับกลไกฉันทามติของ PoW ที่ใช้โดย Ethereum (ETH) (ซึ่งตอนนี้ได้เปลี่ยนจาก PoW เป็น PoS ด้วยการเปิดตัว Ethereum 2.0)

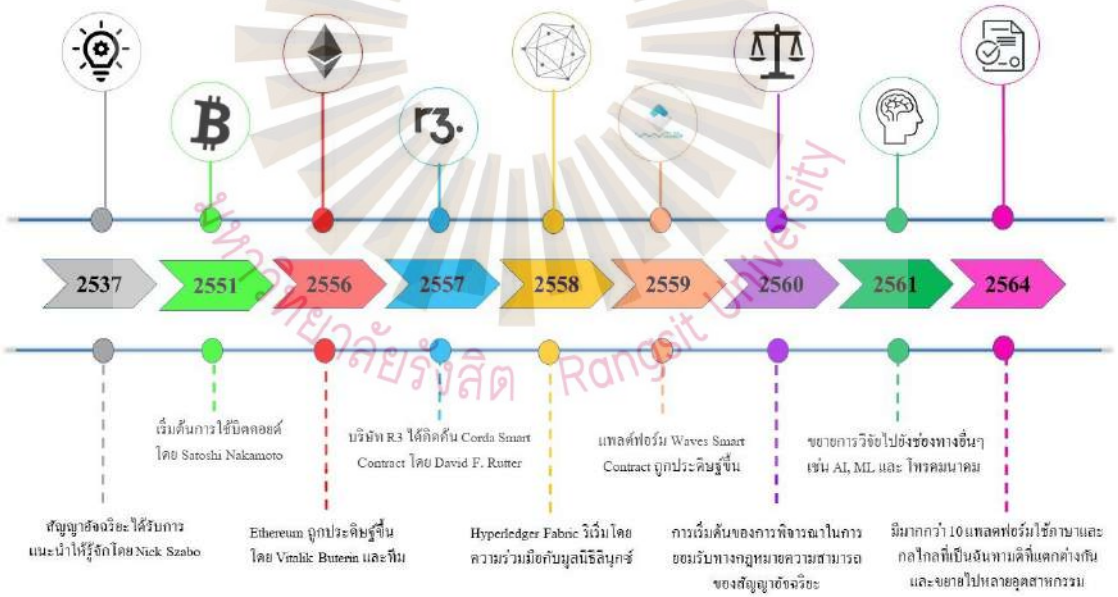
2.2 สัญญาอัจฉริยะ (Smart Contract-สมาร์ตคอนแทรค)

แนวคิดของสัญญาอัจฉริยะได้รับการแนะนำครั้งแรกในปีพ.ศ. 2537 โดย Nick Szabo ที่เป็นผู้เสนอแนวคิดที่ว่า บล็อกเชนสามารถใช้ในการบันทึกข้อตกลงของสัญญาที่สามารถดำเนินการได้ด้วยตนเองไม่จำเป็นต้องมีคนกลางหรือใช้พนักงานในการตรวจสอบเอกสาร โดยทุกอย่างให้คอมพิวเตอร์และโปรแกรมเป็นตัวจัดการ และการแฮกหรือการโจมตีข้อมูลทำได้ยาก โดยมีอีเธอเรียมเป็นหนึ่งในแพลตฟอร์มสัญญาอัจฉริยะที่โดดเด่นที่สุดกับแอปพลิเคชันมากมายในบริบทที่แตกต่างกัน ในขั้นต้นสัญญาอัจฉริยะมีเป้าหมายเฉพาะสำหรับแอปพลิเคชันทางด้านการเงินเท่านั้น เช่น ERC20 Tokens เมื่อเวลาผ่านไปมีการประดิษฐ์แพลตฟอร์มสัญญาอัจฉริยะที่หลากหลายเกิดขึ้น เนื่องมาจากข้อกำหนดทางอุตสาหกรรมต่าง ๆ (Szabo, 2017, pp. 4-8)

2.2.1 วิวัฒนาการของสัญญาอัจฉริยะ

รูปที่ 2.4 แสดงเหตุการณ์สำคัญทางประวัติศาสตร์การวิวัฒนาการของสัญญาอัจฉริยะบนบล็อกเชน เป็นการแนะนำแนวคิดของสัญญาอัจฉริยะ โดย Nick Szabo ในปีพ.ศ. 2537 ซึ่งถือเป็นจุดกำเนิดของสัญญาอัจฉริยะ การนำบิตคอยด์มาใช้ในระบบการชำระเงินแบบกระจายศูนย์ มีการจัด

เก็บประวัติการทำธุรกรรมไว้ในบัญชีแยกประเภทที่ถูกสร้างขึ้นจากบล็อก การประดิษฐ์อีเธอเรียมเป็นหนึ่งในการก้าวกระโดดที่สำคัญที่สุดของประวัติศาสตร์สัญญาอัจฉริยะ บล็อกเชนสาธารณะของอีเธอเรียมอนุญาตให้ผู้ใช้เข้าร่วมและปรับใช้แอปพลิเคชันสัญญาอัจฉริยะในบล็อกเชนสาธารณะ อีเธอเรียมเป็นเป้าหมายหลักสำหรับการแลกเปลี่ยนสกุลเงินในตอนเริ่มต้น โครงการไฮเปอร์เลดเจอร์แฟบริค (Hyperledger Fabric) ริเริ่มโดยความร่วมมือกับมูลนิธิลินุกซ์ (Linux Foundation) ทิศทางของไฮเปอร์เลดเจอร์แฟบริคมีการเบี่ยงเบนไปจากอีเธอเรียมเนื่องจากไฮเปอร์เลดเจอร์ตั้งใจให้เป็นบล็อกเชนระดับองค์กร แพลตฟอร์มจำนวนมากที่ได้รับการพัฒนาให้ตรงกับเป้าหมายความต้องการขององค์กร การวิจัยมุ่งเน้นไปที่การทำให้ถูกต้องตามกฎหมายของสัญญาอัจฉริยะพร้อมกับการครบกำหนดของบริบทของสัญญาอัจฉริยะที่มีหลากหลายแพลตฟอร์มและการใช้งานที่หลากหลายกรณีแตกต่างกันไป ปัจจุบันมีมากกว่า 10 แพลตฟอร์มที่ทำงานบนเครือข่ายบล็อกเชนต่าง ๆ และใช้ภาษาสัญญาอัจฉริยะและกลไกลที่เป็นฉันทามติที่แตกต่างกัน การวิจัยรุ่นถัดไปมุ่งเน้นอย่างมากเกี่ยวกับตำแหน่งของสัญญาอัจฉริยะในหัวข้อการวิจัยที่เกิดขึ้นใหม่ในส่วนของวิทยาการคอมพิวเตอร์ (Hewa, Hu, Liyanage, Kanhare, & Ylianttila, 2021, pp. 87645-87646)



รูปที่ 2.4 วิวัฒนาการของสัญญาอัจฉริยะ

ที่มา: Hewa, Hu, Liyanage, Kanhare, & Ylianttila, 2021

2.2.2 คุณสมบัติของเทคโนโลยีสัญญาอัจฉริยะบนบล็อกเชน

สัญญาอัจฉริยะเป็นโปรแกรมที่บังคับตนเองและดำเนินการด้วยตัวเอง ซึ่งเป็นข้อ

กำหนดและเงื่อนไขเฉพาะข้อตกลงโดยใช้ชุดคำสั่งและโครงสร้างพื้นฐานการคำนวณ สัญญาอัจฉริยะเป็นโปรแกรมกระจายศูนย์ที่ขยายการใช้งานเครือข่ายบล็อกเชนพื้นฐาน โปรแกรมนี้เปลี่ยนรูปไม่ได้และได้รับการตรวจสอบด้วยการเข้ารหัสเพื่อความน่าเชื่อถือ

คุณสมบัติบางอย่างของสัญญาอัจฉริยะได้สืบทอดมาจากพื้นฐานของเทคโนโลยีบล็อกเชน คุณลักษณะเหล่านี้ช่วยให้มีการจ้างงานเกี่ยวกับสัญญาอัจฉริยะได้หลากหลายมากขึ้น โดยทั่วไปแล้ว สัญญาอัจฉริยะจะดำเนินการในโหมดการให้บริการระหว่างบุคคลหรือบริษัทโดยตรง (เพียร์ทูเพียร์, peer-to-peer) โดยไม่มีการแทรกแซงจากคนกลาง ให้ความพร้อมในการให้บริการโดยไม่พึ่งพาการรวมศูนย์แต่อย่างใด และอนุญาตให้ดำเนินการธุรกรรมอัตโนมัติเมื่อถึงเงื่อนไขที่กำหนดไว้ล่วงหน้า รายละเอียดของคุณสมบัติหลักของสัญญาอัจฉริยะบนบล็อกเชนมีดังนี้ (Hewa, Hu, Liyanage, Kanhare, & Ylianttila, 2021, pp. 87646-87647)

2.2.2.1 การกำจัดคนกลางและเป็นอิสระในการดำเนินการ

ข้อได้เปรียบที่สำคัญที่สุดของสัญญาอัจฉริยะบนบล็อกเชน คือ การกระจายศูนย์ความต้องการของคนกลาง เช่น นายหน้า ตัวแทน หรือ ผู้ให้บริการ สามารถขับออกได้เมื่อมีการรวมระบบเฉพาะเข้าด้วยกันกับสัญญาอัจฉริยะบนบล็อกเชน การกำจัดคนกลางได้นั้นจะช่วยให้ลดต้นทุนการทำธุรกรรมและลดอำนาจที่ถูกกำหนดนโยบายจากหน่วยงานส่วนกลาง ตัวอย่างที่สำคัญที่สุดอย่างหนึ่ง คือ เงินตราเข้ารหัสลับ หรือ คริปโทเคอร์เรนซี (Cryptocurrency) ซึ่งใช้สัญญาอัจฉริยะเพื่อเปลี่ยนบทบาทของคนกลาง เช่น ธนาคารกลาง คนกลางจะกำหนดค่าใช้จ่ายที่สูงสำหรับการทำธุรกรรมและปฏิบัติตัวเป็นองค์กรสูงสุด ผู้ใช้จำเป็นต้องปฏิบัติตามกฎระเบียบที่กำหนดโดยการรวมศูนย์อำนาจ

ในทางตรงกันข้าม สัญญาอัจฉริยะได้จัดเตรียมขั้นตอนข้อตกลงที่จะกำหนดโดยผู้เข้าร่วมเองแบบประชาธิปไตยสูงสุด ผู้เข้าร่วมกำหนดกฎและข้อบังคับสำหรับการสร้างสัญญาอัจฉริยะและปรับใช้ข้อตกลงร่วมกัน เงื่อนไขโปรแกรมและการไหลของเหตุการณ์ควรดำเนินการเมื่อบล็อกเชนได้ถึงสถานะที่กำหนดไว้ล่วงหน้า จะมีการกำหนดสถานะเฉพาะในสัญญาอัจฉริยะตามข้อตกลงของทุกฝ่ายในเครือข่ายบล็อกเชน โดยสถานะนี้อาจเป็นเงื่อนไขใดก็ได้ เช่น ยอดเงินคงเหลือเฉพาะในกระเป๋าเงินหรือระยะเวลาที่กำหนด เป็นต้น จากนั้นการดำเนินการจะเป็นไปโดยอัตโนมัติโดยไม่มีการแทรกแซงจากคนกลาง รับประกันความพร้อมในการให้บริการ เนื่องจากการ

ดำเนินการไม่ได้อาศัยคนกลางและดำเนินการแบบการให้บริการระหว่างบุคคลหรือบริษัทโดยตรง การดำเนินการอัตโนมัติตามเงื่อนไข ช่วยให้มั่นใจได้ถึงความถูกต้องของการทำงานโดยไม่ต้องคำนึงถึงความผิดพลาดของมนุษย์หรือแม้จะไม่มีการกระทำที่ลำเอียงก็ตาม ดังนั้นสัญญาอัจฉริยะถือเป็นโซลูชันที่มีแนวโน้มที่ดีสำหรับการใช้งานส่วนใหญ่ซึ่งต้องการทางเลือกอื่นที่ปราศจากคนกลาง

2.2.2.2 ป้องกันการปลอมแปลงและไม่สามารถแก้ไขได้

ความสมบูรณ์ของการบันทึกธุรกรรมในบัญชีแยกประเภทแบบกระจายได้รับการตรวจสอบด้วยลายเซ็นดิจิทัล นอกจากนี้การตรวจสอบการทำธุรกรรมแต่ละรายและได้รับการอนุมัติก่อนการต่อท้ายในบัญชีแยกประเภท บัญชีแยกประเภทที่เพิ่มขึ้นเรื่อย ๆ ประกอบด้วยธุรกรรมที่ได้รับอนุมัติที่ไม่เปลี่ยนรูป การเปลี่ยนแปลงไม่ได้ถูกกระทำโดยบุคคล การปรับใช้รหัสสัญญาอัจฉริยะบนบล็อกเชนนั้นไม่ถูกเปลี่ยนรูป สามารถนำรหัสไปใช้ได้ในแต่ละโหนดโดยใช้เทคนิคต่าง ๆ ตัวอย่างเช่น ไฟล์เรียกทำงานที่อยู่ในคอนเทนเนอร์ รหัสสัญญาอัจฉริยะเห็นได้ชัดว่ามีการดัดแปลงและสัญญาอัจฉริยะที่ถูกแก้ไขไม่สามารถดำเนินการได้ อย่างไรก็ตามสัญญาอัจฉริยะสามารถอัปเดตได้หากต้องการตามข้อตกลงของโหนดในเครือข่ายบล็อกเชน ดังนั้น ทุกฝ่ายในเครือข่ายบล็อกเชนสามารถเชื่อถือสัญญาอัจฉริยะ และเชื่อมั่นว่า รหัสที่ดำเนินการมีตรรกะที่เปิดเผยและตกลงโดยสมาชิกแต่ละคนของเครือข่ายบล็อกเชน

2.2.2.3 ความโปร่งใส

ความโปร่งใสเป็นหนึ่งในคุณสมบัติที่แตกต่างที่สำคัญที่สืบทอดจากบล็อกเชนถึงสัญญาอัจฉริยะ ความโปร่งใสของสัญญาอัจฉริยะนั้นเป็นถึงสองเท่า ประการแรกคือ รหัสที่กำหนด ไว้ในสัญญาอัจฉริยะนั้นมีความโปร่งใสต่อฝ่ายที่แทรกแซง รวมทั้งต่อสาธารณชน ประการที่สองคือ ชุดของการทำธุรกรรมที่รวมอยู่ในบล็อกก็ยังมีความโปร่งใสต่อสาธารณะ ดังนั้นที่ฝ่ายแทรกแซงของเครือข่ายบล็อกเชนสามารถเชื่อถือตรรกะและการทำธุรกรรมในเครือข่ายบล็อกเชนได้ในตัวอย่างที่เป็นรูปธรรมมากขึ้น ถ้าตรรกะของสัญญาอัจฉริยะที่กำหนดโดยอำนาจของรัฐบาลซึ่งเป็นผู้มีส่วนร่วมของเครือข่ายบล็อกเชน การดำเนินการเฉพาะที่ถูกดำเนินการตามตรรกะนั้นถือได้ว่าเชื่อถือได้และเป็นกลาง เนื่องจากรหัสนั้นปรากฏต่อสาธารณะ นอกจากนี้การทำธุรกรรมที่เพิ่มลงในบัญชีแยกประเภทยังปรากฏต่อสาธารณะเพื่อให้เกิดความมั่นใจ ในทางตรงกันข้ามสถาปัตยกรรมบริการแบบรวมศูนย์ไม่ได้โปรงใสและมีแนวโน้มที่จะเกิดช่องโหว่ เช่น การโจมตีแบบ Asman-in-the-

Middle ฐานข้อมูลส่วนกลางก็มีความเสี่ยงเช่นกันและไม่สามารถติดตามได้หากมีการแก้ไขดัดแปลงใด ๆ เกิดขึ้นกับข้อมูลที่เหลือ ความโปร่งใสของสัญญาอัจฉริยะทำให้สมาชิกระบบนิเวศบล็อกเชนสามารถตรวจสอบความถูกต้องของการเปิดเผยต่อสาธารณะได้

2.2.3 ข้อดีข้อเสียของสัญญาอัจฉริยะ (Sabzwari, 2024 p.1)

2.2.3.1 ข้อดีของสัญญาอัจฉริยะ

1) ความเป็นอิสระและการลดต้นทุน: ความต้องการคนกลาง เช่น นายหน้า ตัวแทน และนักกฎหมาย ไม่จำเป็นอีกต่อไป เนื่องจากสัญญาอัจฉริยะจะทำให้ธุรกรรมเป็นแบบอัตโนมัติและลดต้นทุนที่เกี่ยวข้องกับธุรกรรม ความเป็นอิสระนี้รับประกันได้ว่าธุรกรรมจะดำเนินการได้รวดเร็วยิ่งขึ้น และไม่มีความเป็นไปได้ที่จะเกิดอคติหรือข้อผิดพลาดที่เกิดจากบุคคลที่สาม

2) ความน่าเชื่อถือและโปร่งใส: สัญญาอัจฉริยะให้ความโปร่งสที่ไม่มีใครเทียบได้เมื่อมีการนำไปใช้บนแพลตฟอร์มแบบกระจายอำนาจ เนื่องจากทุกธุรกรรมได้รับการลงทะเบียนบนบล็อกเชน จึงสามารถตรวจสอบได้ทันทีและยังคงไม่สามารถเปลี่ยนแปลงได้ การเปิดกว้างนี้ส่งเสริมความไว้วางใจและลดความเป็นไปได้ของความขัดแย้งโดยรับประกันว่าทุกฝ่ายจะสามารถเข้าถึงข้อมูลเดียวกันได้

3) ประสิทธิผลและความปลอดภัย: สัญญาอัจฉริยะมีความปลอดภัยสูง ด้วยการใช้เทคโนโลยีการเข้ารหัสที่ป้องกันการเข้าถึงและการฉ้อโกงโดยไม่ได้รับอนุญาต ได้รับการตั้งโปรแกรมในลักษณะที่จะดำเนินการเมื่อตรงตามเงื่อนไขบางประการ ช่วยประหยัดเวลาและความพยายามในการประมวลผลธุรกรรม

4) การเข้าถึงทั่วโลก: เทคโนโลยีบล็อกเชนที่พร้อมใช้งานทั่วโลกขับเคลื่อนการดำเนินการสัญญาอัจฉริยะ เนื่องจากมีการเข้าถึงทั่วโลก ธุรกิจต่าง ๆ จึงสามารถดำเนินการค้าขายข้ามพรมแดนได้โดยปราศจากความไม่สะดวกและค่าใช้จ่ายจากการทำธุรกรรมข้ามพรมแดนแบบเดิม ๆ

2.2.3.2 ข้อเสียของสัญญาอัจฉริยะ

1) ข้อผิดพลาดและข้อจำกัดทางเทคนิค: ความไม่ถูกต้องและช่องโหว่ในชุดคำสั่งพื้นฐานของสัญญาอัจฉริยะสามารถถูกนไปใช้ประโยชน์ได้อย่างง่ายดาย หากไม่มีการตรวจสอบที่เหมาะสม ข้อผิดพลาดใด ๆ ที่มีอยู่ ณ เวลาที่ปรับใช้อาจไม่สามารถย้อนกลับได้ เนื่องจากเมื่อมีการปรับใช้สัญญาบนบล็อกเชนจะเป็นการเปลี่ยนแปลงได้ยาก

2) การเปลี่ยนแปลงทางกฎหมายและข้อบังคับ: สัญญาอัจฉริยะยังอยู่ในวัยทารกในฐานะเครื่องทางกฎหมาย เนื่องจากอาจไม่ถือว่ามีผลผูกพันทางกฎหมายในทุกประเทศเสมอไป ฝ่ายที่ขึ้นอยู่กับสัญญาอัจฉริยะสำหรับธุรกรรมขนาดใหญ่อาจมีความเสี่ยงจากการขาดกรอบการกำกับดูแลที่ชัดเจน

3) ปัญหาเรื่องความสามารถในการปรับขนาดและประสิทธิภาพ: ด้วยแพลตฟอร์มบล็อกเชน โดยเฉพาะแพลตฟอร์มอย่างอีเธอเรียมสามารถส่งผลต่อการทำงานของสัญญาอัจฉริยะได้ ความล่าช้าในการประมวลผล ค่าธรรมเนียมการทำธุรกรรมที่สูงขึ้น และความแออัดของเครือข่ายอาจเป็นผลมาจากปริมาณธุรกรรมที่สูง

4) ความเข้าใจผิดและความสงสัยของผู้ใช้: เทคโนโลยีบล็อกเชนและสัญญาอัจฉริยะอาจดูเข้าใจยากสำหรับผู้ใช้ที่ไม่มีความรู้ด้านเทคนิค ซึ่งนำไปสู่ความสับสน ความสงสัย และความเข้าใจผิด ในอุตสาหกรรมที่อาจได้รับประโยชน์อย่างมากจากสัญญาอัจฉริยะ การขาดความเข้าใจนี้อาจขัดขวางการยอมรับและทำให้นวัตกรรมช้าลง

2.3 ภาษาซอลิดิตี (Solidity Language)

ซอลิดิตี เป็นภาษาเชิงวัตถุระดับสูงที่พัฒนาขึ้นโดยเฉพาะสำหรับการสร้างและใช้งานสัญญาอัจฉริยะบนแพลตฟอร์มการพัฒนาบล็อกเชนต่าง ๆ โดยเฉพาะอีเธอเรียมซอลิดิตี (Ethereum Solidity) ได้รับการพัฒนาขึ้นครั้งแรกในปีพ.ศ. 2557 โดย Gavin Wood และได้รับความสนใจจากธุรกิจที่ต้องการเปลี่ยนจากสัญญาแบบเดิมเป็นสัญญาแบบอัจฉริยะ ซอลิดิตีเป็นภาษาที่ได้รับอิทธิพลมาจากภาษา C++ Python และ JavaScript ที่สำคัญเลยก็คือเป็นการพิมพ์แบบคงที่ (Statically typed) รองรับการสืบทอด ไลบรารี และประเภทที่ผู้ใช้กำหนดที่ซับซ้อนท่ามกลางคุณสมบัติอื่น ๆ และเป็นภาษาแบบเชิงวัตถุ (Object Oriented Programming – OOP) เพราะว่ามีคุณสมบัติของการสืบทอดและการทำโครงสร้างเป็นต้น การเขียนด้วยภาษาซอลิดิตีทำให้สามารถสร้างสัญญาสำหรับการใช้งานต่าง ๆ ได้เช่น การลงคะแนน การระดมทุน การประมูลของคนพิการทางสายตา การซื้อระยะไกลที่ปลอดภัย และกระเป๋าเงินแบบหลายลายเซ็น (Bauer, 2022, pp.13-16)

ในขั้นพื้นฐานที่สุด สัญญาอัจฉริยะซอลิดิตี (Solidity Smart Contracts) ช่วยให้ทำธุรกรรมดิจิทัลที่มีความปลอดภัยสูงซึ่งจะไม่เกี่ยวข้องกับคนกลาง สัญญาอัจฉริยะถูกรวมเข้ากับเทคโนโลยีบล็อกเชน ทำให้สามารถตรวจสอบย้อนกลับได้ โปร่งใส ย้อนกลับไม่ได้และในทันที ประมาณ 90% ของการพัฒนาสัญญาอัจฉริยะของโลกเสร็จสิ้นด้วยซอลิดิตี ซอลิดิตีเป็นภาษาการเขียนโปรแกรม

หลักสำหรับการพัฒนาสัญญาอัจฉริยะบนบล็อกเชนอีเธอเรียมซึ่งเป็นบล็อกเชนที่ได้รับความนิยมเป็นอันดับสอง เนื่องจากเป็นโอเพนซอร์ส ทุกคนจึงสามารถใช้อีเธอเรียมเป็นแพลตฟอร์มทางเลือกสำหรับการสร้างและใช้งานสัญญาอัจฉริยะ

ในปัจจุบัน มีสัญญาอัจฉริยะที่กว่า 2.5 ล้านรายการ ซอลิดิตีจึงเป็นภาษายอดนิยมที่สุดสำหรับการพัฒนาสัญญาอัจฉริยะ ทั้ง Ethereum, Tron, Polygon, BNB, Optimism และเชน หรือโพรโทคอล อื่น ๆ อีก 30 รายบน EVM ที่ใช้ภาษาซอลิดิตี โดยปกติแล้วการตรวจสอบคริปโตส่วนใหญ่จะทำในซอลิดิตี

2.4 ภาษาไพทอนและไลบรารี่ Scikit-learn (Python and Scikit-learn)

ไพทอนเป็นภาษาโปรแกรมระดับสูงสำหรับใช้งานทั่วไปซึ่งกลายเป็นแกนนำในโลกการพัฒนาซอฟต์แวร์ เนื่องจากสามารถอ่านได้และมีไวยากรณ์ที่ตรงไปตรงมา ออกแบบโดย Guido Van Rossum และเปิดตัวครั้งแรกในปีพ.ศ. 2534 ปรัชญาการออกแบบของไพทอน คือ เน้นความสามารถในการอ่านชุดคำสั่งด้วยการใช้ช่องว่างที่สำคัญอย่างน่าทึ่ง ช่วยให้นักพัฒนาสามารถแสดงแนวคิดด้วยชุดคำสั่งจำนวนบรรทัดที่น้อยกว่าเมื่อเทียบกว่าภาษาต่าง ๆ เช่น C++ หรือ Java (Gowrishankar & Veena, 2019, p. 7)

ภาษามีการพิมพ์แบบไดนามิก และรวบรวมขยะซึ่งหมายความว่าได้รับการออกแบบให้มีความยืดหยุ่นและใช้งานง่าย ไพทอนรองรับกลไกการเขียนโปรแกรมหลายรูปแบบรวมถึงการเขียนโปรแกรมแบบมีโครงสร้างเชิงวัตถุและเชิงฟังก์ชัน ทำให้มีความหลากหลายอย่างไม่น่าเชื่อสำหรับแอปพลิเคชันที่หลากหลาย ตั้งแต่การพัฒนาเว็บและระบบอัตโนมัติ ไปจนถึงการประมวลผลทางวิทยาศาสตร์และการวิเคราะห์ข้อมูลไลบรารี่มาตรฐานที่กว้างขวางของไพทอน และระบบนิเวศที่ใหญ่กว่าของโปรแกรมสำเร็จจากภายนอก ทำให้สามารถจัดการกับงานการเขียนโปรแกรมแทบทุกอย่างได้

Scikit-learn หรือที่รู้จักในชื่อ Sklearn เป็นไลบรารี่การเรียนรู้ของเครื่องแบบโอเพนซอร์สสำหรับไพทอน ซึ่งขึ้นชื่อเรื่องความเรียบง่ายและมีประสิทธิภาพ ถูกพัฒนาโดย David Cournapeau ในฐานะโครงการกูเกิ้ลฤดูร้อนของรหัส (Google Summer of Code Project) ในปีพ.ศ. 2550 (Maker, 2019, p. 1) Sklearn สร้างขึ้นมาจากรากฐานของไลบรารี่ไพทอนอีกสองไลบรารี่ได้แก่ NumPy และ SciPy และมุ่งเน้นไปที่การสร้างแบบจำลองข้อมูล ไม่ใช่การโหลด การจัดการ และการสรุปข้อมูล เป็นหนึ่ง

ในเครื่องมือที่ต้องการมากที่สุดในการเรียนรู้ของเครื่อง สำหรับการดำเนินการเรียนรู้ทั้งแบบมีผู้สอนและไม่มีผู้สอน Scikit-learn มาพร้อมกับอัลกอริทึมมากมายสำหรับการสร้างแบบจำลองที่ซับซ้อนและการทำนายด้วยข้อมูลรวมถึงการจำแนกประเภท การถดถอย การจัดกลุ่ม และการลดขนาด ส่วนเชื่อมต่อประสานที่สอดคล้องกันและเอกสารประกอบที่ครอบคลุมช่วยให้ผู้เริ่มต้นสามารถเข้าถึงได้สูงแต่ยังคงมีประสิทธิภาพเพียงพอสำหรับการปรับใช้ขนาดใหญ่และการปรับแต่งที่ซับซ้อนสำหรับผู้เชี่ยวชาญในสาขานั้น (Kaul, 2024, p. 1)

ไพทอนและ Scikit-learn ร่วมกันนำเสนอชุดเครื่องมือที่ทรงพลังและครอบคลุมสำหรับทุกคนที่ต้องการเจาะลึกในการวิเคราะห์ข้อมูลและการเรียนรู้ของเครื่อง และการคำนวณทางวิทยาศาสตร์ โดยให้การผสมผสานระหว่างความสะดวกในการใช้งานและความยืดหยุ่นที่ยากจะเทียบได้ในโลกของการเขียนโปรแกรมและวิทยาศาสตร์ข้อมูล

2.4.1 แอปพลิเคชันของไพทอน:

ไพทอนเป็นผู้นำด้านนวัตกรรมการเรียนรู้ของเครื่อง วิทยาศาสตร์ข้อมูล และปัญญาประดิษฐ์ นอกจากนี้แอปพลิเคชันไพทอนยังช่วยให้สร้างแอปหลากหลาย กระบวนการพัฒนาเว็บและอื่น ๆ อีกมากมายได้อย่างง่ายดาย ตัวอย่าง 10 อันดับแรกของแอปพลิเคชันไพทอน (GeeksforGeeks, 2024, p. 1) ได้แก่

2.4.1.1 การพัฒนาเว็บ: เป็นหนึ่งในแอปพลิเคชันที่น่าทึ่งที่สุดของไพทอน เนื่องจากไพทอนมีกรอบการทำงานที่หลากหลาย เช่น Django, Flask, Bottle และอีกมากมายที่ช่วยให้นักพัฒนาสะดวก นอกจากนี้ไพทอนยังมีไลบรารีและเครื่องมือในตัวที่ทำให้กระบวนการพัฒนาเว็บเป็นเรื่องง่ายอย่างสมบูรณ์ การใช้ไพทอนสำหรับการพัฒนาเว็บยังนำเสนอในส่วนของ การสร้างภาพที่น่าทึ่ง ความสะดวกสบายในการพัฒนา การรักษาความปลอดภัยชั้นสูง และ กระบวนการพัฒนาที่รวดเร็ว

2.4.1.2 การเรียนรู้ของเครื่องและปัญญาประดิษฐ์: การเรียนรู้ของเครื่องและปัญญาประดิษฐ์เป็นวิชาที่ร้อนแรงที่สุดในขณะนี้ ไพทอนพร้อมด้วยไลบรารีและเครื่องมือในตัวช่วยอำนวยความสะดวกในการพัฒนาอัลกอริทึมปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง นอกจากนี้ ยังมีชุดคำสั่งที่เรียบง่าย กระชับ และอ่านง่าย ซึ่งช่วยให้นักพัฒนาเขียนอัลกอริทึมที่ซับซ้อนได้ง่ายขึ้น และมอบการไหลที่หลากหลาย ไลบรารี่และเครื่องมือในตัวบางส่วนที่ปรับปรุงกระบวนการการเรียนรู้

ของเครื่องและปัญญาประดิษฐ์ ได้แก่ Numpy, Keras, SciPy และ Seabon

2.4.1.3 วิทยาศาสตร์ข้อมูล: วิทยาศาสตร์ข้อมูลเกี่ยวข้องกับการรวบรวมข้อมูล การเรียงลำดับข้อมูล การวิเคราะห์ข้อมูล และการแสดงภาพข้อมูล ไพทอนมีฟังก์ชันการทำงานในการจัดการกับสถิติและการคำนวณทางคณิตศาสตร์ที่ซับซ้อน การมีไลบรารี่เป็นตัวช่วยเพิ่มความสะดวกให้กับผู้เชี่ยวชาญด้านวิทยาศาสตร์ข้อมูล ไลบรารียอดนิยมบางตัวที่อำนวยความสะดวกในกระบวนการวิทยาศาสตร์ข้อมูล ได้แก่ TensorFlow, Pandas และ Socket Learning ไลบรารีเหล่านี้จัดเตรียมระบบนิเวศสำหรับการปรับแต่งแบบจำลองข้อมูล การประมวลผลข้อมูลล่วงหน้า และดำเนินการวิเคราะห์ข้อมูลที่ซับซ้อน

2.4.1.4 การพัฒนาเกม: ด้วยอุตสาหกรรมเกมที่เติบโตอย่างรวดเร็ว ไพทอนได้พิสูจน์แล้วว่าเป็นตัวเลือกที่ยอดเยี่ยมสำหรับการพัฒนาเกม เกมยอดนิยมเช่น Pirates of the Caribbean, Bridge Commander และ Battlefield 2 ใช้การเขียนโปรแกรมไพทอน สำหรับฟังก์ชันและส่วนเสริมที่หลากหลาย การมีอยู่ของไลบรารีเกม 2 มิติ และ 3 มิติยอดนิยมเช่น pygame, panda3D และ Cocos2D ทำให้กระบวนการพัฒนาเกมเป็นเรื่องง่ายอย่างสมบูรณ์

2.4.1.5 แอปพลิเคชันเสียงและภาพ: แอปพลิเคชันเสียงและวิดีโอถือเป็นคุณสมบัติที่น่าทึ่งที่สุดของไพทอนอย่างไม่ต้องสงสัย ไพทอนมีเครื่องมือและไลบรารีมากมายเพื่อช่วยให้งานสำเร็จได้อย่างไร้ที่ติ แอปพลิเคชันที่เข้ารหัสด้วยไพทอน รวมถึงแอปพลิเคชันยอดนิยมเช่น Netflix, Spotify และ YouTube สิ่งนี้สามารถจัดการได้โดยไลบรารีเช่น Dejavu, Pyo, Mingus, SciPy และ OpenCV

2.4.1.6 การพัฒนาซอฟต์แวร์: ไพทอนเป็นเพียงตัวเลือกที่สมบูรณ์แบบสำหรับการพัฒนาซอฟต์แวร์ แอปพลิเคชันยอดนิยมอย่าง Google, Netflix และ Reddit ต่างก็ใช้ไพทอน ภาษานี้มีคุณสมบัติที่น่าทึ่งเช่น ความเป็นอิสระของแพลตฟอร์ม มีไลบรารีและเฟรมเวิร์กในตัวเพื่อให้ง่ายต่อการพัฒนา ปรับปรุงการนำชุดคำสั่งกลับมาใช้ใหม่และอ่านง่าย ความเข้ากันได้สูง นอกเหนือจากไพทอนเหล่านี้แล้ว ยังมีคุณลักษณะที่ได้รับการปรับปรุงเพื่อทำงานร่วมกับเทคโนโลยีที่เติบโตอย่างรวดเร็ว เช่น การเรียนรู้ของเครื่องและปัญญาประดิษฐ์

2.4.1.7 แอปพลิเคชัน CAD: CAD หมายถึงการออกแบบโดยใช้คอมพิวเตอร์ช่วยเป็นกระบวนการสร้างแบบจำลอง 3 มิติ และ 2 มิติในรูปแบบดิจิทัล แอปพลิเคชันนี้ได้เข้ามาแทนการดริฟท์ด้วยมือ และถูกใช้โดยสถาปนิก นักออกแบบผลิตภัณฑ์ และผู้จัดการฝ่ายก่อสร้าง เพื่อออกแบบผลิตภัณฑ์ที่มีความสม่ำเสมอสูงมาก ไพทอนถูกฝังอยู่ในแอปพลิเคชันที่น่าทึ่งเช่น Blender, FreeCAD, Open Cascade และอื่น ๆ อีกมากมายเพื่อการออกแบบผลิตภัณฑ์อย่างมีประสิทธิภาพ สิ่งเหล่านี้มอบคุณสมบัติที่ได้รับการปรับปรุง เช่น การวดภาพทางเทคนิค การพัฒนาระบบไดนามิก การบันทึก การ

ส่งออกไฟล์ และการนำเข้า

2.4.1.8 การใช้งานทางธุรกิจ: ไพทอนนำเสนอคุณสมบัติด้านความปลอดภัยและความสามารถในการปรับขนาดที่ยอมเยี่ยม ซึ่งทำให้สมบูรณ์แบบสำหรับการส่งมอบแอปพลิเคชันทางธุรกิจที่มีประสิทธิภาพสูง มีไลบรารีและเครื่องมือในตัวเช่น Odoo และ Tryton คุณสมบัติที่โดดเด่นทั้งหมดนี้ทำให้เหมาะสำหรับการสร้างแอปพลิเคชันทางธุรกิจ

2.4.1.9 ส่วนต่อประสานกราฟิกกับผู้ใช้ที่ออกแบบมาสำหรับคอมพิวเตอร์: ไพทอนเป็นภาษาโปรแกรมเชิงโต้ตอบที่ช่วยให้นักพัฒนาสร้าง GUI ได้อย่างง่ายดายและมีประสิทธิภาพ มีรายการเครื่องมือในตัวมากมายสำหรับการใช้งานไพทอน ได้แก่ PyQT, kivy, wxWidgets และไลบรารีอื่น ๆ อีกมากมายที่คล้ายกันเพื่อสร้าง GUI ที่ทำงานได้อย่างสมบูรณ์ในลักษณะที่ปลอดภัยและมีประสิทธิภาพอย่างยิ่ง

2.4.1.10 แอปพลิเคชันขูดเว็บ: การขูดเว็บเป็นกระบวนการอัตโนมัติที่ใช้ในการดึงข้อมูลจากเว็บไซต์ด้วยวิธีที่ง่ายและรวดเร็วยิ่งขึ้น ข้อมูลนี้ถูกใช้โดยนักวิจัย องค์กร และนักวิเคราะห์สำหรับงานที่หลากหลาย ไพทอนมีคุณสมบัติมากมายที่ทำให้เหมาะสำหรับการขูดเว็บ บางส่วนได้แก่ ไวยากรณ์ที่กระชับช่วยเพิ่มความสามารถในการอ่านและช่วยคุณประหยัดเวลา ไลบรารีและเครื่องมือที่หลากหลาย เช่น Pandas, Matplotlib และ Selenium ทำให้กระบวนการขูดเว็บง่ายและมีประสิทธิภาพใช้งานง่ายและเข้าใจง่าย

2.4.2 ข้อดีข้อเสียของภาษาไพทอน: (Kumari, 2024, p. 1)

2.4.2.1 ข้อดีของภาษาไพทอน

1) ง่ายต่อการเรียนรู้และการใช้งาน: ไวยากรณ์ง่าย ๆ ของไพทอนสะท้อนภาษามนุษย์อย่างใกล้ชิด ทำให้เรียนรู้และเข้าใจได้ง่ายเป็นพิเศษ ความง่ายดายนี้กระตุ้นให้ผู้คนหันมาสนใจการเขียนโปรแกรมมากขึ้น ช่วยลดขั้นตอนการเรียนรู้ลงอย่างมาก

2) ไลบรารีและกรอบการทำงานที่กว้างขวาง: ไพทอนมีระบบนิเวศที่กว้างขวางของไลบรารีและกรอบการทำงาน เช่น Django สำหรับการพัฒนาเว็บ, Pandas สำหรับการวิเคราะห์ข้อมูล และ TensorFlow สำหรับการเรียนรู้ของเครื่อง เครื่องมือเหล่านี้ช่วยลดเวลาที่ต้องใช้ในการพัฒนาแอปพลิเคชันที่ซับซ้อนได้อย่างมาก

3) การสนับสนุนชุมชน: ไพทอนมีชุมชนการเขียนโปรแกรมที่ใหญ่ที่สุดแห่งหนึ่ง ชุมชนที่มีชีวิตชีวาแห่งนี้นำเสนอทรัพยากร บทช่วยสอนและฟอรัมที่กว้างขวางซึ่งนักพัฒนาสามารถค้นหาคำตอบและแบ่งปันความรู้

4) ความเก่งกาจ: ตั้งแต่เว็บแอปพลิเคชันไปจนถึงการวิเคราะห์ข้อมูลและการเรียนรู้ของเครื่อง ไพทอนมีอยู่ทุกที่ ความคล่องตัวทำให้สามาถนำไปใช้งานในโดเมนต่าง ๆ ช่วยเพิ่มความยืดหยุ่นของนักพัฒนาในตลาดงาน

5) ผลผลิตที่ได้รับการปรับปรุง: ไวยากรณ์ที่ตรงไปตรงมาและไลบรารีอันทรงพลังของไพทอนช่วยให้นักพัฒนาสามารถทำงานได้มากขึ้นโดยใช้ชุดคำสั่งน้อยลง เมื่อเทียบกับภาษาการเขียนโปรแกรมอื่น ๆ มากมาย ซึ่งช่วยเพิ่มประสิทธิภาพการทำงาน

6) การตีความ: ไพทอนเป็นภาษาที่ตีความ ซึ่งหมายความว่าชุดคำสั่งสามารถทำงานได้ทันทีที่เขียน ช่วยให้สามารถทดสอบและแก้ไขข้อบกพร่องได้อย่างรวดเร็ว ทำให้การพัฒนาซ้ำราบรื่นยิ่งขึ้น

7) ความสามารถในการบูรณาการ: ไพทอนสามารถรวมเข้ากับภาษาการเขียนโปรแกรมอื่น ๆ เช่น C, C++ หรือ Java ได้อย่างง่ายดาย ทำให้มีแอปพลิเคชันที่มีประสิทธิภาพมากขึ้นและใช้เครื่องมือที่เหมาะสมสำหรับงานที่เหมาะสม

8) โอเพ่นซอร์สพร้อมการพัฒนาที่กระตือรือร้น: เนื่องจากเป็นโอเพ่นซอร์ส ไพทอนจึงสามารถใช้งานได้ฟรีและได้รับการปรับปรุงอย่างต่อเนื่องโดยชุมชนนักพัฒนาทั่วโลก เพื่อให้มั่นใจว่าจะยังคงมีความเกี่ยวข้องและมีประสิทธิภาพ

9) การพกพา: โดยทั่วไปโปรแกรมไพทอนจะไม่ขึ้นอยู่กับแพลตฟอร์ม ชุดคำสั่งที่เขียนบนแพลตฟอร์มอื่น ๆ แทบทุกชนิด ทำให้เหมาะสำหรับการพัฒนาข้ามแพลตฟอร์ม

10) ฝังและขยายได้: ชุดคำสั่งไพทอนสามารถฝังลงในโปรแกรม C/C++ เพื่อให้มีความสามารถในการเขียนสคริปต์สำหรับผู้ใช้โปรแกรม หรือเพื่อปรับปรุงประสิทธิภาพโดยการขยายไพทอนด้วยมอดูล C/C++

2.4.2.2 ข้อเสียของภาษาไพทอน

1) ข้อจำกัดความเร็ว: ไพทอนเป็นภาษาที่ตีความ ซึ่งอาจส่งผลให้การดำเนินการล่าช้าลง เมื่อเทียบกับภาษาที่คอมไพล์ เช่น C หรือ C++ ความเร็วที่ช้าลงนี้อาจเป็นอุปสรรคเมื่อประสิทธิภาพมีความสำคัญ เช่น ในการเล่นเกมหรือแอปพลิเคชันการซื้อขายที่มีความถี่สูง

2) การใช้หน่วยความจำ: ความยืดหยุ่นและความสะดวกในการใช้งานของไพทอนมาพร้อมกับค่าใช้จ่ายในแง่ของการใช้หน่วยความจำ โดยทั่วไปโปรแกรมไพทอนจะใช้หน่วยความจำมากกว่าโปรแกรมที่เขียนในภาษาอื่น เช่น Java หรือ C++

3) ข้อผิดพลาดขณะรันโปรแกรม: เนื่องจากลักษณะแบบไดนามิกของไพทอนจึงมีแนวโน้มที่จะเกิดข้อผิดพลาดขณะรันโปรแกรม ข้อผิดพลาดที่อาจพบได้ในระหว่างขั้นตอน

มหาวิทยาลัยรังสิต Rangsit University

การคอมไพล์ในภาษาอื่นมักจะตรวจพบได้ที่ขณะรันโปรแกรมในไพทอนเท่านั้น

4) ข้อจำกัดของการประมวลผลบนอุปกรณ์พกพา: โดยทั่วไปแล้วไพทอนไม่ได้ใช้ในการพัฒนาบนอุปกรณ์พกพา ภาษาอื่น ๆ เช่น Swift สำหรับ iOS และ Java สำหรับ Android ครองแอปพลิเคชันบนอุปกรณ์พกพา ซึ่งจำกัดบทบาทของไพทอนในระบบนิเวศอุปกรณ์พกพา

5) การเข้าถึงฐานข้อมูล: เมื่อเปรียบเทียบกับเทคโนโลยีอื่น ๆ ชั้นของการเข้าถึงฐานข้อมูลของไพทอนยังด้อยพัฒนาและยังไม่สมบูรณ์ สิ่งนี้อาจทำให้ไม่เหมาะกับแอปพลิเคชันที่ต้องการการโต้ตอบที่ซับซ้อนและมีปริมาณมากกับฐานข้อมูล

6) การแลกเปลี่ยยความเรียบง่าย: ความเรียบง่ายของไพทอนบางครั้งอาจเป็นอุปสรรคได้ ตัวอย่างเช่น การใช้การเยื้องเพื่อกำหนดบล็อคชุดคำสั่งในขณะที่ทำความสะอาดชุดคำสั่ง อาจทำให้เกิดข้อผิดพลาดได้หากไม่ได้รับการจัดการอย่างระมัดระวัง

7) การสนับสนุนที่จำกัดสำหรับการดำเนินการพร้อมกันและแบบขนาน: ไพทอนไม่สามารถจัดการการดำเนินการพร้อมกันและแบบขนานได้อย่างมีประสิทธิภาพเท่ากับภาษาอื่น ๆ บางภาษา ตัวล็อกอินเทอร์พรีเตอร์ระดับโลก (The Global Interpreter Lock - GIL) ในไพทอนหมายความว่าสามารถดำเนินการได้ครั้งละหนึ่งเธรดเท่านั้น ทำให้มีประสิทธิภาพน้อยลงสำหรับงานที่เชื่อมโยงกับหน่วยประมวลผลกลาง

8) การจัดการแพ็คเกจ: แม้ว่าไพทอนจะมีระบบนิเวศของแพ็คเกจที่หลากหลาย แต่การจัดการแพ็คเกจเหล่านี้และการขึ้นต่อกันของแพ็คเกจเหล่านี้อาจมีความยุ่งยากในบางครั้งโดยเฉพาะในโครงการขนาดใหญ่

9) ระบบประเภท: ระบบประเภทของไพทอนมีการพิมพ์แบบไดนามิก ซึ่งหมายความว่าประเภทจะถูกกำหนด ณ ขณะรันโปรแกรม สิ่งนี้สามารถนำไปสู่จุดบกพร่องที่ยากต่อการแก้ไข และอาจทำให้ชุดคำสั่งคาดเดาได้น้องลง

10) ไม่ใช่ภาษาหลักของเบราว์เซอร์: ไพทอนไม่มีการสนับสนุนหลักในเว็บเบราว์เซอร์ ซึ่งแตกต่างจาก JavaScript นี่เป็นการจำกัดการใช้งานในการพัฒนาเว็บส่วนหน้า โดยที่ JavaScript ยังคงเป็นราชาของการเขียนโปรแกรมบนเว็บ

2.5 การจัดการความยินยอม (Consent Management)

การจัดการความยินยอม เป็นกระบวนการขอความยินยอมจากผู้ใช้และอนุญาตให้ผู้ใช้จัดการข้อมูลที่แชร์และวัตถุประสงค์ของการแชร์ การจัดการความยินยอมมีทั้งนโยบายที่นำมาใช้ในการจัดการความยินยอมของผู้ใช้และการใช้งานทางเทคนิคที่ช่วยให้ผู้ใช้ตัดสินใจเกี่ยวกับวิธีการรวบ

รวมหรือใช้ข้อมูลของตน

กุญแจสำคัญของกรอบการจัดการความยินยอม คือ การปฏิบัติความเป็นส่วนตัวของข้อมูลที่มีอยู่ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ปีพ.ศ. 2559 หรือจีดีพีอาร์ (General Data Protection Regulation - GDPR) พระราชบัญญัติความเป็นส่วนตัวของผู้บริโภคแคลิฟอร์เนีย ปี พ.ศ. 2561 หรือซีซีพีเอ (California Consumer Privacy Act - CCPA) ทั้งคู่ควบคุมวิธีการประมวลผลและถ่ายโอนข้อมูลส่วนบุคคล พวกเขาเริ่มเคลื่อนไหวอย่างกว้างขวางเพื่อให้บริษัทต่าง ๆ นำไปปฏิบัติและปฏิบัติตามการจัดการความยินยอม เนื่องจากการไม่ปฏิบัติตามอาจ (และมี) ส่งผลให้เกิดค่าปรับและการลงโทษอย่างร้ายแรง สำหรับประเทศไทยได้นำจีดีพีอาร์ของสหภาพยุโรปมาเป็นต้นแบบและปรับให้เหมาะสม จนออกมาเป็นข้อกฎหมายที่ชื่อว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ พีดีพีเอ (Personal Data Protection Act - PDPA)

2.5.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือพีดีพีเอ (Personal Data Protection Act - PDPA) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมายพีดีพีเอ ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 และได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน พ.ศ. 2565 (ราชกิจจานุเบกษา, 2562, น. 52-95)

สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่บังคับใช้นี้ สิ่งหนึ่งที่ทำให้องค์กรหรือหน่วยงานต่าง ๆ เริ่มจัดดำเนินการ คงหนีไม่พ้นเรื่องของความยินยอม (Consent) ที่ได้ระบุไว้ในพีดีพีเอ มาตรา 19 ความว่า

> ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้ (ราชกิจจานุเบกษา, 2562, น. 60)

มหาวิทยาลัยรังสิต Rangsit University

2.5.1.1 ประเภทของข้อมูลส่วนบุคคล (Personal Data Type)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ข้อมูลส่วนบุคคล คือ ชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือแม้กระทั่งวันเกิดของบุคคลหนึ่ง ๆ ซึ่งให้ความหมายในทางกฎหมาย ว่า ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าจะทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ โดยข้อมูลส่วนบุคคลสามารถแบ่ง ประเภทของข้อมูลส่วนบุคคลได้ดังนี้ (วันพิชิต ชินตระกูลชัย, 2564, น. 1)

1) ข้อมูลส่วนบุคคลทั่วไป (Personal Data) เป็นข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม อาทิเช่น ชื่อ-นามสกุล หรือชื่อเล่น / เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล) / ที่อยู่ อีเมล เบอร์โทรศัพท์ / ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น เลขที่อยู่ไอพี และรหัสประจำตัวของอุปกรณ์ / ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน / ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด เชื้อชาติ สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลการแพทย์ ข้อมูลการศึกษา ข้อมูลการเงิน ข้อมูลการจ้างงาน / ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ / ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง / ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล / ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต เป็นต้น

2) เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เป็นข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลทางชีวมิติ (รูปภาพใบหน้า ลายนิ้วมือ ฟิล์มเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม เป็นต้น หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด ซึ่ง พ.ร.บ. ฉบับนี้ให้ความสำคัญและมีบทลงโทษที่รุนแรงด้วยกรณีเกิดการรั่วไหลสู่สาธารณะ

การขอความยินยอม (Consent) ให้ถูกต้องตามหลักพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามกฎหมายได้ระบุไว้ว่า “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลและพูด

ให้ชัดคือองค์กรห้ามใช้ข้อมูลหรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากลูกค้าหรือเจ้าของข้อมูลก่อน”

2.5.1.2 สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามสิทธิต่าง ๆ ทั้งนี้ตามหลักเกณฑ์และเงื่อนไขที่กฎหมายบัญญัติไว้ ดังนี้ (ศูนย์ข้อมูลภาครัฐเพื่อประชาชน, 2022, น. 1)

1) สิทธิได้รับการแจ้งให้ทราบ: การเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบ รวมข้อมูลส่วนบุคคล (ยกเว้นเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว) โดยมีรายละเอียดการแจ้งให้ทราบ เช่น เก็บข้อมูลส่วนบุคคลอะไรบ้าง วัตถุประสงค์การเก็บข้อมูล การนำไปใช้หรือส่งต่อไปมีให้ใครบ้าง เก็บข้อมูลอย่างไร เก็บข้อมูลนานแค่ไหน วิธีขอการเปลี่ยนแปลงแก้ไข เพิกถอนข้อมูลส่วนบุคคลที่ให้ไปสามารถทำได้อย่างไรบ้าง

2) สิทธิขอเข้าถึงข้อมูลส่วนบุคคล: เจ้าของข้อมูลส่วนบุคคล มีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมได้ โดยสิทธินี้จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล หรือส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น ถ้าไม่ขัดหรือส่งผลกระทบดังกล่าว เจ้าของข้อมูลส่วนบุคคลจะได้รับสิทธิ์ภายใน 30 วันนับจากวันที่ผู้ควบคุมข้อมูลส่วนบุคคล ได้รับคำขอ

3) สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล: เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับคนเมื่อใดก็ได้ แต่ต้องไม่ขัดด้วยกฎหมายที่สำคัญยิ่งกว่า หรือขัดต่อสิทธิการเรียกร้องตามกฎหมาย หรือข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

4) สิทธิขอให้ลบหรือทำลาย: กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลสาธารณะ และผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของได้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องรับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเอง

5) สิทธิในการเพิกถอนความยินยอม: ถ้าเจ้าของข้อมูลเคยให้ความยินยอมไปแล้ว ต่อมาภายหลังต้องการยกเลิกความยินยอมนั้น ก็สามารถทำเมื่อใดก็ได้ และการยกเลิกความ

ยินยอมนั้นจะต้องทำได้ง่ายเหมือนกับตอนแรกที่เจ้าของข้อมูลให้ความยินยอมด้วย โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิ์ในการถอนความยินยอมทางกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้

6) สิทธิขอให้ระงับการใช้ข้อมูล: เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคล ไม่ว่าจะในกรณีที่เกิดการเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการเรียกร้องสิทธิก็สามารถทำได้

7) สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล: เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้องเป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริตและไม่ขัดต่อหลักกฎหมาย

8) สิทธิในการขอให้โอนข้อมูลส่วนบุคคล: ในกรณีที่เจ้าของข้อมูลต้องการนำข้อมูลที่เคยให้ไว้กับผู้ควบคุมข้อมูลรายหนึ่ง ไปใช้กับผู้ควบคุมข้อมูลอีกราย เช่น ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกได้จัดทำข้อมูลส่วนบุคคลของเราไปให้อยู่ในรูปแบบต่าง ๆ ที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ เจ้าของข้อมูลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลที่จัดทำข้อมูลนั้น ทำการส่งหรือโอนข้อมูลดังกล่าวให้ได้ หรือจะขอให้ส่งไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นโดยตรงก็สามารถทำได้ หากไม่ติดขัดทางวิธีการและเทคนิค โดยการใช้สิทธินั้นต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของบุคคลอื่น

รูปที่ 2.5 สิทธิของเจ้าของข้อมูลส่วนบุคคล

ที่มา: สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2566

2.5.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation – GDPR) เป็นกฎหมายความเป็นส่วนตัวและความปลอดภัยที่เข้มงวดที่สุดในโลก แม้ว่าสหภาพยุโรปจะเป็นผู้ร่างและส่งต่อ แต่ก็มีข้อผูกมัดกับองค์กรทุกแห่ง ตราบใดที่องค์กรเหล่านั้นกำหนดเป้าหมายหรือรวบรวมข้อมูลที่เกี่ยวข้องกับผู้คนในสหภาพยุโรป จีดีพีอาร์มีผลบังคับใช้ในปี พ.ศ. 2559 หลังผ่านจากสภายุโรปและข้อบังคับนี้มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2561 ที่ทุกองค์กรจำเป็นต้องปฏิบัติตาม ซึ่งจีดีพีอาร์จะเรียกเก็บค่าปรับที่รุนแรงต่อผู้ที่ละเมิดมาตรฐานความเป็นส่วนตัว และความปลอดภัยโดยมีบทลงโทษสูงถึงหลายสิบล้านยูโร (นคร เสรีรักษ์, ฉรงค์ ใจหาญ, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร และ นิชานันท์ นันทศิริศรณ์, 2562, น. 1- 246) ซึ่งมีสาระสำคัญดังรายละเอียดดังนี้

ภายใต้จีดีพีอาร์ ความยินยอมเป็นหนึ่งในพื้นฐานทางกฎหมายของการประมวลข้อมูล ข้อกำหนดข้อที่ 7 ระบุไว้ว่า “ต้องได้รับความยินยอมอย่างอิสระ เฉพาะเจาะจง แจ้งให้ทราบ และไม่กำกวม” สิ่งเหล่ากำหนดให้ต้องได้รับความยินยอมของบุคคลโดยสมัครใจ โดยไม่มีแรงกดดันหรืออิทธิพลใด ๆ ที่อาจส่งผลต่อการเลือกของเขาหรือเธอได้ ยิ่งไปกว่านั้น บุคคลต้องมีความสามารถในการเพิกถอนความยินยอมของคนเมื่อใดก็ได้ โดยไม่มีผลเสียหายใด ๆ การถอนความยินยอมนั้นต้องง่ายเหมือนการให้ความยินยอม

จีดีพีอาร์ ได้กำหนดนิยามของข้อกำหนดทางกฎหมายที่มีความยาว ด้านล่างนี้คือบางส่วนที่สำคัญที่สุดที่กล่าวถึงในในบทความนี้

1) ข้อมูลส่วนบุคคล (Personal Data): ข้อมูลส่วนบุคคล คือ ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลสามารถระบุได้โดยตรงหรือโดยอ้อม ชื่อและที่อยู่อีเมลเป็นข้อมูลส่วนบุคคลอย่างชัดเจน ข้อมูลตำแหน่ง ชาติพันธุ์ เพศ ข้อมูลชีวมิติ ความเชื่อทางศาสนา เว็บคุกกี้ และความคิดเห็นทางการเมือง สามารถเป็นข้อมูลส่วนบุคคลได้เช่นกัน ข้อมูลแฝง (Pseudonymous) อาจอยู่ภายใต้คำจำกัดความได้เช่นกัน ถ้าหากมันค่อนข้างง่ายที่จะระบุตัวตนของใครบางคนจากข้อมูลนั้น

2) การประมวลผลข้อมูล (Data Processing): การดำเนินการใด ๆ กับข้อมูลไม่ว่าจะเป็นอัตโนมัติหรือแบบทำด้วยมือ ตัวอย่างที่อ้างถึงในบทความนี้ ได้แก่ การรวบรวม การบันทึก การจัดระเบียบ โครงสร้าง การจัดเก็บ การใช้งาน การลบ เป็นต้น

3) เจ้าของข้อมูล (Data Subject): บุคคลที่มีการประมวลผลข้อมูล เหล่านี้คือลูกค้าหรือผู้เยี่ยมเว็บไซต์ของเราก็ได้

4) ผู้ควบคุมข้อมูล (Data Controller): บุคคลที่ตัดสินใจว่าข้อมูลส่วนบุคคลจะถูกประมวลผลอย่างไรและทำไม หากคุณเป็นเจ้าของหรือพนักงานในองค์กรที่จัดการข้อมูลนั้นคือหน้าที่นี้เป็นของคุณ

5) ผู้ประมวลผลข้อมูล (Data Processor): คนกลางที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล จีดีพีอาร์มีกฎพิเศษสำหรับบุคคลและองค์กรเหล่านี้ อาจรวม ถึงเครื่องคอมพิวเตอร์แม่ข่ายระบบคลาวด์หรือผู้ให้บริการอีเมล

2.5.2.1 หลักการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principle)

จีดีพีอาร์ได้กำหนดหลักการพื้นฐานไว้ 7 ประการที่ใช้เป็นฐานของข้อบังคับและกฎที่ต้องการปฏิบัติตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคล มีดังนี้

1) ความถูกต้องตามกฎหมาย ความยุติธรรม และความโปร่งใส (Lawfulness, Fairness, and Transparency): เจ้าของข้อมูลจะต้องได้รับการแจ้งให้ทราบอย่างชัดเจนเกี่ยวกับวิธีการใช้ข้อมูล เพื่อให้การประมวลผลต้องถูกต้องตามกฎหมาย ยุติธรรม และโปร่งใส

2) ข้อจำกัดเรื่องวัตถุประสงค์ (Purpose Limitation): สามารถรวบรวมข้อมูลเพื่อวัตถุประสงค์เฉพาะเท่านั้น

3) การลดขนาดข้อมูล (Data Minimization): จำนวนข้อมูลที่รวบรวมจะจำกัดเฉพาะสิ่งที่จำเป็นสำหรับการประมวลผลเฉพาะเท่านั้น

4) ความถูกต้อง (Accuracy): องค์กรที่รวบรวมข้อมูลส่วนบุคคลต้องรับรองความถูกต้องและปรับปรุงให้เป็นปัจจุบัน ข้อมูลจะต้องถูกลบหรือถูกเปลี่ยนแปลงเมื่อเจ้าของข้อมูลได้มีการร้องขอ

5) ข้อจำกัดในการจัดเก็บ (Storage Limitation): ข้อมูลที่รวบรวมจะไม่ถูกเก็บไว้นานเกินความจำเป็นสำหรับวัตถุที่ระบุไว้เท่านั้น

6) ความซื่อสัตย์และการรักษาความลับ (Integrity and Confidentiality): ต้องมีมาตรการป้องกันที่เหมาะสมกับข้อมูลส่วนบุคคล เพื่อให้แน่ใจว่าปลอดภัยและป้องกันการโจรกรรมหรือการใช้งานโดยไม่ได้รับอนุญาต

7) ความรับผิดชอบ (Accountability): ผู้ควบคุมข้อมูลมีหน้าที่รับผิดชอบใน

การแสดงการปฏิบัติตามหลักการของจีดีพีอาร์เหล่านี้ทั้งหมด

2.5.2.2 สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)

จีดีพีอาร์ได้ตระหนักถึงสิทธิความเป็นส่วนตัวใหม่สำหรับเจ้าของข้อมูลไว้ 8 ประการ โดยสามารถสรุปได้ดังนี้

1) สิทธิที่จะได้การแจ้งให้ทราบ (The right to be informed): องค์กรจำเป็นต้องแจ้งให้แต่ละคนทราบว่าข้อมูลใดถูกเก็บรวบรวมใช้งานอย่างไร จะถูกเก็บไว้นานเท่าใด และจะแบ่งปันกับคนกลางหรือไม่ ข้อมูลนี้จะต้องสื่อสารอย่างกระชับและเป็นภาษาธรรมดาทั่วไป

2) สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล (The right to access): แต่ละบุคคลสามารถส่งคำขอเข้าถึงข้อมูลส่วนบุคคลได้ ซึ่งกำหนดให้องค์กรต้องจัดเตรียมสำเนาข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวกับบุคคลดังกล่าว องค์กรจะมีเวลาหนึ่งเดือนในการจัดทำข้อมูลนี้ แม้ว่าจะมีข้อยกเว้นสำหรับคำขอที่ไม่มีมูลความจริงอย่างชัดเจน ซ้ำซาก หรือมากเกินไป

3) สิทธิในการขอให้แก้ไข (The right to rectification): หากแต่ละบุคคลพบว่าข้อมูลที่องค์กรเก็บไว้ไม่ถูกต้องหรือไม่สมบูรณ์ ก็สามารถร้องขอให้ปรับปรุงได้ เช่นเดียวกับสิทธิในการเข้าถึงที่องค์กรมีเวลาเพียงหนึ่งเดือนในการดำเนินการนี้ และมีข้อยกเว้นเดียวกัน

4) สิทธิในการขอให้ลบหรือทำลายข้อมูล (The right to erasure/ The Rights to be forgotten): แต่ละบุคคลสามารถร้องขอให้องค์กรลบข้อมูลของตนได้ในบางกรณี เช่น เมื่อข้อมูลนั้นไม่จำเป็นอีกต่อไป ข้อมูลนั้นถูกประมวลผลโดยมิชอบด้วยกฎหมาย หรือไม่เป็นไปตามหลักกฎหมายที่เก็บรวบรวมอีกต่อไป ซึ่งรวมถึงกรณีที่แต่ละบุคคลถอนความยินยอม สิทธิในการลบเรียกอีกอย่างหนึ่งว่า “สิทธิที่จะถูกลืม (The right to forgotten)”

5) สิทธิในการขอระงับการใช้ข้อมูล (The right to processing): แต่ละบุคคลสามารถร้องขอให้องค์กรจำกัดวิธีการใช้ข้อมูลส่วนบุคคลได้ เป็นอีกทางเลือกหนึ่งในการขอให้ลบข้อมูลและอาจใช้เมื่อแต่ละบุคคลได้มีการโต้แย้งความถูกต้องของข้อมูลส่วนบุคคลของตน นอกจากนี้แต่ละบุคคลยังสามารถใช้สิทธินี้เมื่อพวกเขาไม่ใช้ผลิตภัณฑ์หรือบริการที่ได้รวบรวมไว้อีกต่อไป แต่องค์กรต้องการใช้สิทธินี้เพื่อสร้าง ใช้ หรือปกป้องการเรียกร้องทางกฎหมาย

6) สิทธิในการได้รับและโอนถ่ายข้อมูล (The right to data portability): แต่ละบุคคลได้รับอนุญาตให้ได้รับและใช้ข้อมูลส่วนบุคคลของตนซ้ำได้เพื่อวัตถุประสงค์ของตนเองในบริการต่าง ๆ สิทธินี้ใช้กับข้อมูลส่วนบุคคลที่แต่ละบุคคลได้ให้แก่ผู้ควบคุมข้อมูลโดยมีสัญญาหรือ

ความยินยอมเท่านั้น

7) สิทธิในการคัดค้าน (The right to object): แต่ละบุคคลสามารถคัดค้านการประมวลผลข้อมูลส่วนบุคคลที่รวบรวมด้วยเหตุผลของผลประโยชน์ที่ชอบด้วยกฎหมายหรือการปฏิบัติงานเพื่อประโยชน์/การใช้อำนาจของทางการ องค์กรต้องหยุดการประมวลผลข้อมูล เว้นแต่จะสามารถแสดงเหตุผลที่ถูกต้องตามกฎหมายสำหรับการประมวลผลที่ลบล้างผลประโยชน์ สิทธิ และเสรีภาพของบุคคล นอกจากนี้ยังสามารถปฏิเสธสิทธินี้ได้หากการดำเนินการนั้นมีไว้เพื่อจัดตั้งหรือใช้สิทธิในการป้องกันการเรียกร้องทางกฎหมาย

8) สิทธิที่เกี่ยวข้องกับการตัดสินใจโดยอัตโนมัติรวมถึงการทำโปรไฟล์ (Rights related to automated decision making including profiling): จีดีพีอาร์รวมถึงข้อกำหนดสำหรับการตัดสินใจที่ไม่มีมนุษย์เข้ามาเกี่ยวข้อง เช่น การทำโปรไฟล์ ซึ่งใช้ข้อมูลส่วนบุคคลเพื่อสร้างสมมติฐานที่คำนวณได้เกี่ยวกับบุคคล

2.5.3 สถาปัตยกรรมการจัดการความยินยอม (Consent Management Architecture)

ในเอกสารการวิจัยฉบับนี้ กล่าวถึงบทบาทของการจัดการความยินยอมในบริบทของความเป็นส่วนตัวและการปกป้องข้อมูล โดยเฉพาะอย่างยิ่งในแง่ของกฎระเบียบการปกป้องข้อมูลที่เข้มงวด เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ พีดีพีเอ (Personal Data Protection Act - PDPA) โดยเน้นย้ำถึงความจำเป็นที่องค์กรไม่เพียงต้องได้รับความยินยอมอย่างชัดเจนจากบุคคลก่อนที่จะมีส่วนร่วมในการรวบรวมและประมวลผลข้อมูล แต่ยังต้องสอบตัวตนของบุคคลเหล่านี้ด้วยเพื่อให้แน่ใจว่าข้อมูลถูกต้องตามกฎหมาย และนำเสนอถึงการยอมรับที่เพิ่มขึ้นของเทคโนโลยีบล็อกเชนและสัญญาอัจฉริยะว่าเป็นโซลูชันที่เป็นนวัตกรรมใหม่สำหรับการเพิ่มประสิทธิภาพ ความโปร่งใส และความปลอดภัยของกระบวนการบริหารจัดการความยินยอม สามารถสรุปรายละเอียดได้พอสังเขปดังนี้ (ราชกิจจานุเบกษา, 2562, น. 52-95)

2.5.3.1 ความรับผิดชอบในการจัดการความยินยอม

1) การได้รับความยินยอม: หน้าที่ที่สำคัญที่สุดขององค์กรใด ๆ ที่เกี่ยวข้องกับข้อมูลคือการได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล ซึ่งเกี่ยวข้องกับการแจ้งให้บุคคลทราบเกี่ยวกับข้อมูลที่กำลังรวบรวม วัตถุประสงค์ของการประมวลผลข้อมูล วิธีการใช้หรือแบ่งปัน และใครจะสามารถเข้าถึงข้อมูลดังกล่าวได้ ความยินยอมจะต้องได้รับอย่างอิสระเจาะจง ได้รับแจ้ง และไม่คลุมเครือ ซึ่งสอดคล้องกับหลักการที่กำหนดโดยกฎระเบียบด้านการคุ้มครองข้อมูล

2) การยืนยันและตรวจสอบตัวตน: หลังจากได้รับความยินยอมแล้ว องค์กรต้องรับรองความถูกต้องของเจ้าของข้อมูล การยืนยันและการตรวจสอบตัวตนยังช่วยตอกย้ำความถูกต้องตามกฎหมายของความยินยอมที่ได้รับ เนื่องจากเป็นการยืนยันว่าได้รับความยินยอมจากบุคคลจริงซึ่งมีการรวมรวมและประมวลผลข้อมูล ขั้นตอนนี้มีความสำคัญอย่างยิ่งในการป้องกันการฉ้อโกงและเพื่อให้แน่ใจว่าข้อมูลนั้นสอดคล้องกับบุคคลจริงที่สามารถตรวจสอบได้ เพิ่มชั้นความปลอดภัยและความสมบูรณ์ให้กับกระบวนการจัดการข้อมูล

2.5.3.2 การปฏิบัติตามพีดีพีเอ และเทคโนโลยีเกิดใหม่

1) ความสำคัญของการปฏิบัติตามพีดีพีเอ: พีดีพีเอกำหนดแนวปฏิบัติที่เข้มงวดสำหรับการจัดการข้อมูลส่วนบุคคล โดยเน้นการปกป้องสิทธิ์ความเป็นส่วนตัวของแต่ละบุคคล เช่น การรวบรวม การใช้ การเปิดเผย และการปกป้องข้อมูลส่วนบุคคลโดยองค์กร องค์กรต่าง ๆ จะต้องปฏิบัติตามแนวทางเหล่านี้ และการไม่ปฏิบัติตามอาจนำไปสู่ผลกระทบทางกฎหมายและทางการเงินอย่างมีนัยสำคัญ การรับรองการปฏิบัติตามพีดีพีเอไม่ใช่แค่ภาระผูกพันทางกฎหมาย แต่ยังเป็นองค์ประกอบสำคัญในการรักษาความไว้วางใจและความน่าเชื่อถืออีกด้วย

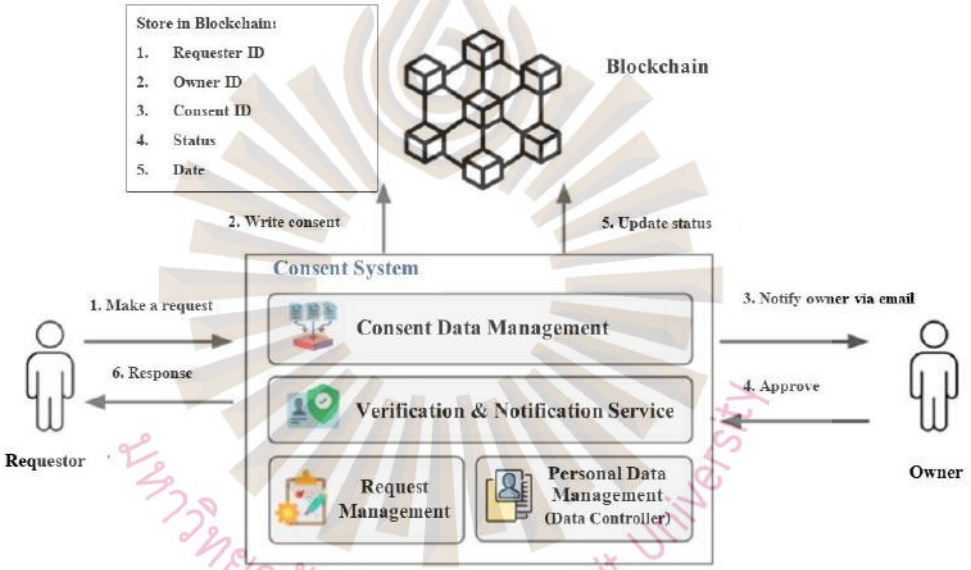
2) เทคโนโลยีบล็อกเชน: ได้รับการยอมรับมากขึ้นว่าเป็นเครื่องมืออันทรงพลังสำหรับการจัดการความยินยอมในขอบเขตของการปฏิบัติตามพีดีพีเอ ลักษณะการกระจายศูนย์และระบบบัญชีแยกประเภทที่ไม่เปลี่ยนรูปแบบทำให้เกิดแพลตฟอร์มที่ปลอดภัย และโปร่งใสสำหรับการบันทึกและจัดการธุรกรรมการยินยอม การดำเนินการยินยอมทุกรายการเมื่อบันทึกไว้ในบล็อกเชนจะมีการประทับเวลาและไม่สามารถเปลี่ยนแปลงย้อนหลังได้ ทำให้มั่นใจได้ถึงเส้นทางการตรวจสอบที่เชื่อถือได้ สิ่งนี้สามารถเป็นเครื่องมือในการแสดงให้เห็นถึงการปฏิบัติตามพีดีพีเอ เนื่องจากองค์กรสามารถจัดทำบันทึกการรับและการจัดการความยินยอมที่ปฏิเสธไม่ได้

3) สัญญาอัจฉริยะ: สามารถปฏิวัติการจัดการความยินยอมโดยทำให้กระบวนการต่าง ๆ เป็นแบบอัตโนมัติ สัญญาที่ดำเนินการด้วยตนเองโดยมีเงื่อนไขของข้อตกลงที่เขียนลงไว้ในชุดคำสั่งโดยตรง ทำให้กระบวนการจัดการความยินยอมเป็นอัตโนมัติ โดยดำเนินการตามที่กำหนดไว้ล่วงหน้า เมื่อตรงตามเงื่อนไขบางประการ เช่น การให้สิทธิ์การเข้าถึงข้อมูลเมื่อได้รับความยินยอม หรือการเพิกถอนการเข้าถึงและการลบข้อมูลหากความยินยอมถูกเพิกถอน สัญญาอัจฉริยะปรับปรุงความคล่องตัวในการจัดการความยินยอมโดยลดความจำเป็นในการกำกับดูแลด้วยตนเองและรับรองว่าเงื่อนไขความยินยอมได้รับการบังคับใช้อย่างสม่ำเสมอและโปร่งใส

จากรูปที่ 2.6 ได้แสดงภาพรวมของแผนภาพระบบ การจัดการจัดข้อมูลส่วนบุคคลทำ

หน้าที่เป็นผู้ควบคุมข้อมูล (Data controller) ของพีดีพีเอ ในกรณีนี้การใช้งานมอดูลการจัดการส่วนบุคคล (Data controller) จะอยู่ในเครื่องคอมพิวเตอร์แม่ข่ายหลักของศูนย์ข้อมูล ซึ่งเก็บบันทึกข้อมูลของลูกค้าที่ใช้งานอยู่ทั้งหมด

ผู้ร้องขอ คือบุคคลที่ต้องการขอใบอนุญาตในการจัดเก็บหรือประมวลผล ถอน หรือปรับปรุงจากเจ้าของข้อมูล จากขั้นตอนที่ 1 ถึงขั้นตอนที่ 5 ไม่มีข้อมูลของเจ้าของในบล็อกความยินยอมเพื่อหลีกเลี่ยงการละเมิดข้อมูล โดยแต่ละบล็อกจะประกอบด้วย เลขประจำตัวของผู้ร้องขอ (Requestor ID) เลขประจำตัวของเจ้าของ (Owner ID) เลขประจำตัวของความยินยอม (Consent ID) สถานะ (Status) และวันที่ (Date) (Lapwattanaworakul, Srisa-An, & Aribarg, 2023, p. 2472)



รูปที่ 2.6 แสดงแผนภาพสถาปัตยกรรมของระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS Architecture Diagram)

ที่มา: Lapwattanaworakul, Srisa-An, & Aribarg, 2023

จากรูปที่ 2.6 แสดงแผนผังการจัดการความยินยอมของมหาวิทยาลัยรังสิตซึ่งเป็นรูปแบบแนวคิดในการจัดการข้อมูลส่วนบุคคลที่บูรณาการร่วมกับสัญญาอัจฉริยะภายในโครงสร้างพื้นฐานบล็อกเชนส่วนตัว ระบบนี้ได้รับการออกแบบมาเพื่อจัดการความยินยอมอย่างปลอดภัยและเพื่อตรวจสอบตัวตนของเจ้าของข้อมูลภายในสภาพแวดล้อมบล็อกเชนส่วนตัว ทั้งนี้เพื่อเพิ่มความเป็นส่วนตัวและความปลอดภัยของข้อมูล เพื่อให้มั่นใจว่าสอดคล้องและปฏิบัติตามกฎหมายคุ้มครองข้อมูล เช่น พีดีพีเอ ประเด็นสำคัญของระบบมีรายละเอียดดังนี้ (Lapwattanaworakul, Srisa-An, & Aribarg, 2023, p. 2473)

1) ภารกิจที่ 1 การได้รับความยินยอม: องค์กรจะต้องได้รับความยินยอมจากบุคคล (เจ้าของข้อมูล) ก่อนจึงจะสามารถรวบรวมหรือประมวลผลข้อมูลส่วนบุคคลของตนได้ ความยินยอมนี้จะต้องชัดเจนและปฏิบัติตามกฎหมายคุ้มครองข้อมูล เช่น พีดีพีเอ ในส่วนสัญญาอัจฉริยะทำหน้าที่เป็นโทเค็นการอนุญาต ซึ่งแสดงถึงความยินยอมที่ได้รับจากเจ้าของข้อมูล โทเค็นเหล่านี้ควบคุมพารามิเตอร์ของวิธีการใช้ข้อมูลส่วนบุคคล

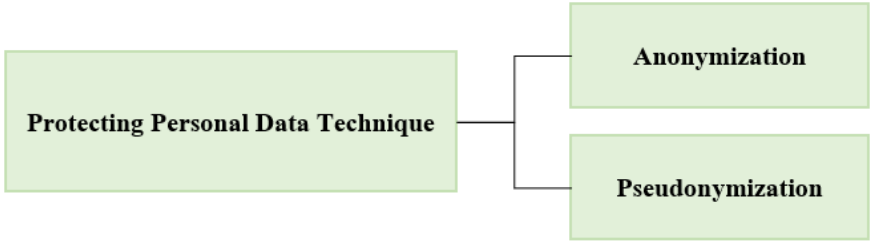
2) ภารกิจที่ 2 การยืนยันตัวตน: องค์กรจะต้องสามารถตรวจสอบตัวตนของเจ้าของข้อมูลได้เพื่อให้แน่ใจว่าความยินยอมนั้นถูกต้องตามกฎหมาย ซึ่งทำได้โดยใช้โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure - PKI) ซึ่งเป็นเฟรมเวิร์กที่ใช้กุญแจคู่ (กุญแจสาธารณะและกุญแจส่วนตัว) สำหรับการเข้ารหัสและลายเซ็นดิจิทัล รับประกันการปกป้องความเป็นส่วนตัวผ่านการเข้ารหัส ซึ่งอนุญาตให้เฉพาะเจ้าของข้อมูลซึ่งมีกุญแจส่วนตัวเท่านั้นที่สามารถเข้าถึงข้อมูลได้ สิ่งนี้รับประกันการรักษาความลับและความปลอดภัยของข้อมูลที่ละเอียดอ่อน

3) การปฏิบัติตามพีดีพีเอ: การใช้สัญญาอัจฉริยะเป็นโทเค็นการอนุญาต ช่วยให้ระบบปฏิบัติตามข้อกำหนดด้านกฎระเบียบโดยให้แนวทางการยินยอมที่ชัดเจนและสามารถตรวจสอบได้

4) ความเป็นส่วนตัวและความปลอดภัย: การเข้ารหัสบล็อกเชนจำกัดการเข้าถึงข้อมูลสำหรับผู้ที่มีกุญแจส่วนตัวที่เหมาะสม ซึ่งโดยทั่วไปคือเจ้าของข้อมูล ซึ่งรับประกันการรักษาความลับและความปลอดภัยของข้อมูลส่วนบุคคล

2.6 เทคนิคการปกป้องข้อมูลส่วนบุคคล (Protecting Personal Data Technique)

ในการวิจัยฉบับนี้จะกล่าวถึงเทคนิคที่ใช้ในการปกป้องข้อมูลส่วนบุคคลเพียง 2 เทคนิคที่สำคัญเท่านั้น ได้แก่ การแฝงข้อมูล (Pseudonymization) และการทำให้เป็นนิรนาม (Anonymization) ดังรูปที่ 2.7 เทคนิคทั้งสองแตกต่างกันเมื่อเผชิญกับข้อกำหนดของจีดีพีอาร์ ดังนั้นตัวเลือกจะขึ้นอยู่กับระดับความเสี่ยงและวิธีการประมวลผล



รูปที่ 2.7 เทคนิคการปกป้องข้อมูลส่วนบุคคล

ที่มา: Service of the Republic of Poland, 2018

2.6.1 ข้อมูลที่เข้าข่ายเป็นข้อมูลส่วนบุคคล

โดยทั่วไปอาจจำแนกประเภทข้อมูลออกเป็น 3 ประเภท ขึ้นกับระดับความเข้มข้นในความสามารถในการระบุตัวตนเจ้าของข้อมูลดังนี้ (พีรดล สามะศิริ และ อนันต์วัฒน์ ทิพย์ภาวัต, 2564, น. 1)

2.6.1.1 ข้อมูลส่วนบุคคล (Personal Data) คือข้อมูลที่ทำให้สามารถระบุตัวบุคคลนั้นได้ ทั้งนี้การระบุตัวบุคคลอาจทำได้เนื่องจากเลขหรือรหัสประจำตัว รวมไปถึงข้อมูลปัจจัยหนึ่งหรือหลายปัจจัยร่วมกันเช่น ข้อมูลกายภาพ ข้อมูลประชากร ข้อมูลเศรษฐกิจ ข้อมูลสังคม ข้อมูลความเชื่อ ฯลฯ ทั้งนี้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้คำจำกัดความข้อมูลส่วนบุคคลไว้ในมาตรา 6 ว่าคือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่า ทางตรงหรือทางอ้อม

2.6.1.2 ข้อมูลนิรนาม (Anonymous Data) ได้แก่ ข้อมูลซึ่งมีการระบุตัวตนเจ้าของข้อมูลที่ไม่สามารถเป็นไปได้ ไม่ว่าจะโดยผู้ประมวลผลข้อมูลหรือบุคคลอื่นใด แนวปฏิบัติของจีดีพีอาร์กำหนดเกณฑ์ความเป็นนิรนามของข้อมูลไว้สูง กล่าวคือ ข้อมูลชิ้นหนึ่งจะเป็นข้อมูลนิรนามได้ต่อเมื่อไม่สามารถระบุตัวตนเจ้าของข้อมูลได้ไม่ว่าโดยวิธีการใด ด้วยเหตุนี้ จีดีพีอาร์จึงไม่บังคับใช้กับข้อมูลนิรนาม

2.6.1.3 ข้อมูลแฝง (Pseudonymous Data) ได้แก่ ข้อมูลที่ผ่านกระบวนการแฝงหรือพรางข้อมูลบ่งชี้ตัวตัวบุคคลไว้ โดยอาจใช้วิธีเปลี่ยนข้อมูลที่ระบุตัวบุคคล (Identifier) ด้วยข้อมูลเลขหรือรหัสอื่น ข้อแตกต่างทางกฎหมายของข้อมูลแฝงและข้อมูลนิรนาม ได้แก่ การที่จีดีพีอาร์ยังบังคับใช้กับข้อมูลแฝงด้วย เนื่องจากยังสามารถระบุตัวตนเจ้าของข้อมูลแฝงได้

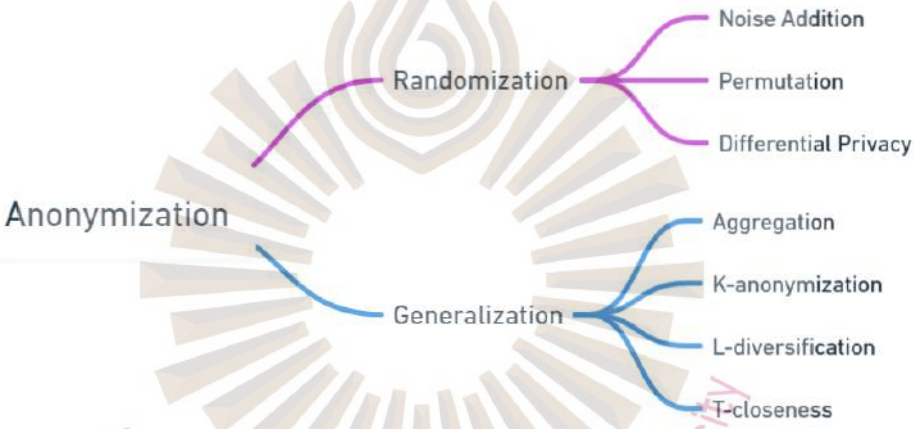
กระบวนการลดความเสี่ยงการระบุตัวตนเจ้าของข้อมูลให้อยู่ในเกณฑ์น้อยมากจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง เรียกว่า การทำให้เป็นนิรนาม (Anonymization) ถึงแม้ข้อมูลนิรนาม จะไม่ถือเป็นข้อมูลส่วนบุคคล ดังจะเห็นได้จากการที่จีดีพีอาร์ซึ่งถือเป็นกฎหมายต้นแบบของพีดีพีเอของประเทศไทย ไม่ถูกบังคับใช้กับข้อมูลที่เป็นข้อมูลนิรนาม ดังระบุในจีดีพีอาร์ มาตราที่ 26 ซึ่งให้คำจำกัดความของข้อมูลข่าวสารนิรนามว่าคือ

> ข้อมูลนิรนาม ได้แก่ ข้อมูลที่ไม่สัมพันธ์กับบุคคลที่ถูกระบุตัวตนหรือสามารถระบุตัวตนได้ใด ๆ หรือข้อมูลส่วนบุคคลที่ถูกทำให้ระบุตัวตนไม่ได้ด้วยวิธีการที่ทำให้ไม่สามารถระบุตัวตนเจ้าของข้อมูลได้หรือไม่สามารถระบุตัวตนได้อีกต่อไป ดังนั้นข้อกำหนดนี้ไม่เกี่ยวข้องกับการประมวลข้อมูลนิรนามอันรวมไปถึงเพื่อวัตถุประสงค์ทาง

สถิติหรือการวิจัย (นคร เสรีรักษ์ และคณะ, 2562, น. 15)

2.6.2 เทคนิควิธีการทำให้เป็นนิรนาม (Anonymization)

การทำให้เป็นนิรนาม (Anonymization) เป็นกระบวนการในการเปลี่ยนแปลงข้อมูลส่วนบุคคลอย่างถาวรและไม่สามารถย้อนกลับได้เพื่อป้องกันการระบุตัวตน เทคนิคนี้ช่วยให้แน่ใจว่าการเชื่อมโยงข้อมูลกับบุคคลใดบุคคลหนึ่งไม่สามารถทำได้ภายในเวลาหรือต้นทุนที่เหมาะสม เทคนิคการทำให้เป็นนิรนามสามารถแบ่งออกเป็นสองประเภท ดังรูปที่ 2.8 โดยมีรายละเอียดดังนี้ (Service of the Republic of Poland, 2018, pp. 12-20)



รูปที่ 2.8 เทคนิคการทำให้เป็นนิรนาม

ที่มา: Service of the Republic of Poland, 2018

2.6.2.1 การสุ่ม (Randomization) เป็นกลุ่มของเทคนิคที่ปรับเปลี่ยนความถูกต้องของข้อมูลเพื่อขจัดความเชื่อมโยงที่ชัดเจนระหว่างข้อมูลกับบุคคลใดบุคคลหนึ่ง ข้อมูลมีความไม่แน่นอนเพียงพอ และไม่สามารถอ้างอิงถึงบุคคลใดบุคคลหนึ่งได้อีกต่อไป การสุ่มโดยตัวมันเองจะไม่ลดความเป็นเอกเทศของแต่ละรายการ เนื่องจากแต่ละรายการจะยังคงได้มาจากหัวข้อข้อมูลเดียว แต่อาจป้องกันการอนุมานได้ เพื่อให้มั่นใจถึงการป้องกันที่แข็งแกร่งยิ่งขึ้น

1) การเพิ่มการรบกวน (Noise Addition) เกี่ยวข้องกับการแก้ไขคุณลักษณะภายในชุดข้อมูลเพื่อลดความแม่นยำในขณะที่ยังคงการกระจายโดยรวม เทคนิคนี้มีประโยชน์อย่างยิ่งในการปกป้องบุคคลเมื่อคุณลักษณะบางอย่างอาจทำให้เกิดผลเสียได้ ค่าที่แก้ไขยังคงมีความถูกต้องในวงกว้างแต่ในระดับที่จำกัดเท่านั้น ตัวอย่างเช่น หากน้ำหนักของบุคคลถูกบันทึกด้วยความแม่นยำไว้ที่ 0.5 กิโลกรัม การเพิ่มการรบกวนอาจปรับค่านี้เป็นความแม่นยำ ±5 กิโลกรัม เมื่อนำไปใช้อย่างมี

มหาวิทยาลัยรังสิต Rangsit University

ประสิทธิภาพ เทคนิคนี้จะป้องกันไม่ให้บุคคลที่สามระบุตัวบุคคล สร้างข้อมูลต้นฉบับขึ้นใหม่ หรือตรวจจับการแก้ไขเฉพาะเจาะจง ตัวอย่างดังรูปที่ 2.9

Age	Weight	Height	City
25	62	180	Lublin
20	80	160	Poznań
35	75	176	Opole
45	49	156	Kraków
25	82	162	Ełk

Original table

Age (+/-5)	Weight (+/-5)	Height (+/-5)	City
25	66	178	Lublin
22	79	165	Poznań
31	72	178	Opole
47	45	161	Kraków
24	79	162	Ełk

Modified table

รูปที่ 2.9 เทคนิคการเพิ่มการรบกวน

ที่มา: Service of the Republic of Poland, 2018

2) การเรียงสับเปลี่ยน (Permutation) เป็นเทคนิคการทำให้ข้อมูลเป็นนิรนาม ซึ่งจะสับเปลี่ยนค่าแอตทริบิวต์ภายในชุดข้อมูล ซึ่งขัดขวางความสัมพันธ์เดิมกับแต่ละบุคคลในขณะที่ยังคงการกระจายโดยรวมไว้ ซึ่งแตกต่างจากการเพิ่มการรบกวนแบบเดิม ๆ ซึ่งจะแก้ไขค่าแบบสุ่ม การเรียงสับเปลี่ยนจะสลับค่าระหว่างรายการ โดยคงคุณสมบัติทางสถิติของชุดข้อมูลไว้ อย่างไรก็ตาม การเรียงสับเปลี่ยนคุณลักษณะอย่างอิสระสามารถทำลายความสัมพันธ์เชิงตรรกะได้ อาจทำให้การเรียงสับเปลี่ยนย้อนกลับได้ เพื่อป้องกันสิ่งนี้ ควรเปลี่ยนแอตทริบิวต์ที่เกี่ยวข้องกันเพื่อรักษาความสอดคล้องและความเป็นส่วนตัว ตัวอย่างดังรูปที่ 2.10

Job	Income (k/year)	Year of birth.	Gender
Shop assistant	24	1990	F
Shop assistant	48	1985	M
Driver	60	1992	F
Worker	72	1986	M
Manager	120	1975	M

Original table

Job	Income (k/year)	Year of birth.	Gender
Shop assistant	24	1980	M
Shop assistant	48	1990	M
Driver	60	1986	F
Worker	72	1985	M
Manager	120	1980	F

Modified table

รูปที่ 2.10 เทคนิคการเรียงสับเปลี่ยน

ที่มา: Service of the Republic of Poland, 2018

3) ความเป็นส่วนตัวที่แตกต่างกัน (Differential Privacy) เป็นเทคนิคที่ปกป้องความเป็นส่วนตัวของแต่ละบุคคลโดยการเพิ่มการรบกวนที่ควบคุมไปยังผลลัพธ์การสืบค้น แทนที่จะแก้ไขชุดข้อมูลดั้งเดิม เจ้าของข้อมูลจะเก็บข้อมูลต้นฉบับและให้การตอบกลับโดยไม่ระบุชื่อสำหรับคำถามเฉพาะ เพื่อให้มั่นใจถึงความเป็นส่วนตัวในขณะที่ยังคงรักษาอรรถประโยชน์ข้อมูลไว้ ข้อได้เปรียบที่สำคัญคือ การจำกัดการเข้าถึงข้อมูลผ่านผลลัพธ์ที่อิงตามการสืบค้น แทนที่จะปล่อยชุดข้อมูลทั้งหมด เพื่อป้องกันการเข้าถึงและการระบุตัวตนซ้ำโดยไม่ได้รับอนุญาต สามารถบันทึกข้อความค้นหาและไม่เปิดเผยตัวตนเพิ่มเติมได้ อย่างไรก็ตาม ความเป็นส่วนตัวที่แตกต่างกันจะต้องได้รับการตรวจสอบอย่างระมัดระวังเพื่อหลีกเลี่ยงการโจมตีแบบเชื่อมโยงและไม่ควรใช้ในสภาพแวดล้อมการค้นหาแบบเปิดโดยไม่มีการตรวจสอบย้อนกลับ

2.6.2.2 การทำให้เป็นลักษณะทั่วไป (Generalization) เป็นเทคนิคสำคัญในการทำให้เป็นนิรนามซึ่งจะลดความจำเพาะของข้อมูลโดยการขยายค่าแอตทริบิวต์ให้กว้างขึ้น สิ่งนี้เกี่ยวข้องกับการปรับเปลี่ยนขนาดหรือระดับของรายละเอียด เช่น การแสดงสถานที่ในระดับภูมิภาคแทนเมืองหรือใช้เดือนแทนสัปดาห์ แม้ว่าการทำให้เป็นลักษณะทั่วไปจะช่วยป้องกันการระบุตัวบุคคล แต่ก็อาจไม่ได้รับประกันว่าจะเป็นการทำให้เป็นนิรนามโดยสมบูรณ์ไป เพื่อป้องกันการเชื่อมโยงและการอนุมานได้อย่างมีประสิทธิภาพ มักจำเป็นต้องใช้วิธีการเชิงปริมาณขั้นสูง

1) การรวมกลุ่มและการทำ k-Anonymization (Aggregation and k-Anonymization) เป็นการปกป้องความเป็นส่วนตัวโดยการจัดกลุ่มหัวเรื่องข้อมูล เพื่อให้บุคคลอย่างน้อย k คนใช้ค่าแอตทริบิวต์เดียวกัน ซึ่งทำได้โดยการสรุปข้อมูล เช่น การลดความแม่นยำของตำแหน่งจากเทศบาลไปยังจังหวัด หรือการแปลงค่าตัวเลขเป็นช่วงที่กว้างขึ้น (เช่น ความสูง 180-190 เซนติเมตร) เทคนิคเหล่านี้ช่วยป้องกันการระบุซ้ำเมื่อค่าแอตทริบิวต์เฉพาะสามารถทำหน้าที่เป็นตัวระบุเสมือนได้ ตัวอย่างดังรูปที่ 2.11

Surnam	Ag	Gende	Count	Illness
Nowak	29	F	Mińsk	Cancer
Kowal	24	F	Otwoc	Mental
Gajda	28	F	Mińsk	Asthma
Halicki	27	M	Płock	None
Górski	24	F	Otwoc	Cardiac
Golec	23	M	Płock	Asthma
Dłuski	19	M	Otwoc	Cancer
Bogucki	29	M	Płock	Cardiac
Leja	17	M	Otwoc	Cardiac
Nowak	19	M	Otwoc	Mental

Original table

Su	Age	Gende	Count	Illness
*	20 < Age ≤ 30	F	Mińsk	Cancer
*	20 < Age ≤ 30	F	Otwoc	Mental
*	20 < Age ≤ 30	F	Mińsk	Asthma
*	20 < Age ≤ 30	M	Płock	None
*	20 < Age ≤ 30	F	Otwoc	Cardiac
*	20 < Age ≤ 30	M	Płock	Asthma
*	Age ≤ 20	M	Otwoc	Cancer
*	20 < Age ≤ 30	M	Płock	Cardiac
*	Age ≤ 20	M	Otwoc	Cardiac
*	Age ≤ 20	M	Otwoc	Mental

Modified table

รูปที่ 2.11 เทคนิคการรวมกลุ่มและการทำ k-Anonymity

ที่มา: Service of the Republic of Poland, 2018

2) การทำ l-Diversity เป็นการเพิ่มประสิทธิภาพของการทำ k-Anonymization เพื่อให้แน่ใจว่าแต่ละกลุ่มที่ไม่ระบุตัวตนจะมีค่าที่แตกต่างกันอย่างน้อย l สำหรับแอตทริบิวต์ที่ละเอียดอ่อน วิธีนี้จะป้องกันการโจมตีโดยอนุมานโดยการจำกัดโอกาสที่ผู้โจมตีจะระบุข้อมูลของแต่ละบุคคลโดยอิงจากความรู้เบื้องหลัง เพื่อให้มีประสิทธิผล คลาสที่เทียบเท่าควรมีความแปรปรวนของแอตทริบิวต์ที่เพียงพอเพื่อให้ผู้โจมตีเหลือความไม่แน่นอนเท่ากับ 1/l อย่างไรก็ตาม หากค่าคุณลักษณะมีการกระจายไม่ดีหรืออยู่ในช่วงแคบ l-Diversity อาจมีประสิทธิภาพน้อยลง ตัวอย่างดังรูปที่ 2.12

	Postal code	Age	Income	Illness
1	47677	29	3,000	ulcers
2	47602	22	4,000	gastritis
3	47678	27	5,000	stomach cancer
4	47905	43	6,000	gastritis
5	47909	49	11,00	influenza
6	47906	47	8,000	bronchitis
7	47605	30	7,000	bronchitis
8	47673	36	9,000	pneumonia
9	47607	32	10,00	stomach cancer
10	47909	52	9,000	gastritis
11	47905	59	12,00	influenza
12	47908	61	10,00	stomach cancer

Postal code	Age	Income	Illness
476**	2*	3,000	ulcers
476**	2*	4,000	gastritis
476**	2*	5,000	stomach cancer
4790*	40-50	6,000	gastritis
4790*	40-50	11,000	influenza
4790*	40-50	8,000	bronchitis
476**	3*	7,000	bronchitis
476**	3*	9,000	pneumonia
476**	3*	10,000	stomach cancer
4790*	≥50	9,000	gastritis
4790*	≥50	12,000	influenza
4790*	≥50	10,000	stomach cancer

รูปที่ 2.12 เทคนิคการ l-Diversity

ที่มา: Service of the Republic of Poland, 2018

3) การทำ t-Closeness คือปรับแต่งความหลากหลายโดยทำให้การกระจายค่าแอตทริบิวต์ภายในกลุ่มที่เป็นนิรนามแต่ละกลุ่มตรงกับการกระจายโดยรวมในชุดข้อมูลอย่างใกล้ชิด วิธีการนี้กำหนดข้อจำกัดในการแจกแจงความน่าจะเป็นเพื่อป้องกันการเปิดเผยทางสถิติในขณะที่ยังคงรักษาอรรถประโยชน์ข้อมูลไว้ด้วยการรักษาการแจกแจงกลุ่มให้ใกล้กับชุดข้อมูลดั้งเดิมมากที่สุด t-Closeness จะให้การป้องกันที่แข็งแกร่งยิ่งขึ้นต่อการโจมตีโดยอนุมาน ตัวอย่างดังรูปที่ 2.13

ID	Postal code	Age	Income	Illness
1	47677	29	3,000	Ulcers
2	47602	22	4,000	gastritis
3	47678	27	5,000	stomach
4	47905	43	6,000	gastritis
5	47909	52	11,000	influenza
6	47906	47	8,000	bronchitis
7	47605	30	7,000	bronchitis
8	47673	36	9,000	pneumonia
9	47607	32	10,000	stomach

ID	Postal code	Age	Income	Illness
1	476**	≤40	3,000	ulcers
3	476**	≤40	5,000	stomach cancer
8	476**	≤40	9,000	pneumonia
4	4790*	≥40	6,000	gastritis
5	4790*	≥40	11,000	influenza
6	4790*	≥40	8,000	bronchitis
2	476**	≤40	4,000	gastritis
7	476**	≤40	7,000	bronchitis
9	476**	≤40	10,000	stomach cancer

รูปที่ 2.13 เทคนิคการ t-Closeness

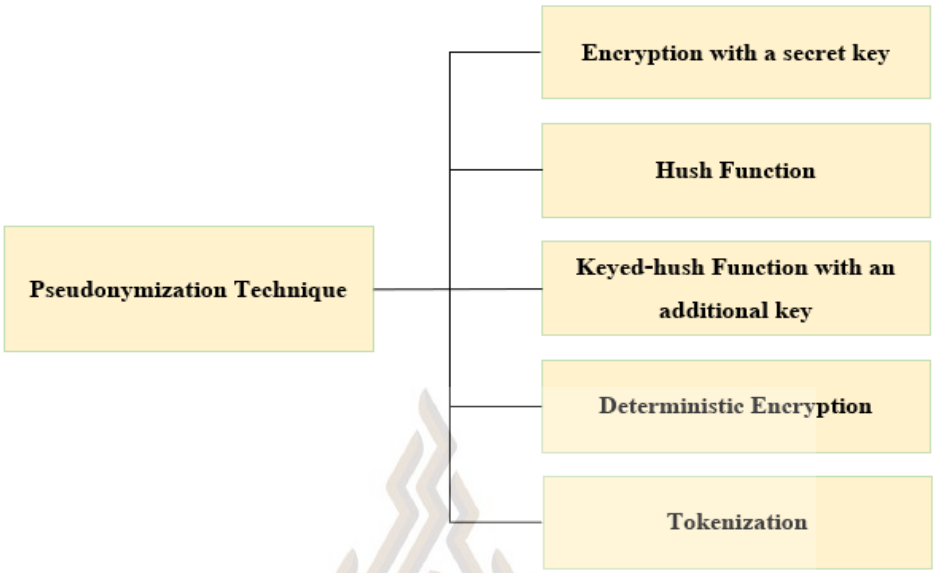
ที่มา: Service of the Republic of Poland, 2018

ทั้งนี้ยังมีเทคนิคอีกกลุ่มหนึ่งที่ช่วยลดความเสี่ยงในการระบุตัวตน ได้แก่ เทคนิคในกลุ่มที่เน้นการกับข้อมูลระบุตัวตนที่ชัดแจ้ง เช่น รหัสประจำตัว ชื่อ นามสกุล ฯลฯ โดยอาจเป็นในลักษณะของการลบทิ้ง การแทนค่าด้วยศูนย์ การปิดทับข้อมูลทั้งหมดหรือบางส่วน การสลับอักขระ ฯลฯ อย่างไรก็ดีเทคนิคกลุ่มนี้มักไม่สามารถรับประกันความเป็นนิรนามของข้อมูลได้ แต่เป็นเทคนิคที่ถูกนำไปใช้ประกอบกับเทคนิคอื่น ๆ ที่กล่าวมาข้างต้นเพื่อลดความสามารถในการระบุตัวตนของข้อมูล

2.6.3 เทคนิคการแฝงข้อมูล (Pseudonymization)

การแฝงข้อมูลตามจีดีพีอาร์เป็นวิธีการจัดการข้อมูลส่วนบุคคลเพื่อลดการเชื่อมโยงโดยตรงของข้อมูลกับบุคคลใดบุคคลหนึ่ง เว้นแต่จะใช้ข้อมูลเพิ่มเติมเพื่อระบุตัวตนเหล่านั้นอีกครั้ง และยังเป็นขั้นตอนการจัดการข้อมูลและการลบการระบุตัวตนที่ช่วยให้องค์กรสามารถใช้และประมวลผลข้อมูลในขณะที่รักษามาตรฐานความเป็นส่วนตัวและการปกป้องข้อมูล (European Network and Information Security Agency, 2019) แนวคิดนี้เป็นพื้นฐานในกฎระเบียบด้านการปกป้องข้อมูลและความเป็นส่วนตัว กระบวนการที่เกี่ยวข้องกับการแยกส่วนที่สามารถระบุตัวตนของข้อมูลออกจากข้อมูลเพิ่มเติมกลับไปยังแต่ละบุคคลได้ เป้าหมายคือการสร้างระดับการปกป้องข้อมูลโดยที่ข้อมูลยังคงมีประโยชน์ สำหรับวัตถุประสงค์ที่ชอบด้วยกฎหมาย เช่น การวิเคราะห์หรือการวิจัย แต่ลดความเสี่ยงของการระบุตัวตนโดยไม่ได้รับอนุญาตหรือโดยไม่ได้ตั้งใจได้อย่างมาก การใช้การแฝงข้อมูลถือเป็นเทคนิคที่มีคุณค่าในยุคของข้อมูลขนาดใหญ่และการวิเคราะห์

การแฝงข้อมูลเป็นเทคนิคการปกป้องข้อมูลแบบย้อนกลับได้ ซึ่งจะแทนที่ค่าจริงด้วยนามแฝง ทำให้การระบุตัวตนโดยตรงทำได้ยากขึ้น ช่วยให้สามารถเชื่อมโยงกิจกรรมต่าง ๆ กับบุคคลคนเดียวกันได้โดยไม่ต้องเปิดเผยข้อมูลส่วนบุคคล และช่วยให้สามารถรวมชุดข้อมูลหลากชุดได้ แม้ว่าการใช้การแฝงจะช่วยเพิ่มความปลอดภัยของข้อมูล แต่ก็ไม่เหมือนกับการทำให้เป็นนิรนาม เนื่องจากข้อมูลต้นฉบับยังสามารถกู้คืนได้ ข้อมูลที่ใช้การแฝงข้อมูลจึงยังคงอยู่ภายใต้กฎข้อบังคับในการคุ้มครอง สามารถแบ่งการใช้การแฝงข้อมูลออกได้เป็นห้าประเภทหลัก ดังรูปที่ 2.14 โดยมีรายละเอียดดังนี้ (Service of the Republic of Poland, 2018, pp. 20-24)



รูปที่ 2.14 เทคนิคการแฝงข้อมูล

ที่มา: Service of the Republic of Poland, 2018

2.6.3.1 การเข้ารหัสด้วยรหัสลับ (Encryption with a Secret Key) การเข้ารหัสช่วยปกป้องข้อมูลส่วนบุคคลโดยการแปลงเป็นรูปแบบที่อ่านไม่ได้ เพื่อให้มั่นใจว่าเฉพาะผู้ที่มีรหัสลับเท่านั้นที่สามารถถอดรหัสและเข้าถึงข้อมูลต้นฉบับได้ แม้ว่าข้อมูลที่เข้ารหัสจะยังคงอยู่ในชุดข้อมูลก็ตาม การรักษาความปลอดภัยจะขึ้นอยู่กับความแข็งแกร่งของอัลกอริทึมการเข้ารหัสและการรักษาความลับของกุญแจ เมื่อใช้รูปแบบการเข้ารหัสที่มีประสิทธิภาพการถอดรหัสจะทำได้เฉพาะเมื่อมีความรู้เกี่ยวกับกุญแจเท่านั้น

2.6.3.2 ฟังก์ชันแฮช (Hash Function) ฟังก์ชันแฮชสร้างเอาต์พุตที่มีขนาดคงที่จากอินพุตที่มีความยาวเท่าใดก็ได้ การแฮชเป็นกระบวนการทางเดียวซึ่งต่างจากการเข้ารหัสตรงและไม่สามารถย้อนกลับได้ อย่างไรก็ตาม หากทราบช่วงอินพุตและวิธีการแฮช ผู้โจมตีสามารถพยายามโจมตีแบบดุร้าย (Brute Force) โดยการแฮชค่าที่เป็นไปได้ทั้งหมดเพื่อค้นหาค่าที่ตรงกัน สร้างตารางความสัมพันธ์เพื่ออนุมานข้อมูลต้นฉบับ ฟังก์ชันแฮชถูกจำแนกตามขนาดเอาท์พุต (วัดเป็นบิต) ตามคำแนะนำของ NIST (สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา) แอปพลิเคชันใหม่ควรใช้ฟังก์ชันแฮชตระกูล SHA-2 โดยที่ SHA-3 เป็นมาตรฐานในอนาคตอัลกอริทึมรุ่นเก่า เช่น MD5 และ SHA-1 เลิกใช้แล้วเนื่องจากมีความปลอดภัยต่ำและมีความเสี่ยงต่อการโจมตี ตัวอย่างดังรูปที่ 2.15

Hash function	Output block (input phrase: Jan Kowalski)
SHA-2*	e70207d004bdffb1702b9c50f5a8c70a49f6f8a68404ca59993d3c39142162ba1bac5cc2c396460c205b0a79676c736ae345257aae26c61444f3efc1efa822c0
SHA-3*	88f2a580725f980b96829210bf3e7a159a5ce23a13f289d077c3e45ef0c5a3876a81618f70c6641f14cd4fc58a5cf80d928909187c772108e9342051e632fdbb

*512 bit version

รูปที่ 2.15 ตัวอย่างการใช้ฟังก์ชันแฮช

ที่มา: Service of the Republic of Poland, 2018

2.6.3.3 ฟังก์ชันคีย์แฮชพร้อมคีย์เพิ่มเติม (Keyed-Hash Function with an Additional Key) ฟังก์ชันคีย์แฮชช่วยเพิ่มความเป็นส่วนตัวด้วยการรวมกุญแจลับเป็นอินพุตเพิ่มเติม ทำให้มีความปลอดภัยมากกว่าการแฮชแบบมาตรฐานอย่างมาก เนื่องจากบุคคลที่สามไม่สามารถดึงข้อมูลต้นฉบับโดยไม่ทราบรหัสได้ เนื่องจากมีกุญแจผสมที่เป็นไปได้จำนวนมาก การถอดรหัสโดยหน่วยงานที่ไม่ได้รับอนุญาตจึงเป็นไปไม่ได้ในทางปฏิบัติ อย่างไรก็ตาม เจ้าของข้อมูลสามารถตรวจสอบหรือสร้างข้อมูลต้นฉบับใหม่ได้อย่างง่ายดายโดยใช้รหัสลับ ตัวอย่างทั่วไปของฟังก์ชันคีย์แฮชได้แก่ HMAC และ UMAC ตัวอย่างดังรูปที่ 2.16

Keyed-hash function	Output block (input phrase: Jan Kowalski with the key Cyfryzacja)
HMAC (SHA1)	cf7449fcdeea860bbfc503410520d6623dd40a1e
HMAC (SHA512)	2fd3e276606e45b474e07fcca1b605e3127f03ce9fb11aec09a5f3cda4f315b41a6ecdfd94016edf49ab35fb1478f13247c7b23c7e5e509e68238ad9088bec70

รูปที่ 2.16 ตัวอย่างการใช้ฟังก์ชันคีย์แฮชพร้อมคีย์เพิ่มเติม

ที่มา: Service of the Republic of Poland, 2018

2.6.3.4 การเข้ารหัสที่กำหนด (Deterministic Encryption) จะกำหนดค่าที่เข้ารหัสอย่างสม่ำเสมอ (ทำหน้าที่นามแฝง) ให้กับแต่ละคุณลักษณะในฐานข้อมูล จากนั้นจะลบตารางการติดต่อออก วิธีการนี้ช่วยลดความเสี่ยงในการระบุตัวบุคคลได้อย่างมาก โดยป้องกันการอ้างอิงโยงกับชุดข้อมูลอื่นที่อาจใช้นามแฝงที่แตกต่างกัน เนื่องจากอินพุตเดียวกันจะสร้างเอาต์พุตที่เข้ารหัสเหมือนกันเสมอ การเข้ารหัสที่กำหนดช่วยให้สามารถเชื่อมโยงข้อมูลได้อย่างปลอดภัยในขณะที่ยังคงรักษาความเป็นส่วนตัว

2.6.3.5 การทำเป็นโทเค็น (Tokenization) การแปลงโทเค็นจะแทนที่ข้อมูลที่ละเอียดอ่อนด้วยตัวระบุเฉพาะ (โทเค็น) ที่ไม่มีความสัมพันธ์ทางคณิตศาสตร์หรือโดยตรงกับค่าดั้งเดิม ต่างจากการเข้ารหัส นี่เป็นกระบวนการทางเดียว ซึ่งหมายความว่าข้อมูลต้นฉบับไม่สามารถได้รับจากโทเค็นหากไม่มีการเข้าถึงระบบการจับคู่ที่ปลอดภัย การทำให้เป็นโทเค็นถูกนำมาใช้กันอย่างแพร่หลายในภาคการเงินโดยเฉพาะอย่างยิ่งสำหรับการรักษาความปลอดภัยธุรกรรมการชำระเงินและการอนุญาตการดำเนินการทางธนาคาร

ความจริง 10 อันดับแรกเกี่ยวกับการใช้การแฝงข้อมูลในจีดีพีอาร์ของสหภาพยุโรป เน้นประเด็นสำคัญเกี่ยวกับวิธีการใช้การแฝงข้อมูลภายใต้จีดีพีอาร์ของสหภาพยุโรป (LaFever, 2021, p. 1) มีรายละเอียดดังนี้

1) การใช้การแฝงข้อมูลไม่เหมือนกับการทำให้เป็นนิรนาม: การใช้การแฝงข้อมูลเกี่ยวข้องกับการแทนที่ตัวระบุในข้อมูลด้วยข้อมูลแฝง ซึ่งทำให้ระบุตัวตนได้น้อยลงแต่ยังคงสามารถย้อนกลับได้ ในทางกลับกันการทำให้เป็นนิรนามเป็นการเปลี่ยนแปลงข้อมูลอย่างถาวรเพื่อป้องกันการระบุตัวตนของเรื่องทำให้ไม่เป็นข้อมูลส่วนบุคคลภายใต้จีดีพีอาร์อีกต่อไป

2) การใช้การแฝงข้อมูลของจีดีพีอาร์เป็นมาตรฐานที่สูงกว่าการใช้การแฝงก่อนจีดีพีอาร์: จีดีพีอาร์กำหนดข้อกำหนดที่เข้มงวดมากขึ้นสำหรับการใช้การแฝงข้อมูลมากกว่ามาตรฐานการปกป้องข้อมูลก่อนหน้านี้ กำหนดให้การใช้การแฝงข้อมูลควรตรวจสอบให้แน่ใจว่าข้อมูลเพิ่มเติมสำหรับการระบุตัวตนซ้ำจะถูกเก็บไว้แยกต่างหาก และอยู่ภายใต้มาตรการทางเทคนิคและองค์กรเพื่อให้แน่ใจว่าไม่มีการระบุแหล่งที่มา

3) การใช้การแฝงข้อมูลไม่ใช่ความล้มเหลวในการทำให้เป็นนิรนาม: การใช้การแฝงข้อมูลไม่ได้เป็นเพียงรูปแบบที่อ่อนแอกว่าของการทำให้ข้อมูลเป็นนิรนามเท่านั้น มันเป็นกระบวนการที่แตกต่างโดยมีวัตถุประสงค์และมาตรฐานของตัวเองโดยมีวัตถุประสงค์หลักเพื่อเพิ่มความเป็นส่วนตัวในขณะที่ยังคงรักษาอรรถประโยชน์ข้อมูลไว้

4) การใช้การแฝงข้อมูลของจีดีพีอาร์ต้องมีการคุ้มครองตัวระบุที่มากกว่าโดยตรง: ภายใต้จีดีพีอาร์ การใช้การแฝงข้อมูลต้องปกป้องไม่เพียงแค่ตัวระบุโดยตรง (เช่น ชื่อหรือหมายเลขประกันสังคม) แต่ยังรวมถึงตัวระบุทางอ้อมที่สามารถระบุตัวบุคคลได้เมื่อรวมกับข้อมูลอื่น ๆ

5) การใช้การแฝงข้อมูลของจีดีพีอาร์จำเป็นต้องมีการควบคุมที่ซับซ้อนมากขึ้น: ข้อบังคับของจีดีพีอาร์กำหนดให้การใช้การแฝงข้อมูลควรเกี่ยวข้องกับการควบคุมที่ซับซ้อนเพื่อให้แน่ใจว่าการระบุตัวตนซ้ำอีกครั้งจะไม่สามารถทำได้หากไม่มีข้อมูลเพิ่มเติม ซึ่งจะต้องแยกจากกันโดย

ผู้ควบคุมข้อมูล

6) การใช้การแฝงข้อมูลของจีดีพีอาร์จำเป็นต้องมีการเปลี่ยนแปลง: จีดีพีอาร์สนับสนุนการใช้การแฝงข้อมูลแบบไดนามิกโดยการใช้การแฝงข้อมูล (โทเค็น) ที่แตกต่างกันในเวลาที่ต่างกันหรือเพื่อวัตถุประสงค์ที่แตกต่างกัน ช่วยเพิ่มความปลอดภัยและลดความเสี่ยงของการระบุตัวตนซ้ำอีกครั้ง

7) การใช้การแฝงข้อมูลของจีดีพีอาร์ช่วยให้สามารถประมวลผลตามมาตรา 11(2) และ 12(2) ได้: การใช้การแฝงข้อมูลภายใต้จีดีพีอาร์สามารถช่วยตอบสนองข้อกำหนดของ Schrems II (คำตัดสินของศาลที่สำคัญเกี่ยวกับการปกป้องข้อมูล) โดยทำหน้าที่เป็นมาตรการเสริมทางเทคนิค ซึ่งช่วยให้สามารถประมวลผลที่ได้รับการควบคุมภายใต้เงื่อนไขแฉพาะได้

8) การใช้การแฝงข้อมูลจีดีพีอาร์สามารถเปิดใช้งานการชดเชยตามสหภาพยุโรปสำหรับความล้มเหลวในการเปิดเผยข้อมูลอย่างเหมาะสม: หากข้อมูลไม่ได้ใช้การแฝงข้อมูลอย่างเหมาะสมตามมาตรฐานจีดีพีอาร์ บุคคลในสหภาพยุโรปมีสิทธิ์ขอการชดเชย ซึ่งสะท้อนถึงแนวทางที่เข้มงวดของกฎระเบียบในการปกป้องข้อมูล

9) การใช้การแฝงข้อมูลของจีดีพีอาร์เป็นตัวอย่างหนึ่งของการควบคุมความน่าเชื่อถือแบบกระจาย: แนวคิดนี้บอกเป็นนัยว่าการใช้การแฝงข้อมูลภายใต้จีดีพีอาร์เป็นส่วนหนึ่งของกลไกความน่าเชื่อถือแบบกระจาย ซึ่งช่วยในการเปิดใช้กระแสข้อมูลที่เชื่อถือได้ ในขณะเดียวกันก็ปกป้องความเป็นส่วนตัวของแต่ละบุคคล

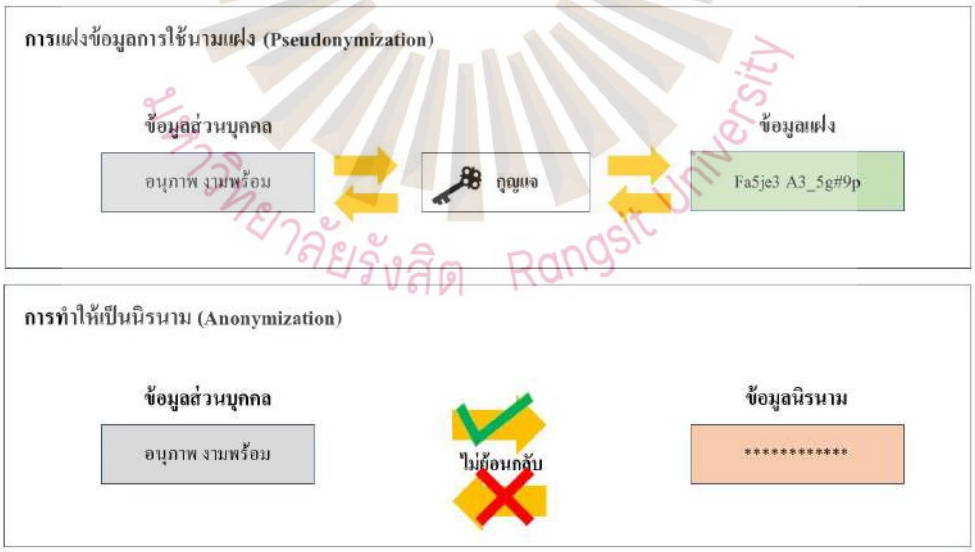
10) การใช้การแฝงข้อมูลของจีดีพีอาร์ช่วยให้เกิดประโยชน์ตามกฎหมายจีดีพีอาร์มากมาย: การใช้การแฝงข้อมูลที่เหมาะสมสามารถช่วยให้องค์กรปฏิบัติตามภาระผูกพันต่าง ๆ ของจีดีพีอาร์ เช่น การลดขนาดข้อมูล และอาจเป็นปัจจัยในการลดบทลงโทษในกรณีของการละเมิดข้อมูล

เนื่องจากการโจมตีเพื่อระบุตัวตนซ้ำอีกครั้งยังคงพัฒนาและมีความซับซ้อนมากขึ้น การโจมดีดังกล่าวจึงเป็นภัยคุกคามที่สำคัญต่อความเป็นส่วนตัวของแต่ละบุคคล แม้แต่ข้อมูลที่ในตอนแรกถือว่าไม่ใช่ข้อมูลส่วนบุคคลหรือไม่เป็นอันตรายก็สามารถเปลี่ยนให้เป็นข้อมูลที่สามารถระบุตัวบุคคลได้ภายใต้สถานการณ์ที่เหมาะสมและด้วยเทคนิคที่เหมาะสม ความสามารถในการโจมตีการระบุตัวตนซ้ำอีกครั้งที่เพิ่มขึ้นอย่างต่อเนื่องนี้ทำให้เกิดข้อกังวลไม่เพียงแต่สำหรับบุคคลที่อาจถูกละเมิดความเป็นส่วนตัว แต่ยังรวมถึงองค์กรและสถาบันที่รับผิดชอบในการจัดการข้อมูลตามกฎหมายและข้อบังคับด้านความเป็นส่วนตัวด้วย (Teodora & Lodie, 2023, p. 1)

2.6.4 การเปรียบเทียบระหว่างการทำให้เป็นนิรนามและการแฝงข้อมูล (Anonymization vs Pseudonymization)

ความแตกต่างที่เห็นได้ชัดระหว่างแนวความคิดทั้งสอง คือ การแฝงข้อมูล หมายความว่า บุคคลยังคงสามารถระบุตัวตนได้ผ่านข้อมูลทางอ้อมหรือข้อมูลเพิ่มเติม ซึ่งหมายความว่า ข้อมูลส่วนบุคคลที่ใช้การแฝงข้อมูลยังคงอยู่ในขอบเขต แต่การทำให้เป็นนิรนาม หมายถึงการไม่สามารถกู้คืนข้อมูลต้นฉบับได้และข้อมูลดังกล่าวอยู่นอกขอบเขตของ GDPR (Tinabo, Mtenzi, & O' Shea, 2009, pp. 1-6) มีรายละเอียดดังนี้

รูปที่ 2.17 แสดงให้เห็นถึงกระบวนการทำงานของการแฝงข้อมูลและการทำให้เป็นนิรนาม ว่าเทคนิคทั้งสองทำงานอย่างไร แม้ว่าการแฝงข้อมูลและการทำให้เป็นนิรนามจะใช้เพื่อปกป้องข้อมูลส่วนตัวของแต่ละบุคคล แต่ก็ไม่ได้ใช้คำพ้องความหมาย ด้วยเทคนิคการแฝงข้อมูลหากได้รับอนุญาตให้เข้าถึงข้อมูลนั้น ก็จะมีรหัสที่จะช่วยให้คุณยกเลิกการระบุข้อมูลได้ แต่ในทางตรงกันข้ามเทคนิคการทำให้เป็นนิรนามเป็นเทคนิคที่เปลี่ยนแปลงข้อมูลอย่างถาวร ดังนั้นบุคคลจึงไม่สามารถระบุตัวตนได้ทั้งทางตรงหรือทางอ้อม



รูปที่ 2.17 แสดงกระบวนการทำงานของการแฝงข้อมูลและการทำให้เป็นนิรนาม

ที่มา: Data Privacy Manager, 2021

ตารางที่ 2.5 เปรียบเทียบลักษณะเฉพาะของเทคนิคการทำให้เป็นนิรนามและการแฝงข้อมูล

การทำให้เป็นนิรนาม	การแฝงข้อมูล
การไม่มีชื่อปรากฏ	การใช้ชื่อปลอม (นามแฝง)
ไม่มีการเชื่อมโยงข้อมูลที่ปกปิดกับข้อมูลต้นฉบับ	เปิดใช้งานการเชื่อมโยงข้อมูลที่เกี่ยวข้องกับตัวตนปลอม (Pseudo-Identities) ภายใต้เงื่อนไขเฉพาะ
ใช้งานง่าย	ไม่ง่ายที่จะนำไปใช้งาน
ส่วนใหญ่นิยมใช้	ส่วนใหญ่ไม่นิยมใช้

ที่มา: Tinabo, Mtenzi, & O' Shea, 2009

เป็นการยากที่จะบอกได้ว่าเทคนิคใดเป็นเทคนิคที่ดีที่สุด ในทางปฏิบัติเทคนิคเดียวกันอาจมีระดับความเสี่ยงที่ต่างกันในกรณีใช้งานที่ต่างกัน ผู้ควบคุมข้อมูลจำเป็นต้องพิจารณาการใช้งานข้อมูลประกอบผ่านการประเมินความเสี่ยงในรูปแบบที่ยกมาข้างต้น ในเบื้องต้นอาจพิจารณาตามตารางที่ 2.6 ที่แสดงภาพรวมความเสี่ยงของกระบวนการป้องกันข้อมูลทั้ง 8 เทคนิคตามที่ได้กล่าวไว้ข้างต้น (Service of the Republic of Poland, 2018, pp. 23-24)

ตารางที่ 2.6 ภาพรวมแสดงความเสี่ยงของการป้องกันข้อมูลแต่ละเทคนิค

วิธีการ	การถูกแยกตัวออกมายังคงมีความเสี่ยง	ความสามารถในการเชื่อมโยงยังคงมีความเสี่ยง	การอนุมานยังคงมีความเสี่ยง
การเพิ่มการรบกวน	ใช่	อาจจะไม่	อาจจะไม่
การเรียงสับเปลี่ยน	ใช่	ใช่	อาจจะไม่
การรวมกลุ่มและการทำ k-Anonymization	ไม่ใช่	ใช่	ใช่
การทำ L-diversity	ไม่ใช่	ใช่	อาจจะไม่
ความเป็นส่วนตัวที่แตกต่างกัน	อาจจะไม่	อาจจะไม่	อาจจะไม่
การทำโทเค็น	ใช่	ใช่	อาจจะไม่
การแฝงข้อมูล	ใช่	ใช่	ใช่

ที่มา: Service of the Republic of Poland, 2018

มหาวิทยาลัยรังสิต Rangsit University

2.6.5 การออกแบบสถาปัตยกรรมการใช้การแฝงข้อมูลบนบล็อกเชน (Architecture design for Pseudonymization on Blockchain)

เนื่องจากคุณสมบัติที่แข็งแกร่งของเทคโนโลยีบล็อกเชน งานวิจัยฉบับนี้ตั้งใจที่จะใช้แนวคิดบล็อกเชนกับความเป็นส่วนตัวของข้อมูล ข้อมูลบนเทคโนโลยีบล็อกเชนนั้นทนทานต่อการดัดแปลงและแก้ไขได้ยาก จากข้อกำหนดของจีดีพีอาร์ ทำให้บล็อกเชนสาธารณะไม่เป็นไปตามข้อกำหนดของจีดีพีอาร์ รวมถึงบทความวิจัยที่ 14, 15 และ 8 (Zemler, 2019, pp. 96-107)

จากบทความวิจัยที่ 14 เจ้าของข้อมูลมีสิทธิ์แก้ไขข้อมูลหากเชื่อว่าไม่ถูกต้อง หากเจ้าของข้อมูลเชื่อว่าข้อมูลปัจจุบันผิดพลาดหรือไม่สมบูรณ์พวกเขาสามารถอัปเดตข้อมูลใหม่และเปลี่ยนผู้ควบคุมข้อมูลใด ๆ ที่มีอยู่แล้ว จากหัวข้อนี้บล็อกเชนเพียงอย่างเดียวใช้ไม่ได้เนื่องจากข้อมูลในบล็อกเชนสาธารณะนั้นเปลี่ยนแปลงได้ยาก ตารางเสริมทั้งหมดในบล็อกเชนถูกประกอบขึ้นใหม่เพื่ออัปเดตข้อมูลและทำกระบวนการซ้ำ เชนในบล็อกเชนจะเก็บข้อมูลที่อัปเดตล่าสุดในกล่องสุดท้ายและเก็บประวัติไว้ในเชนด้วย

จากบทความวิจัยที่ 15 ระบุว่าสามารถลบข้อมูลออกจากบล็อกเชนได้ ดังนั้นเจ้าของข้อมูล/อาสาสมัครจึงไม่สามารถใช้สิทธิ์ในการลบข้อมูลในบล็อกเชนได้ ผู้ควบคุมข้อมูลไม่สามารถจัดเก็บข้อมูลส่วนบุคคลของประชากรสหภาพยุโรปบนบล็อกเชนได้ ด้วยเหตุนี้ งานวิจัยฉบับนี้จึงเลือกบล็อกเชนเป็นระบบช่วยเหลือ เครื่องคอมพิวเตอร์แม่ข่ายสำหรับฐานข้อมูลเก็บข้อมูลทั้งหมดซึ่งเป็นตัวควบคุมส่วนกลาง เมื่อข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่ายถูกลบ ลิงค์บนบล็อกเชนก็จะไม่ถูกต้องและไม่มีประโยชน์อีกต่อไป

ในที่สุด จากบทความวิจัยที่ 8 (Haque, Islam, Hyrynsalmi, Nagvi, & Smolander, 2021, pp. 50593-50606) ให้สิทธิ์ในการจำกัดวิธีการควบคุมข้อมูลในการประมวลผลข้อมูล เนื่องจากทุกคนสามารถใช้บล็อกเชนสาธารณะได้ จึงไม่เป็นไปตามมาตรา 18 ของจีดีพีอาร์ วิธีการแก้ปัญหาสำหรับมาตราที่ 18 นั้นคือ บล็อกเชนที่ได้รับอนุญาตแทนบล็อกเชนสาธารณะ บล็อกเชนที่ได้รับอนุญาตนั้นจำกัดไว้เฉพาะบุคคลที่ได้รับอนุญาตให้เข้าถึงเท่านั้น หรือกล่าวอีกนัยหนึ่งก็คือบล็อกเชนที่อนุญาตนั้นไม่ได้มีไว้สำหรับเข้าถึงแบบสาธารณะ

ในขอบเขตของเทคโนโลยีบล็อกเชน ความแตกต่างระหว่างบล็อกเชนสาธารณะและบล็อก

เชนที่ได้รับอนุญาตเป็นสิ่งสำคัญ โดยเฉพาะอย่างยิ่งเมื่อกล่าวถึงการจัดการและความเป็นส่วน ตัวของข้อมูล บล็อกเชนสาธารณะเป็นเครือข่ายแบบเปิดซึ่งหมายความว่าใครก็ตามที่มีการเชื่อมต่ออินเทอร์เน็ตก็สามารถเข้าร่วมเครือข่าย ทำธุรกรรม และดูข้อมูลใด ๆ ที่เก็บไว้ในบล็อกเชนได้ซึ่งลักษณะที่เปิดกว้างของบล็อกเชนสาธารณะ ขณะเดียวกันก็ส่งเสริมความโปร่งใสและการไม่เปลี่ยนแปลง ถือเป็นดาบสองคมเมื่อกล่าวถึงความเป็นส่วนตัว ข้อมูลทุกชิ้นบนบล็อกเชนจะถูกเปิดเผยต่อใครก็ตามที่มีส่วนร่วมในเครือข่ายซึ่งอาจเป็นปัญหาสำหรับข้อมูลส่วนบุคคลหรือข้อมูลที่ละเอียดอ่อน การไม่จำกัดการเข้าถึงบนบล็อกเชนสาธารณะทำให้ไม่เหมาะสำหรับแอปพลิเคชันที่ต้องการรักษาความลับของข้อมูล ในส่วนบล็อกเชนที่ได้รับอนุญาตนั้น เพื่อตอบสนองต่อความท้าทายด้านความเป็นส่วนตัวที่เกิดจากบล็อกเชนสาธารณะ บล็อกเชนที่ได้รับอนุญาตจึงนำเสนอสภาพแวดล้อมที่มีการควบคุมมากขึ้น สิ่งเหล่านี้เรียกอีกอย่างว่า “บล็อกเชนส่วนตัว” การเข้าถึงบล็อกเชนที่ได้รับอนุญาตนั้นถูกจำกัดและต้องได้รับอนุญาต กลไกการดูแล เงื่อนไขเหล่านี้ทำให้มั่นใจได้ว่าเฉพาะบุคคลหรือหน่วยงานที่ได้รับการตรวจสอบและอนุมัติเท่านั้นที่สามารถเข้าร่วมในเครือข่ายได้ ลักษณะเฉพาะของบล็อกเชนที่ได้รับอนุญาตทำให้เหมาะสำหรับองค์กรและองค์กรที่ต้องการรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล จากคุณสมบัติข้างต้นของบล็อกเชนที่ได้รับอนุญาตจึงถูกใช้เป็นระบบเสริมหรือระบบช่วยเหลือเพื่อวัตถุประสงค์ดังนี้

2.6.5.1 วัตถุประสงค์ที่ 1: โครงการเชื่อมโยงข้อมูล

ภายในกรอบงานบล็อกเชนที่ได้รับอนุญาต รูปแบบการเชื่อมโยงข้อมูลเป็นระบบที่ออกแบบมาเพื่อจัดการข้อมูลส่วนบุคคลอย่างปลอดภัย ระบบนี้เกี่ยวข้องกับเครื่องแม่ข่ายที่ปลอดภัยซึ่งมีการควบคุมการเข้าถึงแบบจำกัด ซึ่งหมายความว่าเฉพาะบุคลลที่ได้รับอนุญาตเท่านั้นที่สามารถอ่านหรือเขียนไปยังเครื่องแม่ข่ายได้ เครื่องแม่ข่ายนี้จัดเก็บข้อมูลส่วนบุคคลอย่างปลอดภัยและในลักษณะที่ไม่เปิดเผยต่อสาธารณะหรือเข้าถึงได้ การเชื่อมโยงที่ปลอดภัยทำให้มั่นใจได้ถึงความเป็นส่วนตัวในขณะที่ยังรักษาความสมบูรณ์และตรวจสอบข้อมูลได้ ซึ่งเป็นข้อได้เปรียบที่สำคัญของเทคโนโลยีบล็อกเชน

2.6.5.2 วัตถุประสงค์ที่ 2: การเข้าถึงแบบจำกัด

การจงใจจำกัดผู้ที่สามารถดูหรือโต้ตอบกับข้อมูลได้ การเข้าถึงที่จำกัดนี้ไม่ได้เป็นเพียงผลพลอยได้แต่เป็นคุณลักษณะที่ออกแบบของบล็อกเชนที่ได้รับอนุญาต ด้วยการควบคุมการเข้าถึง ระบบจะทำให้แน่ใจว่าเฉพาะผู้มีส่วนได้ส่วนเสียหรือฝ่ายที่จำเป็นตามกฎหมายเท่านั้นจึงจะสามารถโต้ตอบกับข้อมูลได้ ซึ่งอาจรวมถึงผู้เข้าร่วมในห่วงโซอุปทาน บุคลากรที่ได้รับ

อนุญาตในระบบการดูแลสุขภาพ หรือ สถาบันการเงินที่จัดการธุรกรรมที่ละเอียดอ่อน การควบคุมการเข้าถึงแบบจำกัดเป็นส่วนสำคัญในการปฏิบัติตามกฎระเบียบ การปฏิบัติตามกฎหมายคุ้มครองข้อมูล และการรักษาความลับในการปฏิบัติงานตามที่จำเป็น

ฟังก์ชันแฮชเป็นอัลกอริทึมการเข้ารหัสที่แปลงข้อมูลนำเข้าให้เป็นสตริงอักขระที่มีขนาดคงที่ซึ่งก็คือแฮช กระบวนการนี้ทำหน้าที่เป็นเครื่องมือสำหรับทั้งความปลอดภัยและความสมบูรณ์ของข้อมูลภายในเครือข่ายที่เกี่ยวข้องกับหลายโหนดและเครื่องแม่ข่ายฐานข้อมูลกลาง โดยมีคุณสมบัติหลักของฟังก์ชันแฮช ดังนี้ (Lapwattanaworakul, Srisa-An, & Aribarg, 2023, p. 2472)

1) ฟังก์ชันทางเดียว (One-way Function): ฟังก์ชันแฮชถูกอธิบายว่าเป็นแบบทางเดียว เนื่องจากได้รับการออกแบบให้ไม่สามารถย้อนกลับได้ ซึ่งหมายความว่าเมื่อข้อมูลถูกส่งผ่านฟังก์ชันแฮชแล้ว ผลลัพธ์ (ค่าแฮช) จะไม่สามารถ “ถอดรหัส” กลับเข้าไปนข้อมูลต้นฉบับได้ สิ่งนี้ช่วยต้นฉบับได้ สิ่งนี้ช่วยปกป้องการรักษาความลับของข้อมูลเพราะแม้ว่าผู้อื่นจะเห็นแฮช แต่ก็ไม่สามารถแปลงกลับเป็นรูปแบบดั้งเดิมได้

2) พิสูจน์ความถูกต้อง (A Hush function can be prove): ฟังก์ชันแฮชมีความอ่อนไหวต่อการเปลี่ยนแปลงข้อมูลนำเข้า ค่าแฮชที่ถูก ต้องสามารถยืนยันได้ว่าไฟล์หรือการป้อนข้อมูลไม่มีการเปลี่ยนแปลงนับตั้งแต่แฮชถูกสร้างขึ้น หากไฟล์ถูกแก้ไข การเปลี่ยนแปลงเพียงเล็กน้อยก็ส่งผลให้เกิดแฮชที่แตกต่างไปจากเดิมอย่างสิ้นเชิง ดังนั้น ด้วยการเปรียบเทียบค่าแฮชในการช่วงเวลาหนึ่งเราจึงสามารถตรวจจับการแก้ไขข้อมูลที่ได้ รับอนุญาตได้

การประยุกต์ใช้ในการจัดการข้อมูลและความเป็นส่วนตัว: ระบบที่อธิบายไว้ใช้แฮชเพื่อเชื่อมโยงข้อมูลบนเครื่องแม่ข่ายไปยังรายการที่เกี่ยวข้องอย่างปลอดภัย (แฮชของกล่อง) เมื่อผู้ควบคุมข้อมูลของระบบ (หน่วยงานที่รับผิดชอบในการจัดการข้อมูล) ได้รับคำขอให้ลบข้อมูล ซึ่งเป็นกระบวนการที่เป็นส่วนหนึ่งของสิทธิ์ที่ได้รับตามกฎหมายความเป็นส่วนตัว เช่น จีดีพีอาร์ ข้อมูลจริงจะถูกลบออกจากเครื่องแม่ข่ายหลัก หลังจากการลบแฮชที่เกี่ยวข้องจะกลายเป็นรายการที่ถูกละเลยซึ่งไม่มีข้อมูลที่เกี่ยวข้องที่จะตรวจสอบอีกต่อไป ด้วยเหตุนี้แฮชจึงไม่มีประสิทธิภาพ มันไม่มีวัตถุประสงค์ในทางปฏิบัติเพราะไม่มีข้อมูลต้นฉบับที่จะตรวจสอบหรือเป็นตัวแทน ในบริบทของกฎระเบียบด้านความเป็นส่วนตัว แฮชที่ไม่มีข้อมูลที่เกี่ยวข้องจะไม่ถือว่าเป็น “ข้อมูลส่วนบุคคล” ข้อมูลส่วนบุคคลหมายถึงข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม หากไม่มี

ข้อมูลต้นฉบับแฮชจะไม่สามารถใช้เพื่อระบุบุคคลได้ ซึ่งจะทำให้แฮชเป็นนิรนามได้อย่างมีประสิทธิภาพและสอดคล้องกับข้อกำหนดในการลบข้อมูล

2.7 วิธีการสำรวจวรรณกรรม

2.7.1 โพรโทคอลการสำรวจ (Survey Protocol)

วิธีการวิจัยที่ผู้วิจัยได้ปฏิบัติตามเพื่อการรวบรวมและทบทวนทางวิชาการและด้านเทคนิค รวมถึงบทความ งานวิจัย วิทยานิพนธ์ เอกสารทางเทคนิค และเนื้อหาในเว็บไซต์ที่เกี่ยวข้อง โพรโทคอลการสำรวจที่ผู้เขียนนำมาใช้นั้นไม่ได้คิดขึ้นเองตั้งแต่ต้น แต่ได้รับแรงบันดาลใจจากชุดแนวทางที่มีอยู่แล้วในงานวิจัยของ Dara Tith สำหรับการพัฒนาโพรโทคอลการทบทวนผู้วิจัยได้ปรับปรุงให้เหมาะสมกับความต้องการและวัตถุประสงค์การวิจัย โดยเริ่มจากการนำเสนอระเบียบวิธีการสำรวจการวิจัยซึ่งเป็นการสรุปขั้นตอน วิธีการ และมาตรฐานที่ใช้ในการรวบรวมและทบทวนวรรณกรรมอย่างเป็นระบบ ดังรูปที่ 2.18 (Tith, 2020, p. 17)

โพรโทคอลการสำรวจได้รับการปรับปรุงเพื่อให้แน่ใจว่าการทบทวนวรรณหรือการสำรวจเป็นไปอย่างเป็นระบบ และรวมเฉพาะเอกสารที่เกี่ยวข้องและมีคุณภาพมากที่สุดเท่านั้นที่จะรวมอยู่ในการทบทวนขั้นสุดท้าย สำหรับการวิเคราะห์ การใช้จุดตัดสินใจตามเกณฑ์เฉพาะจะช่วยปรับแต่งผลการค้นหาและมุ่งเน้นไปที่ข้อมูลที่เกี่ยวข้องมากที่สุดสำหรับเป้าหมายของการสำรวจ สามารถอธิบายทีละขั้นตอนได้ดังนี้

เริ่มต้น: ขั้นตอนเริ่มต้นถือเป็นจุดเริ่มต้นของกระบวนการสำรวจวรรณกรรม

2.7.1.1 ขั้นตอนที่ 1 การค้นหาวรรณกรรมเบื้องต้น:

การท่องอินเทอร์เน็ต: ขั้นตอนนี้เกี่ยวข้องกับการค้นหาวรรณกรรมที่เกี่ยวข้องในอินเทอร์เน็ตซึ่งอาจรวมถึงเอกสารทางวิชาการ วิทยานิพนธ์ และเอกสารทางเทคนิคที่เกี่ยวข้องกับสาขาวิชา

2.7.1.2 ขั้นตอนที่ 2 การคัดกรองเบื้องต้น:

การกรองกระดาษ: เอกสารที่พบระหว่างการค้นหาจะต้องผ่านกระบวนการคัดกรองเบื้องต้น ส่วนบทคัดย่อและบทนำของแต่ละเอกสารจะได้รับการตรวจสอบเพื่อประเมินความ

เกี่ยวข้องตามเกณฑ์การตัดสินใจต่อไปนี้

1) L1: ตรวจสอบว่าเอกสารมีแนวคิดและต้นแบบของระบบรวมศูนย์และกระจายอำนาจสำหรับรูปแบบจำลองการจัดการความยินยอม การแฝงข้อมูล และการปฏิบัติตามกฎระเบียบด้านปกป้องข้อมูล เช่น จีดีพีอาร์ หรือ พีดีพีเอ หรือไม่

2.7.1.3 ขั้นตอนที่ 3 การทบทวนและการจำแนกประเภทโดยละเอียด

การจำแนกประเภทกระดาษ: เอกสารที่ผ่านการคัดกรองเบื้องต้นจะได้รับการตรวจสอบเพิ่มเติม ส่วนบทคัดย่อ บทนำ และการอภิปรายจะได้รับการทบทวนตามเกณฑ์เพิ่มเติมเพื่อพิจารณาความเหมาะสมในการรวมไว้ในการศึกษา

1) L2: ประเมินว่าเอกสารกล่าวถึงต้นแบบของการบริหารจัดการความยินยอมที่ใช้บล็อกเชน และ/หรือ การใช้เทคนิคการแฝงข้อมูลบนบล็อกเชน หรือไม่

2) L3: ค้นหาการอภิปรายเชิงแนวคิดเกี่ยวกับบล็อกเชนเพื่อการจัดการความยินยอม และ/หรือ การใช้เทคนิคการแฝงข้อมูลบนบล็อกเชน เพื่อความสอดคล้องและปฏิบัติตามกฎระเบียบด้านการปกป้องข้อมูล เช่น จีดีพีอาร์ หรือ พีดีพีเอ

3) L4: ค้นหาการอภิปรายเกี่ยวกับรูปแบบจำลองการควบคุมการเข้าถึง

4) L5: ค้นหาข้อมูลเกี่ยวกับการจัดการวัตถุประสงค์ภายในระบบดังกล่าว ที่จุดตัดสินใจแต่ละจุด หากเอกสารไม่ตรงตามเกณฑ์ที่กำหนด เอกสารนั้นจะถูกปฏิเสธ หากผ่านก็จะเข้าเกณฑ์ต่อไป

2.7.1.4 ขั้นตอนที่ 4 การวิเคราะห์ที่ครอบคลุม

การทบทวนรายงานฉบับเต็มและวิทยานิพนธ์: เอกสารที่ตรงตามเกณฑ์การจำแนกประเภททั้งหมดจะต้องได้รับการตรวจสอบฉบับเต็ม โดยมีการตรวจสอบเนื้อหาทั้งหมดของรายงานหรือวิทยานิพนธ์โดยละเอียด นี่คือการวิเคราะห์ที่ครอบคลุมซึ่งอาจรวมถึงวิธีการ ผลลัพธ์ และส่วนข้อสรุป

2.7.1.5 ขั้นตอนที่ 5 การรวบรวมข้อมูลเสริม

การสำรวจบนหน้าเว็บ: นอกเหนือจากวรรณกรรมเชิงวิชาการแล้ว แนวทางการสำรวจยังรวมถึงการค้นหาข้อมูลที่เกี่ยวข้องบนหน้าเว็บ กระดานสนทนา แหล่งข่าว และสื่อต่าง ๆ ที่อาจให้ข้อมูลเสริม เพื่อรวบรวมข้อมูลที่ครอบคลุมในหัวข้อนั้น ขั้นตอนนี้อาจมุ่งเป้าไปที่การรวบรวมการอภิปรายและการพัฒนาล่าสุดที่ยังไม่ได้เผยแพร่อย่างเป็นทางการ

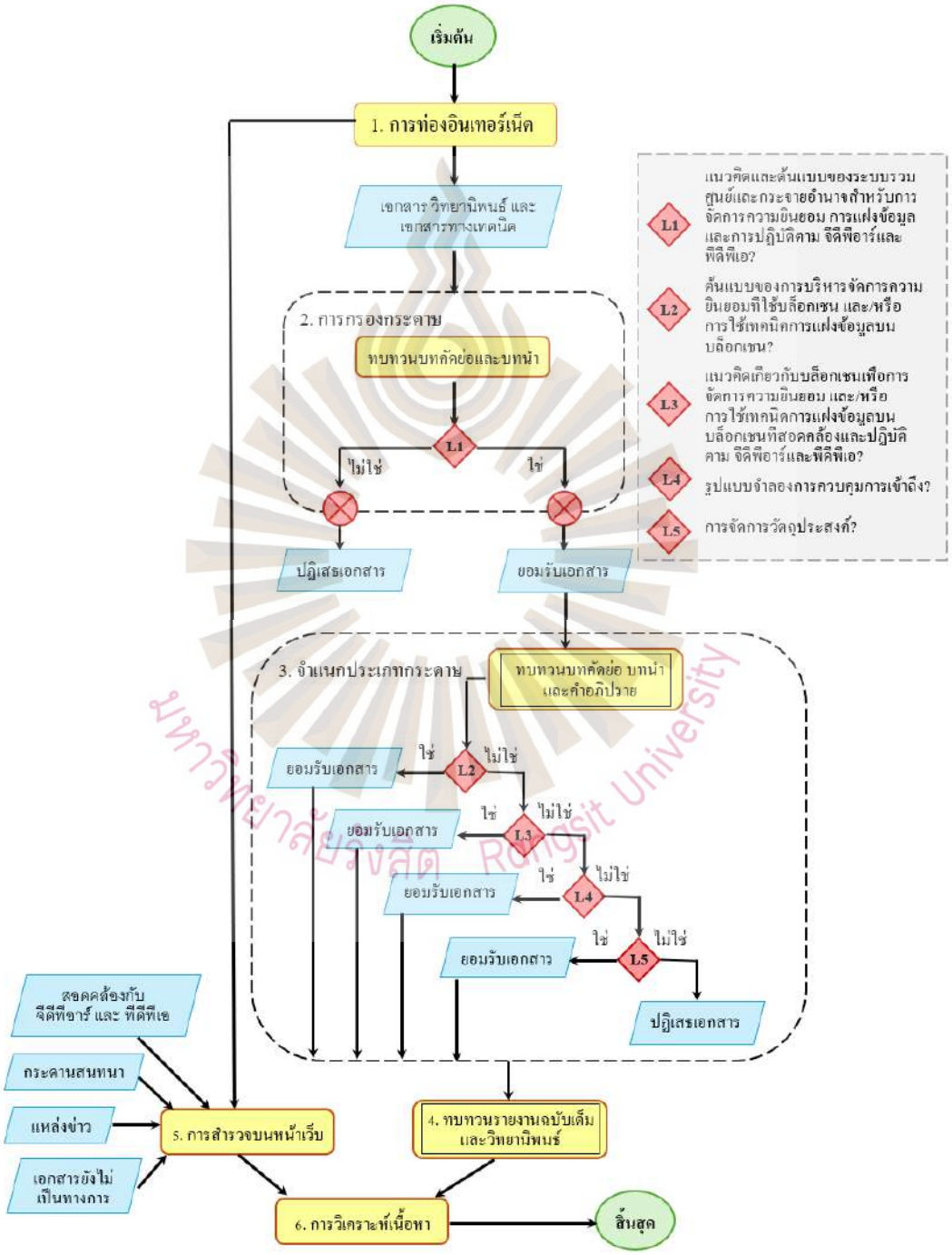
2.7.1.6 ขั้นตอนที่ 6 การสังเคราะห์ขั้นสุดท้าย

การวิเคราะห์เนื้อหา: ขั้นตอนสุดท้ายเกี่ยวข้องกับการวิเคราะห์เนื้อหาอย่างละเอียดของเอกสารและข้อมูลที่ได้รับการยอมรับทั้งหมดที่รวบรวม เป้าหมายคือการสังเคราะห์ผล

การวิจัย สรุปผล และอาจระบุประเด็นสำหรับการวิจัยในอนาคต

2.7.1.7 ขั้นตอนที่ 7 เสร็จสิ้นกระบวนการ

หยุด: ขั้นตอนสุดท้ายแสดงถึงความสมบูรณ์ของโครงร่างการวิจัยวรรณกรรม



รูปที่ 2.18 โพรโทคอลการสำรวจ

ที่มา: Tith, 2020

2.7.2 งานวิจัยที่เกี่ยวข้อง

ในงานวิจัยของ Suripeddi and Purandare (2021, p. 10) ได้ทำการศึกษาเพื่อตรวจสอบความเข้ากันได้ระหว่างเทคโนโลยีบล็อกเชนและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (จีดีพีอาร์) ผลการศึกษาพบว่ามีปัญหาความเข้ากันได้ระหว่างบทความบางบทความในจีดีพีอาร์และคุณสมบัติของเทคโนโลยีบล็อกเชน กล่าวอีกนัยหนึ่งคือ แง่มุมต่าง ๆ ของจีดีพีอาร์ดูเหมือนจะขัดแย้งหรือไม่สอดคล้องกับคุณสมบัติและฟังก์ชันการทำงานของบล็อกเชน โดยเฉพาะอย่างยิ่งหลักการ “สิทธิในการถูกลืม (Right to be Forgotten)” ซึ่งขัดกับคุณลักษณะของบล็อกเชนที่มุ่งเน้นความไม่เปลี่ยนแปลงของข้อมูล นอกจากนี้ ประเด็นเรื่องการกำหนดตัวผู้ควบคุมข้อมูลภายในเครือข่ายบล็อกเชนแบบกระจายอำนาจก็เป็นอีกหนึ่งความท้าทาย เนื่องจากไม่มีหน่วยงานกลางที่สามารถรับผิดชอบการจัดการข้อมูลได้โดยตรง สิ่งนี้ชี้ให้เห็นว่าการปรับระบบบล็อกเชนให้สอดคล้องกับข้อกำหนดของจีดีพีอาร์อาจต้องอาศัยแนวทางใหม่ ๆ เช่น การใช้โซลูชันบล็อกเชนแบบผสมผสาน (Hybrid Blockchain Solution) หรือการนำเทคนิคเช่น Zero-Knowledge Proofs และ Off-Chain Storage มาช่วยลดผลกระทบของข้อจำกัดเหล่านี้

ความกังวลของ Mohanta, Jena, Panda, and Sobhanayak (2019, pp. 1-19) นั้นมุ่งเน้นไปที่ความท้าทายด้านความเป็นส่วนตัวที่เกิดจากการต่อต้านการเปลี่ยนแปลงข้อมูลโดยธรรมชาติของบล็อกเชน บล็อกเชนได้รับการออกแบบมาเพื่อการจัดเก็บข้อมูลที่มีการกระจายศูนย์และความโปร่งใส ช่วยให้มั่นใจถึงความไม่เปลี่ยนแปลงผ่านกลไกการแฮชชิงที่เข้ารหัสลับและข้อตกลงร่วมกัน ในขณะที่เพิ่มความปลอดภัยของระบบ ความไม่เปลี่ยนแปลงนี้ก่อให้เกิดปัญหาความเป็นส่วนตัวโดยเฉพาะอย่างยิ่งในการปฏิบัติตามสิทธิ์ เช่น การลบที่ระบุไว้ในจีดีพีอาร์ ฐานข้อมูลแบบเดิมอนุญาตให้แก้ไขข้อมูลได้อย่างตรงไปตรงมา แต่การเปลี่ยนแปลงข้อมูลบล็อกเชนจะยากเป็นพิเศษเมื่อเพิ่มลงในบล็อก ยิ่งไปกว่านั้น งานวิจัยนี้ยังระบุว่าความโปร่งใสของบล็อกเชนอาจนำไปสู่การเปิดเผยข้อมูลที่ละเอียดอ่อนของผู้ใช้ แม้ว่าข้อมูลจะถูกเก็บในรูปแบบแฮชหรือเข้ารหัสไว้ก็ตาม แต่การวิเคราะห์ธุรกรรมแบบออฟเชนหรือการเชื่อมโยงข้อมูลจากแหล่งอื่น อาจช่วยให้สามารถระบุตัวตนของบุคคลได้โดยอ้อม นอกจากนี้ การใช้สัญญาอัจฉริยะซึ่งดำเนินการซึ่งดำเนินการโดยอัตโนมัติตามเงื่อนไขที่กำหนดไว้อาจยิ่งทำให้เกิดความเสี่ยงด้านความเป็นส่วนตัว หากไม่ได้รับการออกแบบให้คำนึงถึงข้อจำกัดด้านข้อมูลส่วนบุคคล ปัญหาเหล่านี้ชี้ให้เห็นถึงความจำเป็นในการพัฒนาแนวทางใหม่เพื่อลดผลกระทบของข้อจำกัดด้านความเป็นส่วนตัวที่เกิดจากธรรมชาติของบล็อกเชน

ในงานวิจัยของ Melin (2019, pp. 45-46) ชี้ให้เห็นว่าบล็อกเชนส่วนตัวแตกต่างจากวิธีการทั่วไป มีความสามารถในการเพิ่มความปลอดภัยและความเป็นส่วนตัวต่างจากบล็อกเชนสาธารณะ ซึ่งเปิดเผยข้อมูลแก่ผู้เข้าร่วมทุกคน บล็อกเชนส่วนตัวจำกัดการเข้าถึงเฉพาะหน่วยงานที่ได้รับอนุญาตเท่านั้น การเข้าถึงที่มีการควบคุมนี้สามารถเสริมความปลอดภัยได้โดยการจำกัดการเปิดเผยข้อมูลที่ละเอียดอ่อน นอกจากนี้การยืนยันในการลดความเสี่ยงของการรวบรวมข้อมูลที่ได้เหมาะสมหมายความว่า บล็อกเชนส่วนตัวอาจให้การควบคุมการเข้าถึงและการแบ่งปันข้อมูลได้มากขึ้น ลดโอกาสที่บุคคลไม่ได้รับอนุญาตจะรวบรวมหรือใช้ข้อมูลในทางที่ผิด การวิพากษ์วิจารณ์การรวมศูนย์การจัดเก็บข้อมูลส่วนบุคคล ในแนวทางปฏิบัติในปัจจุบัน ชี้ให้เห็นว่าบล็อกเชนส่วนตัวที่มีลักษณะการกระจายศูนย์ นำเสนอทางเลือกที่ดีกว่าการจัดเก็บข้อมูลแบบรวมศูนย์มักจะเผชิญกับการละเมิดความปลอดภัยและการเข้าถึงที่ไม่ได้รับอนุญาต ในขณะที่บล็อกเชนส่วนตัวมีเป้าหมายที่จะแก้ไขข้อกังวลเหล่านี้ โดยการกระจายข้อมูลไปยังผู้เข้าร่วมที่เชื่อถือได้ ซึ่งอาจปรับปรุงมาตรการรักษาความปลอดภัยและความเป็นส่วนตัว

คำแนะนำของ Zhang, Xue, and Liu (2020, pp. 17, 25) เกี่ยวข้องกับการนำแนวคิดการแฝงข้อมูลไปใช้โดยมีเป้าหมายเพื่อปกป้องชื่อจริงของผู้ใช้โดยเฉพาะ การใช้การแฝงข้อมูลถูกนำมาใช้เป็นวิธีการร่วมสมัยในการปกปิดตัวตนในขณะที่ยังคงรักษาทรัพย์สินส่วนตัว แนวทางนี้นำเสนอวิธีการที่เหมาะสมยิ่งในการปกป้องข้อมูลส่วนตัวของผู้ใช้ โดยไม่ต้องอาศัยการไม่เปิดเผยตัวตนโดยสมบูรณ์ ในบริบทของเทคโนโลยีบล็อกเชน พวกเขาได้ทบทวนกลไกฉันทามติการพิสูจน์ด้วยการมีอำนาจ (Proof of Authority - PoA) ซึ่งถูกระบุว่าเป็นกลไกฉันทามติที่อำนวยความสะดวกแก่ผู้ตรวจสอบในการอนุมัติธุรกรรมภายในเครือข่ายบล็อกเชนอย่างรวดเร็ว การประยุกต์ใช้แนวคิดเหล่านี้ในทางปฏิบัติแสดงให้เห็นผ่านการจัดตั้งเครือข่ายบล็อกเชนส่วนตัวชื่อ “เอ็กซ์เชน (xChain)” ซึ่งทำหน้าที่เป็นระบบช่วยเหลือที่ใช้กลไกฉันทามติการพิสูจน์ด้วยการมีอำนาจ จุดประสงค์คือการรวมการแฝงข้อมูลและการพิสูจน์ด้วยการมีอำนาจเพื่อเพิ่มความเป็นส่วนตัวและประสิทธิภาพการอนุมัติธุรกรรมภายในเครือข่ายบล็อกเชน จัดการกับข้อกังวลที่เกี่ยวข้องกับการปกป้องข้อมูส่วนตัวและความเร็วของธุรกรรม

ในงานวิจัยของ Zou et al. (2021, pp. 2085-2106) เน้นย้ำถึงการยอมรับการพัฒนาโปรแกรมประยุกต์บนบล็อกเชนผ่านการใช้สัญญาอัจฉริยะ ได้รับการยอมรับอย่างรวดเร็วและแพร่หลายนับ ตั้งแต่มีการแนะนำแนวคิดที่ก้าวล้ำนี้โดย Nick Szabo ในปีพ.ศ. 2533 ซึ่งถือเป็นการเปลี่ยนแปลงครั้งสำคัญในการดำเนินการตามข้อตกลงในยุคดิจิทัล วิวัฒนาการนี้โดดเด่นด้วยการ

ยอมรับในวงกว้างถึงประโยชน์ที่เป็นไปได้ของสัญญาอัจฉริยะ ส่งผลให้มีการบูรณาการเข้ากับภาคส่วนที่หลากหลายและมีส่วนช่วยในการพัฒนาเทคโนโลยีบล็อกเชนอย่างต่อเนื่อง งานวิจัยนี้ยังระบุว่าการใช้สัญญาอัจฉริยะในภาคส่วนต่าง ๆ เช่น การเงิน ห่วงโซ่อุปทาน บริการสุขภาพ และการจัดการเอกลักษณ์ดิจิทัล ก่อให้เกิดทั้งโอกาสและความท้าทาย แม้ว่าจะช่วยลดต้นทุนธุรกรรม เพิ่มความโปร่งใส และลดการพึ่งพาตัวกลางแต่สัญญาอัจฉริยะยังเผชิญกับปัญหาด้านความปลอดภัย เช่น ช่องโหว่ในชุดคำสั่งที่อาจถูกโจมตีจากนักโจรกรรมข้อมูล และข้อจำกัดด้านความเป็นส่วนตัวเนื่องจากข้อมูลธุรกรรมสามารถตรวจสอบได้บนบล็อกเชน นอกจากนี้ ปัญหาด้านกฎหมายและการบังคับใช้สัญญาอัจฉริยะก็เป็นอีกประเด็นสำคัญ เนื่องจากชุดคำสั่งไม่สามารถคำนึงถึงความซับซ้อนทางกฎหมายหรือเงื่อนไขที่เปลี่ยนแปลงได้อย่างยืดหยุ่น

ในงานวิจัยของ Zyskind, Nathan, and Pentland (2015, pp. 180-184) เสนอโพรโทคอลใหม่ซึ่งใช้เทคโนโลยีบล็อกเชนเป็นผู้จัดการโหนด โพรโทคอลนี้ออกแบบมาเพื่อจัดการการเก็บ การสืบค้น และการแบ่งปันข้อมูลที่ละเอียดอ่อน โดยให้ความสำคัญกับการปฏิบัติตามมาตรฐานการกำกับดูแลที่เข้มงวด โพรโทคอลนี้แสดงถึงแนวทางบุกเบิกในการจัดการข้อมูล โดยใช้ประโยชน์จากธรรมชาติของบล็อกเชนที่มีการกระจายอำนาจและความโปร่งใส เพื่อจัดการกับความท้าทายที่เกี่ยวข้องกับการจัดการข้อมูลที่ละเอียดอ่อน ในขณะเดียวกันก็ปฏิบัติตามมาตรฐานการกำกับดูแลที่เข้มงวด นอกจากนี้ งานวิจัยยังชี้ให้เห็นว่าโพรโทคอลดังกล่าวสามารถช่วยให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น จีดีพีอาร์ ได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในการปฏิบัติตามหลักการ Data Minimization และ User Consent ซึ่งเป็นข้อกำหนดสำคัญของกฎหมายดังกล่าว อย่างไรก็ตาม ความท้าทายยังคงอยู่ในแง่ของการปรับใช้ในวงกว้าง เช่น การเพิ่มประสิทธิภาพการประมวลผล การลดค่าใช้จ่ายด้านพลังงาน และการออกแบบกลไกที่ช่วยให้มั่นใจว่าผู้ใช้ทั่วไปสามารถจัดการสิทธิ์ข้อมูลของตนเองได้โดยง่ายโดยไม่ต้องมีความรู้เชิงเทคนิคขั้นสูง

ในงานวิจัยของ Sirur, Nurse, and Webb (2019, pp. 88-95) ได้เน้นไปที่การสำรวจและเสนอคำแนะนำสำหรับการใช้เทคโนโลยีบล็อกเชนเพื่อให้สอดคล้องกับจีดีพีอาร์ การศึกษานี้ครอบคลุมทั้งองค์กรขนาดใหญ่และวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) โดยมุ่งเน้นไปที่แนวทางที่ช่วยให้องค์กรสามารถใช้บล็อกเชนได้อย่างมีประสิทธิภาพ ในขณะที่ยังคงปฏิบัติตามข้อกำหนดการปกป้องข้อมูลที่เข้มงวดของจีดีพีอาร์ การศึกษานี้ชี้ให้เห็นว่าปัญหาหลักของการใช้บล็อกเชนภายใต้กรอบของจีดีพีอาร์อยู่ที่การรักษาสมดุลระหว่างคุณสมบัติของบล็อกเชน เช่น ความไม่เปลี่ยนแปลงของข้อมูลและความโปร่งใสกับข้อกำหนดของจีดีพีอาร์ เช่น สิทธิในการถูกลืม และ

ความสามารถในการแก้ไขหรือจำกัดการประมวลผลข้อมูล ซึ่งเป็นความท้าทายสำคัญ โดยเฉพาะอย่างยิ่งสำหรับองค์กรที่ต้องจัดการข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้ การศึกษายังระบุว่าองค์กรขนาดใหญ่มีแนวโน้มที่จะสามารถนำแนวทางเหล่านี้ไปใช้ได้เร็วกว่าวิสาหกิจขนาดกลางและขนาดย่อม เนื่องจากมีทรัพยากรในการลงทุนด้านเทคโนโลยีและกฎระเบียบมากกว่า อย่างไรก็ตาม สำหรับ SMEs การใช้เครื่องมือและกรอบการทำงานที่ได้รับการพัฒนาให้สอดคล้องกับจีดีพีอาร์ หรือการร่วมมือกับผู้ให้บริการโซลูชันบล็อกเชนที่มีมาตรฐานด้านการปกป้องข้อมูลอาจเป็นทางเลือกที่เหมาะสม

มุมที่ท้าทายที่สุดในการใช้เทคโนโลยีบล็อกเชน คือการรับรองการปฏิบัติตามมาตรา 14 ของจีดีพีอาร์ ซึ่งเกี่ยวข้องกับ “สิทธิ์ที่จะถูกลืม” หรือ “สิทธิในการลบ” หรือ “สิทธิในการลบ” ความท้าทายนี้เกิดจากคุณสมบัติของเทคโนโลยีบล็อกเชนที่ไม่เปลี่ยนแปลง ซึ่งหมายความว่าเมื่อข้อมูลถูกบันทึกลงในบล็อกเชนแล้ว จะไม่สามารถแก้ไขหรือลบออกได้โดยง่าย ซึ่งขัดแย้งกับข้อกำหนดของจีดีพีอาร์ที่ให้สิทธิบุคคลในการร้องขอให้ข้อมูลส่วนบุคคลของตนถูกลบออกจากระบบ การบรรลุการปฏิบัติตามข้อกำหนดในบริบทของบล็อกเชนต้องใช้โซลูชันที่รอบคอบและสร้างสรรค์เพื่อสร้างสมดุลระหว่างสิทธิความเป็นส่วนตัวและข้อจำกัดทางเทคนิคของระบบการกระจายอำนาจและความไม่เปลี่ยนแปลง งานวิจัยของ Mumu, Kappos, & Sumroy (2021, pp. 7-17) ยังเน้นว่าการปฏิบัติตามสิทธิที่จะถูกลืมภายใต้บล็อกเชนนั้นไม่สามารถพิจารณาเฉพาะด้านเทคนิคเพียงอย่างเดียว แต่ต้องรวมถึงการออกแบบนโยบายภายในองค์กร การทำงานร่วมกับหน่วยงานกำกับดูแล และการพัฒนาแนวทางปฏิบัติทางกฎหมายที่ช่วยให้สามารถใช้บล็อกเชนได้โดยไม่ขัดต่อกฎระเบียบด้านความเป็นส่วนตัว

ในงานวิจัยของ Kondova and Erbguth (2020, pp. 342-345) นำเสนอมุมมองหรือวิธีการใหม่ ๆ สำหรับการนำอัตลักษณ์อธิปไตยของตนเอง (Self-Sovereign Identity -SSI) ไปใช้บนบล็อกเชนสาธารณะ โดยเน้นไปที่แพลตฟอร์มไฮเปอร์เลดเจอร์อินดี้ (Hyperledger Indy) โดยเฉพาะ ข้อเสนอนี้มีแนวโน้มที่จะสนับสนุนการสำรวจโซลูชันการระบุตัวตนผ่านบล็อกเชนอย่างต่อเนื่อง โดยมุ่งเน้นไปที่การจัดการกับความท้าทายที่เกี่ยวข้องกับระบบการจัดการข้อมูลประจำตัวแบบรวมศูนย์แบบดั้งเดิม งานวิจัยระบุว่าการนำ SSI ไปใช้บนบล็อกเชนสาธารณะนั้นมีทั้งข้อได้เปรียบและความท้าทาย โดยประเด็นหลักที่ต้องพิจารณา ได้แก่ ความเป็นส่วนตัวและการปฏิบัติตามจีดีพีอาร์ การตรวจสอบและรับรองอัตลักษณ์แบบกระจายศูนย์ และการกำกับดูแลและมาตรฐานสากล นอกจากนี้ การวิจัยนี้ยังชี้ให้เห็นว่าการนำ SSI มาใช้บนบล็อกเชนสามารถช่วยลดปัญหาการโจรกรรมข้อมูลระดับตัวตน (Identity Theft) และช่วยให้บุคคลสามารถควบคุมข้อมูลส่วนตัวของตนเองได้ดี

ขึ้น อย่างไรก็ตาม ยังมีความท้าทายในการปรับใช้ในวงกว้าง โดยเฉพาะอย่างยิ่งการสร้างโครงสร้างพื้นฐานที่รองรับการยอมรับ SSI จากทั้งภาคธุรกิจและภาครัฐ

ในงานวิจัยของ Hristov and Dimitrov (2018, pp. 305-310) ได้เสนอการใช้ไฮเปอร์เลดเจอร์แฟบริค (Hyperledger Fabric) เป็นองค์ประกอบพื้นฐานสำหรับการสร้างกรอบงานที่สอดคล้องกับจีดีพีอาร์ โดยเฉพาะอย่างยิ่งในบริบทของการจัดการข้อมูลส่วนบุคคลที่ต้องการความปลอดภัยและความโปร่งใส อย่างไรก็ตาม งานวิจัยยังได้เน้นย้ำถึงความกังวลเกี่ยวกับการลบข้อมูลจากกล่องประวัติในอดีตบนบล็อกเชน ซึ่งเป็นประเด็นสำคัญ เนื่องจากคุณสมบัติของบล็อกเชนที่ไม่เปลี่ยนแปลงขัดแย่งกับสิทธิที่จะถูกลืม ซึ่งเป็นหลักการสำคัญที่ระบุไว้ในมาตรา 14 ของจีดีพีอาร์ งานวิจัยยังชี้ให้เห็นว่าไฮเปอร์เลดเจอร์แฟบริคมีศักยภาพในการเป็นบล็อกเชนที่สามารถปรับให้สอดคล้องกับจีดีพีอาร์ได้มากกว่าบล็อกเชนสาธารณะ การพัฒนาเทคโนโลยีบล็อกเชนที่สามารถรองรับข้อกำหนดด้านความเป็นส่วนตัวได้อย่างเต็มรูปแบบยังคงเป็นประเด็นที่ต้องมีการศึกษาต่อไปและอาจต้องได้รับการสนับสนุนจากหน่วยงานกำกับดูแลเพื่อกำหนดแนวทางที่เป็นมาตรฐานสำหรับการใช้บล็อกเชนในบริบทของจีดีพีอาร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลอื่น ๆในอนาคต

ในงานวิจัยของ Bernabe, Canovas, Hernandez-Ramos, Moreno, and Skarmeta (2019, pp. 164908, 164909 และ 164934) ได้สำรวจโซลูชันการเข้ารหัสที่ส่งเสริมการไม่เปิดเผยตัวตนในธุรกรรมของผู้ใช้ ซึ่งจำเป็นสำหรับแบบจำลองการระบุตัวตนของอธิปไตยตนเองที่ให้อำนาจแก่บุคคลในการควบคุมข้อมูลของตน งานวิจัยยังระบุถึงปัญหาความเป็นส่วนตัวของบล็อกเชนที่ยังคงมีอยู่ รวมถึงความจำเป็นของระบบต้านทานควอนตัมและการปฏิบัติตามกฎหมาย โดยจะประเมินกลยุทธ์ความเป็นส่วนตัวในปัจจุบัน ผลการศึกษาได้ระบุว่า แม้จะมีความก้าวหน้าแต่ระบบบล็อกเชนที่มีอยู่ก็ไม่สามารถตอบสนองความท้าทายด้านความเป็นส่วนตัวได้อย่างเต็มที่ ซึ่งอาจกระทบต่อสิทธิ์ของผู้ใช้ เช่น การไม่เปิดเผยตัวตน และการลบข้อมูล ผู้วิจัยได้เน้นย้ำถึงการพัฒนาอัลกอริทึมการเข้ารหัสขั้นสูงอย่างเร่งด่วน ซึ่งการปรับปรุงเหล่านี้มีความสำคัญต่อความเป็นส่วนตัวในภาคส่วนต่าง ๆ บทความนี้สนับสนุนการวิจัยที่ยกระดับฟังก์ชันความเป็นส่วนตัวและการปฏิบัติตามกฎระเบียบ โดยส่งเสริมแนวทางการระบุตัวตนที่เน้นความเป็นส่วนตัวและมีอำนาจอธิปไตยในบล็อกเชนอย่างแท้จริง

ในงานวิจัยของ Bonneau et al. (2015, pp. 112 & 116) ได้ทำการทบทวนวิธีการเพิ่มความเป็นส่วนตัวสำหรับบิทคอยน์และสกุลเงินดิจิทัลอื่น ๆ (คริปโทเคอร์เรนซี) การตรวจสอบ

ครอบคลุมประเด็นสำคัญสองประการเกี่ยวกับข้อกังวลด้านความปลอดภัยและความเป็นส่วนตัวภายในขอบเขตของสกุลเงินดิจิทัลที่กระจายอำนาจ ซึ่งสะท้อนให้เห็นถึงความท้าทายและข้อควรพิจารณาที่หลากหลายที่เกี่ยวข้องกับเทคโนโลยีเหล่านี้ รวมถึงแนวทางที่ได้รับการพัฒนาเพื่อปกป้องข้อมูลของผู้ใช้ เช่น CoinJoin, Confidential Transactions และ Zero-Knowledge Proofs ซึ่งเป็นเทคนิคที่ช่วยลดความสามารถในการติดตามธุรกรรม ในขณะที่ยังคงรักษาความโปร่งใสและความถูกต้องของระบบบล็อกเชน

ในงานวิจัยของ Hensriksen-Bulmer and Jeary (2016, pp. 1184–1192) อธิบายถึงการมีอยู่ของแนวโน้มที่เกี่ยวข้องในด้านความเป็นส่วนตัวและความปลอดภัยของข้อมูล โดยเผยให้เห็นว่า ตั้งแต่ปี พ.ศ. 2552 มีเหตุการณ์การ โจมตีเพื่อระบุตัวตนซ้ำอีกครั้งที่ประสบความสำเร็จเกิดขึ้นอย่างน่าสังเกต การโจมตีเหล่านี้เกี่ยวข้องกับความสามารถในการระบุและเชื่อมต่อข้อมูลของบุคคลที่ดูเหมือนจะไม่เปิดเผยตัวตนจากชุดข้อมูลหลายชุดที่เปิดเผยต่อสาธารณะ งานวิจัยชี้ให้เห็นว่า แม้ข้อมูลจะถูกทำให้ดูไม่ระบุตัวตน ผู้ไม่ประสงค์ดียังคงสามารถรวบรวมข้อมูลจากหลายแหล่งเพื่อนำไปใช้เชื่อมโยงและระบุตัวบุคคลที่แท้จริงได้ ซึ่งหมายความว่า การลบหรือแทนที่ข้อมูลระบุตัวบุคคลไม่สามารถรับประกันความเป็นส่วนตัวได้อย่างสมบูรณ์ งานวิจัยยังตอกย้ำว่าความเป็นส่วนตัวของบุคคลอาจตกอยู่ในความเสี่ยง แม้ว่าข้อมูลจะดูไม่ระบุตัวตนก็ตาม เทคโนโลยีการวิเคราะห์ข้อมูลและปัญญาประดิษฐ์ทำให้การระบุตัวตนซ้ำทำได้ง่ายขึ้น ซึ่งทำให้มาตรการปกป้องข้อมูลต้องพัฒนาให้ทันกับภัยคุกคามที่เกิดขึ้น

จากงานวิจัยของ Hewa, Hu, Liyanage, Kanhare, and Ylianttila, (2021, pp. 87643-87662) ได้สำรวจแง่มุมพื้นฐาน ความท้าทาย และทิศทางการวิจัยในอนาคตของสัญญาอัจฉริยะที่ใช้บล็อกเชน โดยเน้นที่คุณสมบัติที่สำคัญ เช่น การกระจายอำนาจ ความไม่เปลี่ยนรูปและความปลอดภัยในการเข้ารหัส ซึ่งช่วยให้เกิดระบบอัตโนมัติที่ไร้ความน่าเชื่อถือในอุตสาหกรรมต่าง ๆ รวมถึงการเงิน การขนส่ง และอินเทอร์เน็ตทุกสรรพสิ่ง การศึกษายังตรวจสอบประเด็นทางเทคนิคที่สำคัญ รวมถึงช่องโหว่ด้านความปลอดภัย (เช่น การโจมตีซ้ำ การโจมดีซีบิล) ข้อกังวลด้านความเป็นส่วนตัว ข้อจำกัดในการขยายขนาด และปัญหาการทำงานพร้อมกัน นอกจากนี้ ยังกล่าวถึงโซลูชันที่มีอยู่ เช่น เทคนิคการรักษาความเป็นส่วนตัว (เช่น Zero-Knowledge Proofs และการจัดเก็บแบบออฟไลน์) กลยุทธ์การปรับประสิทธิภาพของก๊าซและวิธีการตรวจสอบอย่างเป็นทางการเพื่อเพิ่มความน่าเชื่อถือของสัญญาอัจฉริยะ ทิศทางการวิจัยในอนาคตเน้นความจำเป็นในการปรับปรุงกลไกความปลอดภัย เพิ่มความสามารถในการปรับขนาดผ่านการแบ่งส่วนและโซลูชันเลเยอร์2 และการบูรณาการสัญญาอัจฉริยะ

กับเทคโนโลยีใหม่ ๆ เช่น ปัญญาประดิษฐ์ และทฤษฎีเกม

จากงานวิจัยของ Mitra (2022, pp. 1-39) นำเสนอกรอบการทำงานบนบล็อกเชนเพื่อการจัดการความยินยอมที่โปร่งใสและปลอดภัยโดยปฏิบัติตามกฎระเบียบความเป็นส่วนตัวของข้อมูลระดับโลก เช่น จีดีพีอาร์ โดยเน้นถึงความท้าทายของการรวบรวมข้อมูลผู้ใช้บนเว็บไซต์ แอปพลิเคชันบนมือถือ และอุปกรณ์อินเทอร์เน็ตทุกสรรพสิ่ง โดยเน้นถึงความจำเป็นของระบบการจัดการความยินยอมแบบเปิดและขยายได้ โพรโทคอลที่นำเสนอใช้ประโยชน์จากคุณสมบัติการกระจายศูนย์ ไม่เปลี่ยนรูป และโปร่งใสของบล็อกเชน เพื่อให้มั่นใจถึงการติดตามความยินยอมตลอดวงจรชีวิต ตั้งแต่การจับและแก้ไข ไปจนถึงการเพิกถอนและการทำลาย OConsent ใช้สัญญาอัจฉริยะ การพิสูจน์การเข้ารหัส การประทับเวลาที่เชื่อถือได้ และการระบุตัวตนเพื่อเพิ่มความเป็นส่วนตัวและการไม่ปฏิเสธ กรอบการทำงานนี้ออกแบบมาเพื่อสนับสนุนผู้มีส่วนได้ส่วนเสียต่าง ๆ รวมถึงเจ้าของข้อมูล ผู้ควบคุม และผู้ตรวจสอบ โดยจัดเตรียมเส้นทางการตรวจสอบที่ตรวจสอบได้และการบังคับใช้นโยบายความยินยอมโดยอัตโนมัติด้วยแนวทางแบบผสมผสานที่ผสานรวมไซดฺเชนท้องถิ่น (Local Sidechain) ที่ไม่ได้รับอนุญาตและบล็อกเชนระดับโลก เช่น บิตคอยน์และอีเธอเรียมสำหรับการพิมพ์ลายนิ้วมือของรัฐ OConsent มุ่งเน้นที่จะเพิ่มประสิทธิภาพความสามารถในการปรับขนาด ความปลอดภัย และการปฏิบัติตามกฎระเบียบ ในขณะที่ลดต้นทุนการดำเนินงาน

จากงานวิจัยของ Kakarlapudi and Mahmoud (2021, pp. 1-22) นำเสนอกรอบการทำงานที่ขับเคลื่อนด้วยบล็อกเชนที่มุ่งเป้าไปที่การรักษาความปลอดภัยของการจัดการข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในการใช้งาน เช่น การดูแลสุขภาพ การศึกษาเน้นย้ำถึงข้อกังวลเกี่ยวกับการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต และเน้นย้ำถึงความสำคัญของความโปร่งใสเพื่อเพิ่มความไว้วางใจของผู้ใช้ ระบบที่นำเสนอนี้ใช้ไฮเปอร์เลดเจอร์แฟบริค (Hyperledger Fabric) เพื่อบันทึกความยินยอมของผู้ใช้บนบล็อกเชน ในขณะเดียวกันก็จัดเก็บข้อมูลส่วนบุคคลอย่างปลอดภัยในฐานข้อมูลคลาวด์ส่วนตัวนอกเครือข่าย เพื่อให้มั่นว่าสอดคล้องกับจีดีพีอาร์ สถาปัตยกรรมช่วยให้องค์กรสามารถร้องขอการเข้าถึงข้อมูล ซึ่งผู้ใช้สามารถอนุมัติหรือเพิกถอนได้ เพื่อให้มั่นใจว่าสามารถตรวจสอบย้อนกลับและความรับผิดชอบได้อย่างสมบูรณ์ ระบบได้รับการประเมินโดยใช้ไฮเปอร์เลดเจอร์แคลิเปอร์ (Hyperledger Caliper) ซึ่งแสดงให้เห็นถึงความปลอดภัยและประสิทธิภาพที่ดีขึ้น ผลการวิจัยชี้ให้เห็นว่าบล็อกเชนสามารถทำหน้าที่เป็นรากฐานที่แข็งแกร่งสำหรับการจัดการข้อมูลที่รักษาความเป็นส่วนตัว โดยให้การควบคุมที่ดีขึ้นในการเข้าถึงข้อมูลและกระบวนการยินยอม

จากผลการศึกษาของ Alhajri, Rudolph, and Shahraki (2022) เสนอกรอบการทำงานที่มีการกระจายอำนาจ ปฏิบัติตามกฎหมาย และยึดมนุษย์เป็นศูนย์กลางสำหรับการจัดการความยินยอมของผู้ใช้เกี่ยวกับข้อมูลการออกกำลังกายโดยใช้เทคโนโลยีบล็อกเชน เมื่อพิจารณาถึงความเสี่ยงด้านความเป็นส่วนตัวที่เกี่ยวข้องกับอุปกรณ์ออกกำลังกายที่สวมใส่ได้ การศึกษานี้จึงจัดการกับความท้าทายที่เกี่ยวข้องกับความโปร่งใสของการยินยอม การควบคุมข้อมูล และการปฏิบัติตามกฎระเบียบ เช่น จีดีพีอาร์ ระบบที่นำเสนอใช้ประโยชน์จากสัญญาอัจฉริยะเพื่อทำให้การจัดการความยินยอมเป็นอัตโนมัติ ช่วยให้ผู้ใช้สามารถอนุญาต เพิกถอน และติดตามการเข้าถึงข้อมูลของตน ในขณะเดียวกันก็รับประกันความสามารถในการตรวจสอบและความปลอดภัย ด้วยการแยกการจัดการความยินยอมออกจากการจัดเก็บข้อมูล บล็อกเชนจะทำหน้าที่เป็นบัญชีแยกประเภทความยินยอมที่ไม่เปลี่ยนรูปแบบ โดยไม่ต้องจัดเก็บข้อมูลการออกกำลังกายส่วนบุคคลโดยตรง ซึ่งจะช่วยลดความเสี่ยงที่เกี่ยวข้องกับการเปลี่ยนแปลงไม่ได้ของบล็อกเชน การประเมินความปลอดภัยโดยใช้กรอบงาน SeMF แสดงให้เห็นว่าระบบรับประกันความถูกต้อง ความสมบูรณ์ และการไม่ปฏิเสธการทำธุรกรรมความยินยอม การศึกษาสรุปว่าเทคโนโลยีบล็อกเชนผ่านสัญญาอัจฉริยะและครือข่ายที่ได้รับอนุญาต ช่วยเพิ่มการควบคุมผู้ใช้ในการแบ่งปันข้อมูล ลดการพึ่งพาหน่วยงานจากส่วนกลาง และส่งเสริมความโปร่งใสและความไว้วางใจในการจัดการข้อมูลการออกกำลังกาย

จากงานวิจัยของ Rupasinghe, Burstein, and Rudolph (2019, pp. 1-9) นำเสนอกรอบการจัดการความยินยอมแบบกระจายอำนาจ โดยใช้ประโยชน์จากบล็อกเชนและสัญญาอัจฉริยะเพื่อปรับปรุงความเป็นส่วนตัวและความปลอดภัยในการแบ่งปันข้อมูลด้านการดูแลสุขภาพ การศึกษาเน้นย้ำถึงความท้าทายในการเข้าถึงข้อมูลทางคลินิกเนื่องจากความกังวลเรื่องความเป็นส่วนตัว และเสนอรูปแบบการยินยอมแบบไดนามิกที่ช่วยให้ผู้ป่วยสามารถจัดการ ปรับปรุง และเพิกถอนสิทธิ์ในการแบ่งปันข้อมูลได้แบบเรียลไทม์ สถาปัตยกรรมที่สร้างขึ้นบนบล็อกเชนแบบกลุ่มช่วยให้มั่นใจได้ถึงการปฏิบัติตามกฎระเบียบทางกฎหมาย เช่น จีดีพีอาร์ ขณะเดียวกันก็สนับสนุนการทำงานร่วมกันผ่านมาตรฐาน HL7 FHIR ประกอบด้วยเป้าหมายการออกแบบที่สำคัญ ได้แก่ ความปลอดภัยของข้อมูล ความเป็นส่วนตัว การควบคุมการเข้าถึง การตรวจสอบย้อนกลับ และการปฏิบัติตามกฎหมาย ด้วยการบูรณาการสัญญาอัจฉริยะสำหรับการตรวจสอบความยินยอมอัตโนมัติและเทคนิคการใช้การแฝงข้อมูลเพื่อการปกป้องความเป็นส่วนตัว โซลูชันที่นำเสนอจะปรับปรุงการเข้าถึงข้อมูลสำหรับการวิเคราะห์ทางคลินิก ในขณะเดียวกันก็รักษาการควบคุมผู้ป่วยและการรักษาความลับไว้

จากงานวิจัยของ Jaiman and Urovi (2020) นำเสนอกรอบการยินยอมแบบบล็อกเชน เพื่อปรับปรุงการแบ่งปันข้อมูลที่ปลอดภัยและมีความรับผิดชอบ โดยเฉพาะนด้านการดูแลสุขภาพ การศึกษานี้เน้นย้ำถึงความท้าทายในการได้รับและจัดการความยินยอมส่วนบุคคล ในขณะเดียวกันก็รับประกันการปฏิบัติตามกฎระเบียบ เช่น จีดีพีอาร์ แบบจำลองที่นำเสนอใช้ประโยชน์จากสัญญาอัจฉริยะบนบล็อกเชนอีเธอเรียม เพื่อนำเสนอและบังคับใช้ความยินยอมของผู้ใช้เกี่ยวกับข้อมูลสุขภาพแบบไดนามิก ช่วยให้ผู้ร้องขอข้อมูลสามารถค้นหา ร้องขอ และเข้าถึงข้อมูล ในขณะเดียวกันก็รับประกันความสามารถในการตรวจสอบและความปลอดภัย กรอบงานนี้รวม Data Use Ontology (DUO) เพื่อสร้างแบบจำลองการตั้งค่าความยินยอมส่วนบุคคล และ Automatable Discovery and Access Matrix (ADA-M) เพื่อสร้างมาตรฐานการสืบค้นคำขอข้อมูล ด้วยการรักษาบันทึกธุรกรรมการแบ่งปันข้อมูลที่ไม่เปลี่ยนแปลง ระบบจะให้ความโปร่งใส ความรับผิดชอบ และการควบคุมการเข้าถึงอย่างละเอียด ในขณะที่ยังคงรักษาความเป็นส่วนตัวของข้อมูล การประเมินเชิงทดลองแสดงให้เห็นถึงประสิทธิภาพและความสามารถในการปรับตัวของแบบจำลองในสถานการณ์การแบ่งปันข้อมูลในโลกแห่งความเป็นจริง โดยเน้นถึงศักยภาพในการปรับปรุงการกำกับดูแลข้อมูลที่เน้นผู้ใช้เป็นศูนย์กลางในแพลตฟอร์มแบบกระจายอำนาจ

จากงานวิจัยของ Vargas (2019, pp. 165-170) เสนอแบบจำลองที่ใช้บล็อกเชนสำหรับการจัดการความยินยอมข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป การศึกษาเน้นย้ำถึงความท้าทายที่บริษัทต่าง ๆ เผชิญในการปฏิบัติตามกฎระเบียบ ในขณะเดียวกันก็รักษาความปลอดภัยของข้อมูล ความโปร่งใส และระบบอัตโนมัติ แบบจำลองที่นำเสนอซึ่งใช้งานโดยใช้ไฮเปอร์เลดเจอร์แฟบริค ช่วยให้เจ้าของข้อมูลยืนการควบคุมข้อมูลส่วนบุตตลของตนโดยการติดตามและจัดการความยินยอมของพวกเขา ขณะเดียวกันก็อนุญาตให้ผู้ควบคุมข้อมูลและผู้ประมวลผลสามารถรับรองการปฏิบัติตามข้อกำหนดผ่านบันทึกที่ไม่เปลี่ยนรูปแบบและตรวจสอบได้ กรอบการทำงานนี้อำนวยความสะดวกในการแก้ไขคำยินยอมแบบเรียลไทม์ รองรับการตรวจสอบเงื่อนไขความยินยอมโดยอัตโนมัติ และเพิ่มความรับผิดชอบ นอกจากนี้ แบบจำลองดังกล่าวยังเสนอระบบการสร้างรายได้จากข้อมูลที่ยุติธรรมยิ่งขึ้น ซึ่งช่วยให้ผู้ใช้สามารถแบ่งปันรายได้จากการให้ข้อมูลของพวกเขา การวิจัยเน้นย้ำถึงประโยชน์ของบล็อกเชนในการจัดการความยินยอม แต่ยังระบุถึงความท้าทายที่เกี่ยวข้องกับการรวมระบบเข้ากับโครงสร้างพื้นฐานที่มีอยู่และรับประกันการนำไปใช้อย่างกว้างขวางในอุตสาหกรรมต่าง ๆ

จากงานวิจัยของ Kakarlapudi and Mahmoud (2021) ได้ทำการวิเคราะห์บทบาทของเทคโนโลยีบล็อกเชนในการจัดการข้อมูลความยินยอมและความเป็นส่วนตัวอย่างเป็นระบบในภาคส่วนต่าง ๆ รวมถึงการดูแลสุขภาพ อินเทอร์เน็ตทุกสรรพสิ่ง การจัดการข้อมูลประจำตัว และการจัดเก็บข้อมูล การตรวจสอบนี้อิงตามหลักเกณฑ์ของ PRISMA โดยสำรวจคุณลักษณะเฉพาะของบล็อกเชน เช่น ความไม่เปลี่ยนแปลงและการกระจายอำนาจ โดยเน้นถึงศักยภาพในการยกระดับความปลอดภัย ความโปร่งใส และการควบคุมข้อมูลส่วนบุคคลของผู้ใช้ การศึกษาระบุความท้าทายในระบบการจัดการความยินยอมแบบดั้งเดิม รวมถึงการกระจายตัวของข้อมูล การขาดความโปร่งใส และการปฏิบัติตามกฎระเบียบ และประเมินว่าบล็อกเชนสามารถแก้ไขปัญหาเหล่านี้ได้อย่างไรผ่านการจัดเก็บข้อมูลที่ปลอดภัย การควบคุมการเข้าถึงที่โปร่งใส และการติดตามความยินยอมอัตโนมัติโดยใช้สัญญาอัจฉริยะ นอกจากนี้ งานวิจัยนี้ยังกล่าวถึงข้อจำกัดต่าง ๆ เช่น ความสามารถในการทำงานร่วมกัน และ สิทธิที่จะถูกลืมของจีดีพีอาร์ โดยเน้นย้ำถึงความจำเป็นในการวิจัยเพิ่มเติมเพื่อปรับปรุงกรอบการจัดการความยินยอมบนบล็อกเชน

การเน้นย้ำถึงความสำคัญอย่างยิ่งยวดในการปรับการใช้สัญญาอัจฉริยะให้สอดคล้องกับกฎหมายคุ้มครองข้อมูล โดยเฉพาะอย่างยิ่งในบริบทของบุคคลที่ใช้สิทธิ์ในข้อมูลส่วนบุคคลของตน สิ่งนี้จะเกี่ยวข้องโดยเฉพาะอย่างยิ่งเมื่อใช้ประโยชน์จากเทคโนโลยีขั้นสูง เช่น สัญญาอัจฉริยะบนบล็อกเชน ซึ่งได้รับการออกแบบมาเพื่อทำให้ขั้นตอนการปกป้องข้อมูลเป็นแบบอัตโนมัติและแข็ง แกร่งขึ้น ความเสถียรและความน่าเชื่อถือของสัญญาอัจฉริยะ โดยเฉพาะอย่างยิ่งในบริบทของบล็อกเชนสามารถก่อให้เกิดความท้าทายเมื่อบุคคลพยายามใช้สิทธิ์ของตนในการลบหรือแก้ไขข้อมูลส่วนบุคคล การสร้างสมดุลระหว่างข้อดีของเทคโนโลยีบล็อกเชนกับความจำเป็นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูล จำเป็นต้องพิจารณาอย่างรอบคอบและอาจเป็นโซลูชันที่เป็นนวัตกรรมเพื่อจัดการกับความท้าทายระหว่างความไม่เปลี่ยนแปลงของบล็อกเชนกับการใช้สิทธิ์ของเจ้าของข้อมูลบางอย่าง (Voss, 2021)

เมื่อได้ทำการเปรียบเทียบข้อบังคับใช้ระหว่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พีดีพีเอ) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ปี 2016 (จีดีพีอาร์) พบว่ามีความแตกต่างที่สำคัญบางประการ กล่าวคือ พีดีพีเอไม่มีผลบังคับใช้กับหน่วยงานของรัฐบางแห่ง และคำจำกัดความของ “ข้อมูลส่วนบุคคล” ในจีดีพีอาร์จะมีความละเอียดและครอบคลุมมากกว่าในพีดีพีเอ ซึ่งในจีดีพีอาร์จะรวมถึงเลขที่อยู่ไอพี (IP Address) และตัวระบุคุกกี้ด้วย ในขณะที่ในพีดีพีเอไม่ได้กล่าวถึงสิ่งเหล่านี้ นอกจากนี้แม้ว่าพีดีพีเอจะระบุว่าเจ้าของข้อมูลมีสิทธิ์ในการปกปิดข้อมูล

ส่วนตัวของตนได้ ซึ่งมีความแตกต่างจากจีดีพีอาร์แต่พีดีพีเอก็ไม่ได้กำหนดข้อมูลนิรนามหรือข้อมูลแฝง (OneTrust DataGuidance, Blumenthal Richter & Sumet, 2020, p. 5)

จากบทความของ Shah, Forester, Berberich, & Raspe (2019) ได้สำรวจความท้าทายและความตึงเครียดด้านกฎระเบียบระหว่างเทคโนโลยีบล็อกเชนและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (จีดีพีอาร์) และพระราชบัญญัติความเป็นส่วนตัวของผู้บริโภคแห่งแคลิฟอร์เนีย (ซีซีพีเอ) โดยเน้นย้ำคุณลักษณะพื้นฐานของบล็อกเชน เช่น การกระจายอำนาจ ความไม่เปลี่ยนรูปและความโปร่งใส ซึ่งขัดแย้งกับหลักการปกป้องข้อมูลแบบดั้งเดิม รวมถึงสิทธิที่จะถูกลืม การลดขนาดข้อมูล และความรับผิดชอบแบบรวมศูนย์ ข้อกังวลทางกฎหมายที่สำคัญ ได้แก่ การระบุตัวตนของผู้ควบคุมและผู้ประมวลผลข้อมูล ข้อจำกัดในการถ่ายโอนข้อมูลข้ามพรมแดน และความท้าทายในการใช้สิทธิ์ความเป็นส่วนตัวกับบันทึกบล็อกเชนที่ไม่เปลี่ยนรูป การศึกษากล่าวถึงกลยุทธ์การลดผลกระทบที่อาจเกิดขึ้นรวมถึงการจัดเก็บข้อมูลนอกเครือข่าย การใช้การแฝงข้อมูล บล็อกเชนที่ได้รับอนุญาต และเทคนิคการเข้ารหัสทางเลือก เช่น การเข้ารหัสแบบเพิกถอนได้ และการพิสูจน์ความรู้เป็นศูนย์ ผู้เขียนสรุปว่าในขณะที่บล็อกเชนก่อให้เกิดความท้าทายในการปฏิบัติตามกฎระเบียบที่สำคัญ การออกแบบระบบอย่างระมัดระวังและการปรับเปลี่ยนตามกฎระเบียบสามารถเปิดใช้งานการดำเนินการรักษาความเป็นส่วนตัวที่สอดคล้องกับกรอบกฎหมายที่มีอยู่

ในงานวิจัยของ Sardá, Natale, Sotirakopoulos, and Monaghan (2019, pp. 557–564) ได้สำรวจแนวคิดที่กำลังพัฒนาของการไม่เปิดเผยตัวตนบนอินเทอร์เน็ต โดยเน้นที่มิติทางเทคนิคและทางสังคม การศึกษานี้ตรวจสอบว่าการไม่เปิดเผยตัวตนได้เปลี่ยนแปลงไปอย่างไรเมื่อเวลาผ่านไปจากอินเทอร์เน็ตในยุคแรก ๆ ในอุดมคติของการสำรวจข้อมูลประจำตัวด้วยข้อมูลแฝง ไปสู่พื้นที่ที่มีการโต้แย้ง ซึ่งเป็นทั้งเครื่องมือในการปกป้องความเป็นส่วนตัวและความท้าทายในการบังคับใช้ความปลอดภัย งานวิจัยนี้กล่าวถึงเทคโนโลยีที่ไม่เปิดเผยตัวตนต่าง ๆ เช่น VPN, Proxies, Tor และการเข้ารหัส ในขณะเดียวกันก็รับทราบถึงคุณลักษณะของการใช้งานแบบคู่ ซึ่งทำให้เกิดการเคลื่อนไหวทางการเมืองและเสรีภาพในการแสดงออก แต่ยังอำนวยความสะดวกให้กับอาชญกรรมในโลกไซเบอร์และกิจกรรมที่ผิดกฎหมายอีกด้วย ผู้เขียนยืนยันว่าการไม่เปิดเผยตัวตนทางออนไลน์ไม่ควรถูกมองว่าเป็นเงื่อนไขที่แน่นอน แต่เป็นสภาวะที่ลื่นไหลและอยู่ในช่วงเปลี่ยนผ่าน ซึ่งถูกกำหนดโดยปฏิสัมพันธ์ทางสังคม ความก้าวหน้าทางเทคโนโลยี และกรอบนโยบาย รายงานสรุปว่าจำเป็นต้องมีแนวทางที่สมดุลเพื่อจัดการกับทั้งประโยชน์และความเสี่ยงที่เกี่ยวข้องกับการไม่เปิดเผยตัวตนทางออนไลน์ โดยบูรณาการมุมมองด้านเทคนิค กฎหมาย และจริยธรรม

จากรายงานทางเว็บไซต์ของสำนักงานสืบสวนกลางแห่งสหรัฐอเมริกา (Federal Bureau of Investigations, 2015) ได้เปิดเผยให้เห็นการยึดบิทคอยน์มูลค่า 28 ล้านดอลลาร์เพิ่มเติมจากเจ้าของเว็บไซต์ Silk Road โดยมีความเกี่ยวข้องเฉพาะกับการขายเครื่องมือลบข้อมูลระบุตัวตนบนแพลตฟอร์ม Silk Road รายงานดังกล่าวเน้นย้ำถึงสถานการณ์ที่เกี่ยวข้องกับการดำเนินคดีทางกฎหมายกับผู้ให้บริการ Silk Road และการยึดบิทคอยน์จำนวนมาก นอกจากนี้ ความเชื่อมโยงกับการขายเครื่องมือลบข้อมูลระบุตัวตนยิ่งตอกย้ำถึงความสัมพันธ์ที่ซับซ้อนระหว่างเทคโนโลยี กิจกรรมทางอาญา และความพยายามในการบังคับใช้กฎหมายของตลาดผิดกฎหมายออนไลน์ (เว็บตลาดมืด) กรณีของ Silk Road ยังสะท้อนให้เห็นถึงความท้าทายของหน่วยงานบังคับใช้กฎหมายในการต่อสู้กับตลาดผิดกฎหมายที่ใช้เทคโนโลยีบล็อกเชนและคริปโทเคอร์เรนซีเพื่อปกปิดธุรกรรมและลดความเสี่ยงในการถูกตรวจสอบ แม้ว่าการดำเนินคดีจะส่งผลให้เจ้าหน้าที่สามารถยึดบิตคอยน์และระงับแพลตฟอร์มดังกล่าวได้ แต่เหตุการณ์นี้ยังเป็นตัวอย่างสำคัญของการเปลี่ยนแปลงในรูปแบบอาชญกรรมทางไซเบอร์ ซึ่งอาศัยเทคโนโลยีชั้นสูงเพื่อสร้างความท้าทายต่อการบังคับใช้กฎหมายในยุคดิจิทัล

ในงานวิจัยของ Diaz, Seys, Classens, and Praneel (2002, pp. 54–68) แนะนำแบบจำลองข้อมูลและทฤษฎีสำหรับการวัดปริมาณระดับของการไม่เปิดเผยตัวคนที่ได้รับจากระบบการสื่อสารที่ไม่เปิดเผยตัวตน แบบจำลองนี้อิงตามเอนโทรปีของ Shannon และประเมินการกระจายความน่าจะเป็นที่ผู้โจมตีกำหนดให้กับผู้ใช้ที่แตกต่างกันในฐานะผู้สร้างข้อความที่เป็นไปได้ ได้รับการออกแบบมาเพื่อประเมินว่าผู้โจมตีสามารถอนุมานข้อมูลได้มากเพียงใด ทำให้สามารถเปรียบเทียบระบบไม่เปิดเผยตัวตนที่แตกต่างกันภายใต้สถานการณ์การโจมตีต่าง ๆ การศึกษานี้ใช้แบบจำลองกับเทคนิคการรักษานิรนามที่มีอยู่ เช่น Crowds และ Onion Routing ซึ่งแสดงให้เห็นถึงประสิทธิภาพในการประเมินและปรับปรุงกลไกความเป็นส่วนตัว ผู้เขียนเน้นย้ำว่าการไม่เปิดเผยตัวตนไม่ใช่ทรัพย์สินที่แท้จริง แต่เป็นระดับที่สามารถวัดได้ซึ่งได้รับอิทธิพลจากโครงสร้างระบบและความสามารถของผู้โจมตี บทความสรุปว่า แนวทางนี้เป็นตัวชี้วัดที่มีคุณค่าสำหรับการวิเคราะห์และปรับปรุงระบบการไม่เปิดเผยตัวคนในการใช้งานจริง

จากรายงานอาชญกรรมทางไซเบอร์อย่างเป็นทางการประจำปี 2022 ของ Morgan (2023) ได้เน้นย้ำถึงการเพิ่มขึ้นอย่างรวดเร็วของอาชญกรรมทางไซเบอร์ทั่วโลก โดยคาดการณ์ว่าค่าใช้จ่ายต่อปีจะสูงถึง 10.5 ล้านล้านดอลลาร์ภายในปี 2025 ทำให้กลายเป็นประเทศที่มีขนาดเศรษฐกิจใหญ่เป็นอันดับสามรองจากสหรัฐอเมริกาและจีน รายงานสรุปภัยคุกคามที่สำคัญ รวมถึงแรนซัมแวร์ อาชญากรรมเข้ารหัสลับ และการละเมิดข้อมูล โดยแรนซัมแวร์เพียงอย่างเดียวคาดว่าจะ

สร้างความเสียหายมูลค่า 265 พันล้านดอลลาร์ต่อไปภายในปี 2031 อาชญากรรมเงินดิจิทัล โดยเฉพาะอย่างยิ่งในด้านการเงินแบบกระจายอำนาจ (DeFi) คาดว่าจะมีมูลค่าถึง 3 หมื่นล้านดอลลาร์ต่อปีภายในปี 2025 ซึ่งได้แรงหนุนจากจู่โจมการแลกเปลี่ยนและแผนการฉ้อโกง รายงานเน้นย้ำถึงพื้นที่ของการโจมตีทางไซเบอร์ที่เพิ่มมากขึ้น โดยคาดว่าจะมีผู้คนมากกว่า 7.5 พันล้านคนออนไลน์ภายในปี 2030 และเพิ่มช่องโหว่ในอุตสาหกรรมต่าง ๆ โดยเฉพาะด้านการดูแลสุขภาพ สาธารณูปโภค และบริการทางการเงิน นอกจากนี้ยังเน้นย้ำถึงช่องว่างด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีตำแหน่งงานที่ไม่สำเร็จหลายล้านตำแหน่งทั่วโลก รายงานดังกล่าวเน้นย้ำถึงความจำเป็นเร่งด่วนสำหรับธุรกิจต่าง ๆ ในการลงทุนในความปลอดภัยทางไซเบอร์ ใช้มาตรการรักษาความปลอดภัยตามความเสี่ยง และใช้โซลูชันการตรวจจับและตอบสนองที่มีการจัดการ (MDR) เพื่อบรรเทาภัยคุกคามและเพิ่มความยืดหยุ่นทางไซเบอร์

ในงานวิจัยของ Sweeney (2002, pp. 557-570) เน้นย้ำถึงความเสี่ยงด้านความเป็นส่วนตัวที่สำคัญเกี่ยวข้องกับการโจมตีด้วยการระบุตัวตนอีกครั้ง โดยเผยให้เห็นว่าบันทึกส่วนบุคคลสามารถระบุตัวตนได้อีกครั้งโดยใช้คุณลักษณะเฉพาะเพียงสามประการเท่านั้น ได้แก่ วันเกิด เพศ และรหัสไปรษณีย์ ซึ่งเพียงพอที่จะระบุตัวตนของบุคคลได้มากกว่า 87% ของประชากรสหรัฐฯ เมื่อใช้ข้อมูลสาธารณะหรือข้อมูลที่ได้รับความช่วยเหลือจากแหล่งข้อมูลภายนอก เพื่อแก้ไขปัญหาดังกล่าว ผู้เขียนได้เสนอแนวคิดที่เรียกว่า “ซ่อนตัวอยู่ในคลาวด์ (Hiding in the Crowd)” ซึ่งเป็นหลักการพื้นฐานของ k-Anonymity ที่ช่วยให้ข้อมูลส่วนบุคคลสามารถเปิดเผยได้โดยไม่ระบุตัวตนที่แท้จริงของบุคคลที่เกี่ยวข้อง โดยแนวทางนี้อาศัยการทำตัวระบุเสมือนให้มีลักษณะทั่วไปทั้งหมด หรือการรวมกลุ่มข้อมูลเพื่อให้มีบุคคลอย่างน้อย k คนที่มีลักษณะเหมือนกันในชุดข้อมูลเดียวกัน สิ่งนี้ช่วยลดความสามารถของผู้ไม่ประสงค์ดีในการเชื่อมโยงข้อมูลและระบุตัวตนที่แท้จริงของบุคคล

จากบทความของ Riotta (2023) การศึกษาใหม่จากมหาวิทยาลัยเพนซิลวาเนียเผยให้เห็นข้อมูลว่าข้อมูลของสำนักงานสำรวจสำมะโนประชากรของสหรัฐอเมริกามีความอ่อนไหวต่อ “การโจมตีที่สร้างใหม่” ซึ่งอาชญากรไซเบอร์สามารถย้อนกลับข้อมูลทางสถิติทางวิศวกรรมเพื่อเปิดเผยข้อมูลส่วนบุคคลของผู้ตอบแบบสอบถามแต่ละราย นักวิจัยแสดงให้เห็นว่าการโจมตีเหล่านี้โดยใช้อัลกอริทึมการเรียนรู้ของเครื่องสามารถดำเนินการได้โดยใช้คอมพิวเตอร์พกกาเชิงพาณิชย์ ทำให้เกิดความกังวลเกี่ยวกับการขโมยข้อมูลส่วนตัวและการเลือกปฏิบัติ ในขณะที่เทคโนโลยีเพิ่มความเป็นส่วนตัว เช่น Differential Privacy ได้รับการแนะนำ ซึ่งใช้ครั้งแรกในการสำรวจสำมะโนประชากรปี 2020 การศึกษาเน้นย้ำถึงความท้าทายอย่างต่อเนื่องในการสร้างสมดุลระหว่างความแม่นยำ

ของข้อมูลกับความเป็นสวนตัว นอกจากนี้ การตรวจสอบของรัฐบาลยังพบช่องโหว่ในการป้องกันความปลอดภัยทางไซเบอร์ของสำนัก โดยเน้นย้ำถึงความจำเป็นในการใช้มาตรการป้องกันที่แข็งแกร่งยิ่งขึ้น

ในงานวิจัยของ Dwork, Smith, Steinke, and Ullman (2017, pp. 61–84) ได้สำรวจการโจมดีความเป็นส่วนตัวต่าง ๆ ที่กระทบต่อข้อมูลที่ละเอียดอ่อน แม้ว่าสถิติโดยรวมจะถูกเปิดเผยต่อสาธารณะก็ตาม โดยแบ่งประเภทการโจมตีเหล่านี้ออกเป็นการระบุตัวตนใหม่ การสร้างใหม่ และการติดตามการโจมดี การโจมตีแบบสร้างใหม่ใช้สถิติสาธารณะเพื่ออนุมานคุณลักษณะที่ละเอียดอ่อนของบุคคลเกือบทั้งหมดในชุดข้อมูล ในขณะที่การติดตามการโจมดีจะกำหนดว่าข้อมูลของบุคคลใดรวมอยู่ในชุดข้อมูลหรือไม่ การศึกษายังกล่าวถึงความเป็นส่วนตัวที่แตกต่างกัน ซึ่งเป็นวิธีการพิสูจน์ได้ในการป้องกันการโจมดีดังกล่าวโดยการเพิ่มสัญญารบกวนที่ควบคุมได้ให้กับการเปิดเผยข้อมูล ผู้เขียนเน้นย้ำว่าเทคนิคความเป็นส่วนตัวแบบดั้งเดิม เช่น การทำให้ข้อมูลเป็นนิรนามและการรวมกลุ่ม นั้นไม่เพียงพอต่อการโจมดีทางคอมพิวเตอร์สมัยใหม่ โดยเน้นย้ำถึงความจำเป็นของวิธีการรักษาความเป็นส่วนตัวที่เข้มงวด

ในงานวิจัยของ Narayanan, and Shmatikov (2008, pp. 111–125) ผู้เขียนได้มีการแนะนำวิธีการในการไม่ระบุตัวตน ซึ่งการไม่ระบุตัวตนเป็นกระบวนการสำคัญที่ใช้เพื่อปกป้องข้อมูลที่ละเอียดอ่อนโดยการลบหรือแก้ไของค์ประกอบที่สามารถระบุตัวตนได้ และผู้เขียนยังได้แสดงกระบวนการสำหรับการระบุข้อมูลที่ไม่ระบุตัวตนอีกครั้ง แม้ว่าหลังจากลบบันทึกที่สามารถระบุตัวตนโดยตรงทั้งหมดแล้วก็ตาม วิธีการลบการระบุตัวตนที่นำเสนอนั้นจะเกี่ยวข้องกับเทคนิคหรือกลไกที่มุ่งเน้นปกปิดหรือเปลี่ยนแปลงตัวระบุส่วนบุคคลในชุดข้อมูล โดยมีจุดประสงค์เพื่อปกป้องความเป็นส่วนตัวของบุคคล การสาธิตการระบุตัวตนข้อมูลที่ไม่เปิดเผยตัวตนอีกครั้งถือเป็นลักษณะเด่นของการศึกษานี้ การระบุตัวตนซ้ำหมายถึงกระบวนการจับคู่ข้อมูลที่ไม่ระบุตัวตนหรือข้อมูลนิรนามกลับไปยังบุคคลดั้งเดิม

ในงานวิจัยของ Hamidovic, Kabil, and Edina (2019, pp. 219–230) เป็นงานวิจัยที่แนะนำและอภิปรายเกี่ยวกับการใช้การแฝงข้อมูลทั่วไปและขั้นตอนการปกปิดข้อมูล ขั้นตอนเหล่านี้ได้รับการยอมรับว่าเป็นมาตรการป้องกันที่มีประสิทธิภาพสูงภายใต้จีดีพีอาร์ ซึ่งเป็นกฎหมายที่ครอบคลุมซึ่งควบคุมความเป็นส่วนตัวและความปลอดภัยของข้อมูล จุดสนใจหลักของการวิจัยที่นำเสนอคือ การประยุกต์ใช้เทคนิคการแฝงข้อมูลและการปกปิดข้อมูลเหล่านี้ในทางปฏิบัติ เพื่อให้

มั่นใจในความปลอดภัยและความเป็นส่วนตัวของข้อมูลที่เกี่ยวข้องกับสุขภาพของผู้ป่วย การเน้นย้ำถึงความสำคัญอย่างมากในการปกป้องข้อมูลการรักษาพยาบาลที่ละเอียดอ่อน โดยทั่วไปข้อมูลสุขภาพของผู้ป่วยจะประกอบด้วย รายละเอียดการวินิจฉัยทางการแพทย์ แผนการรักษา และตัวระบุส่วนบุคคล ซึ่งหากได้รับการจัดการอย่างไม่เหมาะสม อาจนำไปสู่การละเมิดความเป็นส่วนตัวและอาจเป็นอันตรายต่อบุคคลได้อย่างมีนัยสำคัญ ผู้เขียนเจาะลึกถึงวิธีการใช้การแฝงข้อมูลและการปกปิดข้อมูลอย่างมีประสิทธิภาพในบริบทด้านการดูแลสุขภาพ สิ่งนี้เกี่ยวข้องกับวิธีการแทนที่หรือปกปิดข้อมูลที่สามารถระบุตัวบุคคลได้ด้วยการแฝงข้อมูลหรือการแก้ไขข้อมูลในลักษณะที่คงไว้ซึ่งประโยชน์ใช้สอยสำหรับการวิจัยและการวิเคราะห์ ในขณะเดียวกันก็ลดความเสี่ยงในการระบุตัวตนซ้ำอีกครั้ง

เอกสารฉบับนี้มุ่งเน้นไปที่ผู้ควบคุมข้อมูลที่รับผิดชอบในการจัดการและประมวลผลข้อมูลส่วนบุคคลในบริบทองค์กรต่าง ๆ เป็นหลัก จุดสนใจหลักคือการให้คำแนะนำและข้อมูลเชิงลึกแก่ผู้ควบคุมข้อมูลที่สนใจใช้เทคนิคแฮชเพื่อใช้เป็นการแฝงข้อมูลส่วนบุคคลในระหว่างกิจกรรมการประมวลผลข้อมูล ผู้เขียนได้มีคำเตือนที่สำคัญเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นจากการระบุตัวตนซ้ำอีกครั้ง ซึ่งเป็นข้อกังวลที่สำคัญในด้านความเป็นส่วนตัวของข้อมูล การระบุตัวตนซ้ำอีกครั้งหมายถึงความเป็นไปได้ที่ผู้กระทำความผิดหรือฝ่ายตรงข้ามจะทำวิศวกรรมย้อนกลับข้อมูลที่ใช้การแฝงข้อมูลเพื่อเปิดเผยข้อมูลส่วนบุคคลดั้งเดิม ความพยายามในการระบุตัวตนซ้ำอีกครั้งดังกล่าวอาจนำไปสู่การละเมิดความเป็นส่วนตัวและบ่อนทำลายวัตถุประสงค์ของการใช้การแฝงข้อมูล (European Data Protection Supervisor, 2019)

จากการศึกษาของ Slijepcevic et al. (2021, pp. 1–19) อ้างถึงการตรวจสอบผลกระทบของกระบวนการ k-Anonymity ที่มีต่อคุณภาพของข้อมูลโดยเฉพาะอย่างยิ่งในแง่ของการสูญเสียข้อมูล โดยใช้แบบจำลองการจำแนกประเภทเพื่อประเมินผลกระทบของ k-Anonymity การค้นพบของพวกเขาพบว่าประสิทธิภาพของแบบจำลองการจำแนกประเภททั่วไปจะลดลงเมื่อใช้ข้อมูลที่ประมวลผลผ่านกระบวนการ k-Anonymity ประสิทธิภาพที่ลดลงนี้มีสาเหตุมาจากการสูญเสียความจำเพาะและรายละเอียดของข้อมูล ซึ่งเป็นผลมาจากกระบวนการปกปิดข้อมูล เมื่อข้อมูลกลายเป็นนิรนามมากขึ้น (ด้วยค่า 'K' ที่สูงกว่า) ข้อมูลจะสูญเสียคุณลักษณะเฉพาะที่ช่วยให้แบบจำลองการจำแนกประเภทสามารถคาดการณ์หรือจำแนกประเภทได้อย่างแม่นยำ

2.7.3 ตารางสรุปช่องว่างของการวิจัย

ตารางที่ 2.7 สรุปช่องว่างของการวิจัย

	Blockchain	Smart Contract	Consent Management	Anonymity	Pseudonymity	Data Privacy	Data Protection	GDPR	PDPA
Suripeddi and Purandare (2021)	✓					✓	✓	✓	
Mohanta et al. (2019)	✓	✓		✓		✓	✓	✓	
Melin (2019)	✓			✓		✓	✓	✓	
Zhang et al. (2020)	✓			✓	✓	✓			
Zou et al. (2021)	✓	✓				✓			
Zyskind et al. (2015)	✓			✓	✓	✓			
Sirur et al. (2019)	✓					✓	✓	✓	
Mumu et al. (2021)	✓					✓	✓	✓	
Kondava and Erbguth (2020)	✓					✓	✓	✓	
Hristov and Dimitrov (2018)	✓					✓	✓	✓	
Bernabe et al. (2019)	✓			✓		✓	✓	✓	
Bonneau et al. (2015)	✓			✓		✓			

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.7 สรุปช่องว่างของการวิจัย (ต่อ)

	Blockchain	**Smart Contract**	**Consent Management**	**Anonymity**	**Pseudonymity**	**Data Privacy**	**Data Protection**	**GDPR**	**PDPA**
Hewa et al. (2021)	✓	✓							
Mitra (2021)	✓		Trusted Timestamp proof	IDs or Zero Knowledge Proof		✓		✓	
Kakarlapudi (2021)	✓	- Smart contract - Chaincode	- Ethereum - Hyperledger-based - Cloud-based			✓	✓	✓	
Alhajri et al. (2022)	✓	✓	SeMF			✓		✓	
Rupasinghe et al. (2019)	✓	✓	Dynamic Consent			✓	✓	✓	
Jaiman and Urovi (2020)	✓	✓	Dynamic Consent			✓		✓	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.7 สรุปช่องว่างของการวิจัย (ต่อ)

	Blockchain	**Smart Contract**	**Consent Management**	**Anonymity**	**Pseudonymity**	**Data Privacy**	**Data Protection**	**GDPR**	**PDPA**
Vargas (2019).	✓	✓	Hyperledger Fabric			✓		✓	
Kakarlapudi and Mahmoud (2019)	✓	✓	✓			✓		✓	
Henriksen-Bulmer and Jeary (2016)				✓		✓	✓		
OneTrust DataGuidance et al. (2020)				✓	✓	✓	✓	✓	✓
Voss (2021)	✓	✓					✓	✓	
Shah et al. (2019)	✓					✓		✓	
Sardá et al. (2019)				✓		✓			
Federal Bureau of Investigations (2015)	✓			✓		✓		✓	
Diaz et al. (2002)				✓			✓		
Morgan (2023)						✓	✓		
Sweeney (2002)				✓		✓			

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.7 สรุปช่องว่างของการวิจัย (ต่อ)

	Blockchain	**Smart Contract**	**Consent Management**	**Anonymity**	**Pseudonymity**	**Data Privacy**	**Data Protection**	**GDPR**	**PDPA**
Riotta (2023)				✓		✓		✓	
Dwork et al. (2017)				✓		✓			
Narayanan, and Shmatikov (2008)				✓		✓			
Hamidovic et al. (2019)				✓	✓	✓	✓	✓	
European Data Protection Supervisor (2019)	✓				✓	✓	✓	✓	
Slijepcevic et al. (2021)				✓					
งานวิจัยฉบับนี้	✓	✓	✓	✓	✓	✓	✓	✓	✓

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 3

ระเบียบวิธีการวิจัย

งานวิจัยเรื่อง “ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล” ใช้การวิจัยเชิงปริมาณ (Quantitative Research) ด้วยการทดลองจริง (True Experiment) เป็นการวิจัยที่มีการเก็บข้อมูลและมีวิเคราะห์ข้อมูลโดยใช้การวิเคราะห์เชิงเปรียบเทียบ (Comparative Analysis) ผู้วิจัยเห็นว่าการออกแบบวิจัยเชิงปริมาณประเภทนี้สอดคล้องกับหัวข้อที่ทำการศึกษา โดยเริ่มจากการค้นคว้าเอกสาร การทบทวนวรรณกรรมต่าง ๆ ที่เกี่ยวข้องนำไปสรุปเพื่อสร้างกรอบแนวคิดการวิจัย

3.1 ขั้นตอนการวิจัย

ผู้วิจัยได้มีวิธีการดำเนินการวิจัยดังรูปที่ 3.1 และมีขั้นตอนการดำเนินการวิจัย ดังนี้

3.1.1 ขั้นตอนที่ 1: เตรียมการวิจัย

ผู้วิจัยได้พิจารณาเลือกและกำหนดปัญหาที่จะทำวิจัย ศึกษาค้นคว้าจากทฤษฎี แนวคิด บทความ และงานวิจัยที่เกี่ยวกับเทคโนโลยีบล็อกเชนและการคุ้มครองข้อมูลส่วนบุคคล โดยศึกษาในประเด็นและแง่มุมต่าง ๆ เพื่อเก็บข้อมูล ที่มาและความสำคัญ ปัจจัยที่สำคัญที่มีความเกี่ยวข้อง รวมไปถึงปัญหาที่เกิดขึ้น เพื่อให้ทราบถึงช่องว่างในการวิจัย และประเด็นในการศึกษาวิจัยที่จะก่อ ให้เกิดประโยชน์ในภายภาคหน้า ทำให้เป็นที่มาและการเลือกหัวเรื่องและการตั้งชื่อเรื่องที่มีความสนใจศึกษา

3.1.2 ขั้นตอนที่ 2: การออกแบบวิจัย

ผู้วิจัยนำทฤษฎีที่เกี่ยวข้องกับเทคโนโลยีบล็อกเชนและการคุ้มครองข้อมูลส่วนบุคคล ที่ได้จากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง นำมากำหนดรูปแบบหรือแนวทางการวิจัยให้เหมาะสมกับปัญหาที่จะศึกษา เพื่อกำหนดกรอบแนวคิดการวิจัยหรือแบบจำลองของเรื่อง

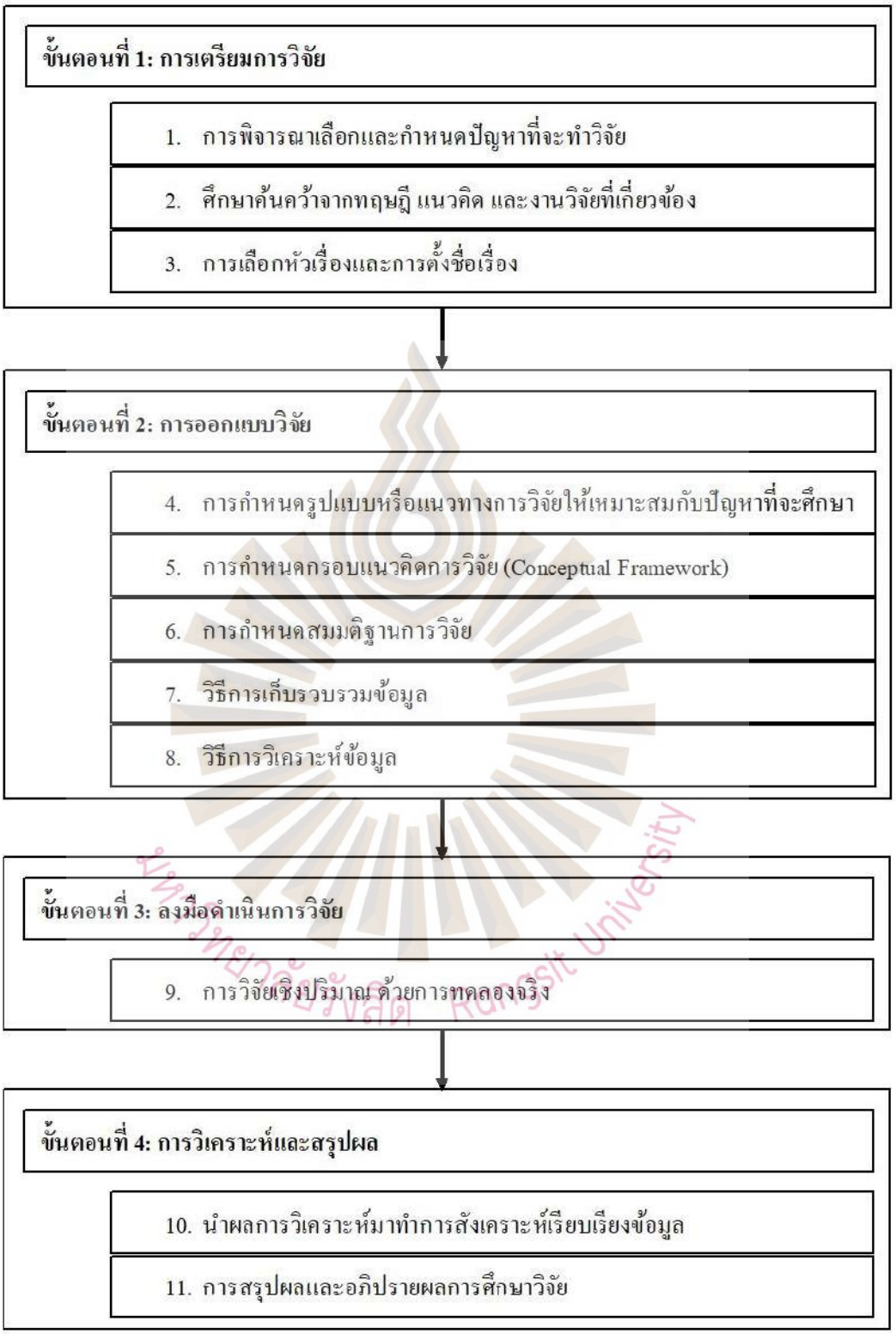
ที่จะศึกษา กำหนดสมมติฐานการวิจัยเพื่อให้บรรลุวัตถุประสงค์การวิจัย วิธีการเก็บรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและข้อมูลทุติยภูมิ และการใช้วิธีการวิเคราะห์ข้อมูลตลอดจนการเลือกใช้เครื่องมือการวิจัย ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยมีจุดมุ่งหมายที่จะนำเทคโนโลยีบล็อกเชนมาใช้ในการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามกรอบข้อกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และที่สำคัญยิ่งคือผลการวิจัยที่เป็นประโยชน์ต่อสังคมส่วนรวมทั้งในเชิงวิชาการและเชิงวิชาชีพที่เกี่ยวข้องกับการประยุกต์ใช้เทคโนโลยีบล็อกเชนในการควบคุม ป้องกัน และคุ้มครองข้อมูลส่วนบุคคลให้เป็น ไปตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3.1.3 ขั้นตอนที่ 3: การลงมือดำเนินงานวิจัย

ผู้วิจัยใช้การวิจัยเชิงปริมาณ (Quantitative Research) ด้วยการทดลองจริง (True Experiment) กับชุดข้อมูลรายได้สำหรับผู้ใหญ่ (US Adult Income dataset) หรือเรียกอีกชื่อหนึ่งว่า “adult.csv” เป็นชุดข้อมูลการสำรวจประชากรของสหรัฐอเมริกาในปีพ.ศ. 2537 นำข้อมูลชุดนี้มาจาก UCI Machine Learning Repository โดยใช้ร่วมกับระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต และเทคนิคการแฝงข้อมูล และใช้การวิเคราะห์เชิงเปรียบเทียบ (Comparative Analysis) เพื่อตอบการวิจัยตามวัตถุประสงค์ที่ตั้งไว้

3.1.4 ขั้นตอนที่ 4: การวิเคราะห์และสรุปผล

จากการศึกษา ทดสอบ และดำเนินการวิจัย ได้ทำการนำเสนอข้อมูล จัดระเบียบข้อค้นพบ สรุปผลการศึกษา อภิปรายผลการวิจัย ปัญหาอุปสรรค และให้ข้อเสนอแนะที่เป็นประโยชน์ในการนำผลวิจัยไปใช้และทำการวิจัยต่อยอดความรู้ต่อไป รวมทั้งจัดทำรูปเล่มเพื่อนำเสนอรายงานการวิจัยและจัดทำดุษฎีนิพนธ์ฉบับสมบูรณ์



รูปที่ 3.1 ขั้นตอนการดำเนินการวิจัย

3.2 แนวคิดหรือสิ่งที่นำเสนอ

3.2.1 ระบบเดิม

ไม่มี

3.2.2 แนวคิดที่นำเสนอ

การวิจัยนี้มุ่งเน้นการพัฒนาระบบที่ผสานบล็อกเชน (Blockchain) กับการจัดการความยินยอม (Consent Management) และการแฝงข้อมูล (Pseudonymization) ดังรูปที่ 3.2 เพื่อสร้างระบบที่มีความปลอดภัย โปร่งใส และสามารถตอบสนองต่อข้อกำหนดด้านการคุ้มครอง ข้อมูลส่วนบุคคลในยุคดิจิทัลได้อย่างมีประสิทธิภาพ ระบบนี้มีเป้าหมายสำคัญเพื่อ:

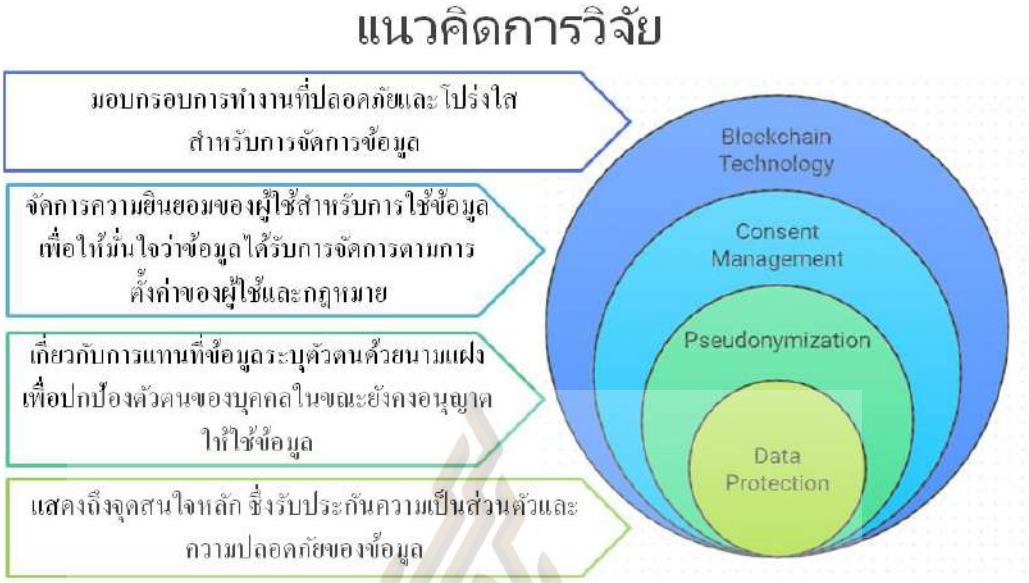
3.2.2.1 เสริมสร้างความเชื่อมั่นให้ผู้ใช้เกี่ยวกับการจัดการข้อมูลส่วนบุคคล โดยให้ผู้ใช้สามารถควบคุมและตรวจสอบการใช้งานข้อมูลของตนได้อย่างชัดเจน

3.2.2.2 ลดความเสี่ยงที่เกิดจากการละเมิดข้อมูลหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ผ่านกระบวนการแฝงข้อมูลที่ไม่เปิดเผยตัวตนจริงของผู้ใช้

3.2.2.3 สนับสนุนการปฏิบัติตามกฎหมายและข้อกำหนด เช่น จีดีพีอาร์หรือพีดีพีเอ ด้วยการจัดการข้อมูลส่วนบุคคลที่โปร่งใสและมีระบบตรวจสอบ

กรอบแนวคิดนี้ครอบคลุมทั้งกระบวนการ “การปกป้องข้อมูล (Data Protection)” “การสร้างระบบการแฝงข้อมูล (Pseudonymization System)” ที่ปลอดภัยและตรวจสอบได้ รวมถึงการออกแบบ “ระบบการจัดการความยินยอม (Consent Management System)” ที่ใช้ประโยชน์จาก ”เทคโนโลยีบล็อกเชน (Blockchain Technology)” เพื่อความโปร่งใสและลดการพึ่งพาหน่วยงานกลาง เทคโนโลยีบล็อกเชนช่วยเสริมความปลอดภัยด้วยการทำให้ข้อมูลเปลี่ยนแปลงไม่ได้ (Immutable) และสนับสนุนการบันทึกความยินยอมของผู้ใช้ในรูปแบบที่ตรวจสอบและบังคับใช้ได้โดยอัตโนมัติผ่านสัญญาอัจฉริยะ (Smart Contracts) ทั้งนี้ ระบบดังกล่าวสามารถนำไปประยุกต์ใช้ในหลากหลายบริบท เช่น การจัดการข้อมูลในภาคสุขภาพ การศึกษา หรือธุรกิจที่ต้องการปกป้องข้อมูลส่วนบุคคลในระดับสูงสุด จากรูปที่ 3.2 สามารถอธิบายแนวคิดการวิจัยที่นำเสนอได้ดังนี้

มหาวิทยาลัยรังสิต Rangsit University



รูปที่ 3.2 แนวคิดการวิจัยที่นำเสนอ

1) เทคโนโลยีบล็อกเชน (Blockchain Technology): มอบการทำงานที่ปลอดภัยและโปร่งใสในกระบวนการจัดการข้อมูล

1.1) บล็อกเชนทำหน้าที่เป็นโครงสร้างพื้นฐานที่เชื่อถือได้ในการบันทึกข้อมูลที่ไม่สามารถแก้ไขได้และช่วยให้เกิดความโปร่งใสในกระบวนการจัดการข้อมูลส่วนบุคคล

1.2) ใช้สัญญาอัจฉริยะเพื่อช่วยดำเนินกระบวนการบริหารจัดการความยินยอมอย่างอัตโนมัติและตรวจสอบได้

1.3) ช่วยลดปัญหาการบิดเบือนข้อมูลและเสริมความเชื่อมั่นให้ผู้ใช้

2) การบริการจัดการความยินยอม (Consent Management): จัดการความยินยอมของผู้ใช้สำหรับการใช้ข้อมูล เพื่อมั่นใจว่าข้อมูลได้รับการจัดการตามการคุ้มครองผู้ใช้และกฎหมาย

2.1) ผู้ใช้สามารถให้หรือถอนความยินยอมได้ตามความต้องการโดยมีบันทึกที่ตรวจสอบได้และไม่สามารถปลอมแปลงได้

2.2) การนำบล็อกเชนมาใช้ทำให้การจัดการความยินยอมสามารถควบคุมได้ในระดับบุคคลและปรับเปลี่ยนได้แบบเรียลไทม์

2.3) สร้างความมั่นใจว่าการใช้ข้อมูลเป็นไปตามกฎหมายที่เกี่ยวข้องเช่น จีดีพีอาร์ หรือ พีดีพีเอ

3) การแฝงข้อมูล (Pseudonymization): เกี่ยวกับการแทนที่ข้อมูลจริงด้วยข้อมูลแฝง เพื่อปกป้องตัวตนของบุคคลจากการอนุญาตให้ใช้ข้อมูล (เช่น ชื่อ หมายเลขบัตรประชาชน) ด้วยตัวระบุที่ไม่สามารถย้อนกลับไปหาเจ้าของข้อมูลได้โดยตรง

3.1) การใช้ฟังก์ชันแฮช (Hash Function) ช่วยลดความเสี่ยงจากการเปิดเผยตัวตนของผู้ใช้โดยตรง

3.2) เพิ่มความปลอดภัยในการจัดการข้อมูลขณะที่ยังสามารถนำไปใช้งานได้ในบริบทที่ไม่ต้องเปิดเผยตัวตน

3.3) การเชื่อมโยงข้อมูลแฝงกับบล็อกเชนช่วยเสริมความปลอดภัยในการจัดเก็บและตรวจสอบ

4) การคุ้มครองและปกป้องข้อมูล (Data Protection): แสดงถึงแกนหลักซึ่งรับประกันความเป็นส่วนตัวและความปลอดภัยของข้อมูล

4.1) การออกแบบระบบให้เป็นไปตามมาตรฐานการคุ้มครองข้อมูลระดับสากล เช่น จีดีพีอาร์ หรือ พีดีพีเอ เพื่อสร้างกรอบในการปกป้องข้อมูล

4.2) เน้นที่การจัดการและรักษาความปลอดภัยของข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือการละเมิด

4.3) การคุ้มครองข้อมูลเป็นหัวใจสำคัญที่ช่วยสร้างความเชื่อมั่นให้กับผู้ใช้ว่าข้อมูล ของตนจะได้รับการจัดการอย่างเหมาะสม

การกำหนดโครงสร้างความสัมพันธ์ของตัวแปรต่าง ๆ (Input-Process-Output-Outcome : IPOO Model): แบ่งออกเป็น 4 ส่วนสำคัญ คือ ปัจจัยนำเข้า (Input) กระบวนการ (Process) ผลผลิต (Output) และผลลัพธ์ (Outcome) การวิจัยฉบับนี้แสดงโครงสร้างความสัมพันธ์ของตัวแปรต่าง ๆ เป็น 3 โครงสร้างดังนี้

1) โครงสร้างความสัมพันธ์ของตัวแปร สำหรับภาพรวมของการวิจัย:

ตามหัวข้อการวิจัยเรื่อง “ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล (Blockchain-based Auxiliary System for Pseudonymization and Consent Management)” มีฟังก์ชันหลัก คือการผสานเทคโนโลยีบล็อกเชนกับเทคนิคการจัดการข้อมูลขั้นสูงเพื่อให้แน่ใจว่าระบบมีความปลอดภัย โปร่งใส และเคารพความเป็นส่วนตัว ช่วยให้องค์กรสามารถจัดการความยินยอมของผู้ใช้ได้อย่างมีประสิทธิภาพในขณะที่ปกป้อง

ข้อมูลผ่านการแปลงข้อมูลเป็นข้อมูลแฝงและการเข้ารหัส สามารถกำหนดโครงสร้างความสัมพันธ์ของตัวแปรต่าง ๆ ได้ดังรูปที่ 3.3 องค์ประกอบแต่ละอย่างมีความสำคัญต่อการออกแบบและการทำงานโดยรวมของระบบดังนี้

1.1) ปัจจัยนำเข้า (Input): แสดงถึงทรัพยากรพื้นฐานหรือข้อมูลที่จำเป็นในการเปิดใช้งานและรักษากระบวนการภายในระบบ ขั้นตอนนี้มีความสำคัญเนื่องจากเป็นการจัดหาข้อมูลดิบที่จำเป็นสำหรับการดำเนินการเพิ่มเติม เพื่อให้แน่ใจว่าระบบทำงานได้อย่างมีประสิทธิภาพ มีส่วนประกอบดังนี้:

(1) ข้อมูลส่วนบุคคล: รวมถึงข้อมูลที่ละเอียดอ่อน เช่น ชื่อ ที่อยู่ หมายเลขประจำตัวประชาชน และวันเกิด จุดข้อมูลเหล่านี้เป็นความลับอย่างยิ่งและต้องได้รับการจัดการอย่างปลอดภัยเพื่อให้แน่ใจว่ามีความเป็นส่วนตัวและเป็นไปตามข้อบังคับการปกป้องข้อมูล

(2) ข้อมูลความยินยอม: ประกอบด้วยการอนุญาตผู้ใช้ที่ชัดเจน ซึ่งให้ราย ละเอียดว่าสามารถเข้าถึง ใช้ หรือแบ่งปันข้อมูลส่วนบุคคลได้อย่างไร ซึ่งจะช่วยให้มีความโปร่งใสและสอดคล้องกับข้อกำหนดทางกฎหมาย เช่น จีดีพีอาร์ หรือ พีดีพีเอ

(3) บทบาทของปัจจัยนำเข้า คือ ทำหน้าที่เป็นจุดเริ่มต้นของกระบวนการของระบบ ปัจจัยนำเข้าจะถูกรับและเตรียมพร้อมสำหรับขั้นตอนต่อไป ซึ่งจะได้รับการแปลงและจัดการอย่างปลอดภัยเพื่อปกป้องความเป็นส่วนตัวของแต่ละบุคคลและเป็นไปตามมาตรฐานทางจริยธรรม

1.2) กระบวนการ (Process): ประกอบด้วยขั้นตอนปฏิบัติการ วิธีการ และเทคโนโลยีที่ใช้ในการแปลงข้อมูลดิบเป็นข้อมูลผลผลิตที่มีโครงสร้างและปลอดภัย ขั้นตอนสำคัญนี้ช่วยให้แน่ใจว่าข้อมูลที่ละเอียดอ่อนได้รับการจัดการในลักษณะที่รักษาความเป็นส่วนตัวของข้อมูล ความสมบูรณ์ และการปฏิบัติตามมาตรฐานทางกฎหมายและจริยธรรม ผ่านการผสมผสานเทคโนโลยี ขั้นสูงและกรอบงานที่แข็งแกร่ง กระบวนการนี้ช่วยให้แน่ใจว่าข้อมูลไหลผ่านระบบอย่างปลอดภัยและโปร่งใส สอดคล้องกับความคาดหวังของผู้ใช้และข้อกำหนดด้านกฎระเบียบ มีส่วนประกอบดังนี้

(1) การจัดการความยินยอม: องค์ประกอบหลักที่ให้กลไกที่มีโครงสร้างสำหรับการรวบรวมบันทึก และจัดการความยินยอมของผู้ใช้ ช่วยให้แน่ใจว่าผู้ใช้สามารถควบคุมวิธี การใช้ แบ่งปัน หรือจัดเก็บข้อมูลส่วนบุคคลของตนได้ ระบบนี้ส่งเสริมความโปร่งใสและความรับผิดชอบ ปฏิบัติตามกฎระเบียบความเป็นส่วนตัว เช่น จีดีพีอาร์ หรือ พีดีพีเอ

(2) การเข้ารหัสข้อมูล: การเข้ารหัสจะแปลงข้อมูลที่ละเอียดอ่อนเป็นรูป แบบที่เข้ารหัสได้ ซึ่งสามารถถอดรหัสได้โดยหน่วยงานที่ได้รับอนุญาตเท่านั้น ซึ่งช่วย

ให้แน่ใจถึงความลับของข้อมูลในขณะที่ถูกจัดเก็บหรือส่งผ่าน และป้องกันไม่ให้มีการเข้าถึงการละเมิดโดยไม่ ได้รับอนุญาต

(3) เทคโนโลยีบล็อกเชน: บล็อกเชนทำหน้าที่เป็นสมุดบัญชีแยกประเภทแบบกระจายอำนาจที่ให้บันทึกการทำธุรกรรมข้อมูลที่ไม่แปลงเปลี่ยน โปรงใส่ และตรวจสอบได้ ช่วยขจัดความเสี่ยงจากการถูกแทรกแซง ทำให้มั่นใจได้ถึงความน่าเชื่อถือในระบบโดยรักษาประวัติการจัดการข้อมูลที่ชัดเจนและไม่เปลี่ยนแปลง

(4) การแฝงข้อมูล: เทคนิคนี้จะแทนที่ข้อมูลที่ระบุตัวตนได้ด้วยนามแฝงหรือข้อมูลแฝง เช่น โทเค็นที่สร้างแบบสุ่มหรือค่าแฮช เพื่อปกป้องความเป็นส่วนตัวของแต่ละบุคคล การแฝงข้อมูลช่วยลดความเสี่ยงในการเปิดเผยข้อมูลที่ละเอียดอ่อนในขณะที่รักษาการใช้งานข้อมูลเพื่อวัตถุประสงค์ที่ถูกต้อง

(5) ฟังก์ชันแฮช: อัลกอริทึมการเข้ารหัส เช่น SHA256 สร้างตัวระบุที่ไม่ซ้ำกันและย้อนกลับไม่ได้สำหรับข้อมูลที่ละเอียดอ่อน การแฮชช่วยเพิ่มความปลอดภัยโดยทำให้แน่ ใจว่าไม่สามารถสร้างข้อมูลต้นฉบับขึ้นใหม่จากแฮชได้ ทำให้มีวิธีการตรวจสอบและความสมบูรณ์ของข้อมูลที่เชื่อถือได้

(6) บทบาทของกระบวนการ คือ ขั้นตอนกระบวนการมีความจำเป็นเพื่อให้แน่ใจว่าข้อมูลได้รับการจัดการอย่างปลอดภัย โปร่งใส และมีประสิทธิภาพ โดยใช้ประโยชน์จากเครื่องมือและเทคโนโลยีขั้นสูง ขั้นตอนนี้ไม่เพียงแต่ปกป้องข้อมูลที่ละเอียดอ่อนเท่านั้น แต่ยังรับประกันการปฏิบัติตามกฎหมายความเป็นส่วนตัวและมาตรฐานอุตสาหกรรมอีกด้วย ขั้นตอนนี้ช่วยวางรากฐานสำหรับความไว้วางใจและความน่าเชื่อถือในการทำงานของระบบ

1.3) ผลผลิต (Output): จะให้ผลลัพธ์ทันทีที่ระบบผลิตขึ้นจากดารประมวล ผลข้อมูลนำเข้า ผลผลิตเหล่านี้ได้รับการออกแบบมาเพื่อตอบสนองความต้องการของผู้ใช้และผู้มีส่วนได้ส่วนเสียโดยให้ข้อมูลที่ได้รับการจัดการอย่างปลอดภัยและเป็นไปตามความเป็นส่วนตัว ผลผลิตเหล่านี้ช่วยให้แน่ใจว่าข้อมูลที่ละเอียดอ่อนได้รับการประมวลผลและจัดเก็บในลักษณะที่ปกป้องความเป็นส่วนตัวในขณะที่ยังคงใช้งานได้สำหรับวัตถุประสงค์ที่ได้รับอนุญาต มีส่วน ประกอบดังนี้

(1) บันทึกความยินยอม: นี่คือบันทึกที่ไม่สามารถเปลี่ยนแปลงได้ซึ่งจัดเก็บไว้บนบล็อกเชน โดยมีรายละเอียดข้อกำหนดและเงื่อนไขในการให้ความยินยอมของผู้ใช้ บันทึกเหล่านี้รวมถึงวันที่และเวลา และรายละเอียดของสิทธิ์ที่ได้รับ เพื่อให้แน่ใจว่ามีความโปร่งใส ความรับผิดชอบ และการตรวจสอบย้อนกลับสำหรับการดำเนินการที่เกี่ยวข้องกับความยินยอมทั้งหมด

(2) ข้อมูลที่ใช้ข้อมูลแฝง: ระบบจะสร้างข้อมูลที่ใช้ข้อมูลแฝงหรือไม่ระบุชื่อเพื่อให้แน่ใจว่าตัวระบุส่วนบุคคลจะถูกแทนที่ด้วยข้อมูลแฝงหรือโทเค็น ซึ่งช่วยให้สามารถใช้ข้อมูลเพื่อการวิเคราะห์ การวิจัย หรือการจัดเก็บที่ปลอดภัยได้โดยไม่เสี่ยงต่อความเป็นส่วนตัวของผู้ใช้

(3) บทบาทของผลผลิค คือ แสดงถึงผลลัพธ์ที่จับต้องได้ของกระบวนการของระบบและทำหน้าที่เป็นตัวเชื่อมผสานที่สำคัญระหว่างระบบกับผู้ถือผลประโยชน์ด้วยการจัดทำผลผลิตที่ปลอดภัยและเน้นความเป็นส่วนตัว ระบบจึงมอบคุณค่าในรูปแบบของบันทึกความยินยอมที่เชื่อถือได้และข้อมูลที่รักษาความเป็นส่วนตัว ปฏิบัติตามมาตรฐานการปฏิบัติตามข้อกำหนด และสนับสนุนแนวทางการจัดการข้อมูลที่มีจริยธรรม

1.4) ผลลัพธ์ (Outcome): ครอบคลุมผลกระทบและประโยชน์ในระยะยาวที่กว้างขึ้นซึ่งเป็นผลมาจากผลผลิตของระบบ แม้ว่าผลผลิตจะแสดงถึงผลลัพธ์ในทันที แต่ผลลัพธ์ก็บ่งบอกถึงคุณค่าและประสิทธิภาพของผลลัพธ์เหล่านั้นในการบรรลุเป้าหมายโดยรวม ขั้นตอนนี้มีความ สำคัญในการวัดผลการสนับสนุนของระบบต่อความเป็นส่วนตัวของข้อมูล ความน่าเชื่อถือและการปฏิบัติตามข้อกำหนด เพื่อให้แน่ใจว่าสอดคล้องกับวัตถุประสงค์ขององค์กรและความคาดหวังของผู้ใช้ มีองค์ประกอบดังนี้

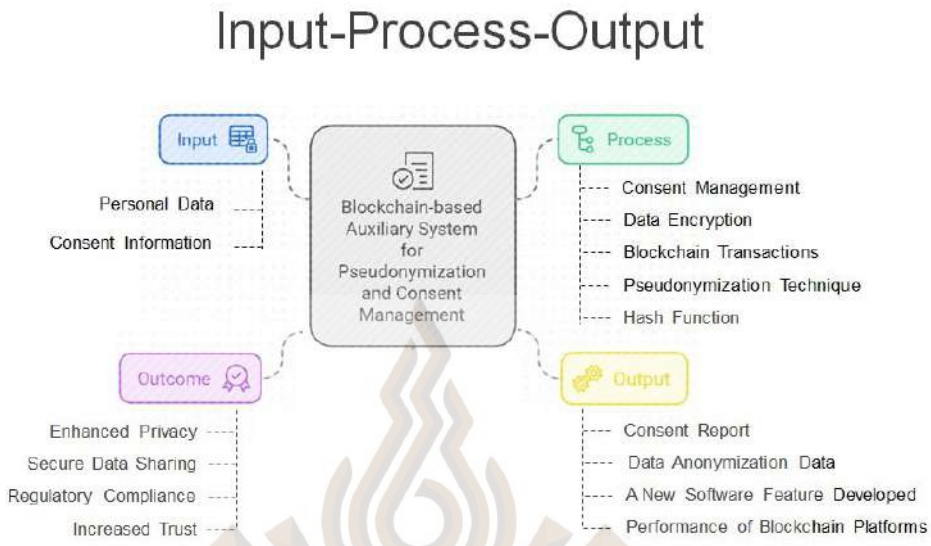
(1) ความเป็นส่วนตัวของข้อมูล: ระบบจะเสริมความแข็งแกร่งให้กับการปกป้องข้อมูลส่วนบุคคลโดยใช้มาตรการรักษาความปลอดภัยขั้นสูง เช่น การสร้างข้อมูลแฝง การเข้ารหัส และบันทึกที่ไม่เปลี่ยนแปลง วิธีนี้ช่วยให้มั่นใจได้ว่าข้อมูลที่ละเอียดอ่อนจะได้รับการปกป้อง ไม่ให้ถูกใช้ในทางที่ผิดหรือถูกละเมิด ส่งเสริมสภาพแวดล้อมดิจิทัลที่ปลอดภัย

(2) ความไว้วางใจของผู้ใช้: ระบบจะเพิ่มความมั่นใจของผู้ใช้ด้วยการแสดงให้เห็นถึงความโปร่งใส ความรับผิดชอบ และการจัดการความยินยอมที่แข็งแกร่ง ผู้ใช้รู้สึกมั่นใจว่าข้อมูลของตนได้รับการจัดการอย่างถูกต้องตามจริยธรรมและปลอดภัย ส่งเสริมความไว้วางใจและการมีส่วนร่วมในระยะยาว

(3) การปฏิบัติตามข้อบังคับ: ระบบจะรับประกันการปฏิบัติตามกฎหมายคุ้มครองข้อมูล เช่น จีดีพีอาร์ หรือ พีดีพีเอ ซึ่งจะช่วยลดความเสี่ยงทางกฎหมายสำหรับองค์กร หลีกเลี่ยงการลงโทษ และสนับสนุนวัฒนธรรมแห่งการปฏิบัติตามกฎเกณฑ์ ส่งผลให้ชื่อเสียงขององค์กรดีขึ้น

(4) บทบาทของผลลัพธ์ คือ ผลลัพธ์ทำหน้าที่เป็นส่วนตัวบ่งชี้หลักของความสำเร็จ ของระบบในการบรรลุวัตถุประสงค์ โดยเน้นย้ำถึงความสามารถของระบบในการปกป้องความเป็นส่วนตัว สร้างความไว้วางใจ และปฏิบัติตามข้อกำหนดด้านข้อบังคับ และจะ

ช่วยให้มั่นใจได้ถึงคุณค่า ที่ยั่งยืนสำหรับทั้งผู้ใช้และองค์กร



รูปที่ 3.3 IPOO Model ภาพรวมงานวิจัย

2) โครงสร้างความสัมพันธ์ของตัวแปร สำหรับระบบบริหารจัดการความยินยอม:

เป็นกรอบงานที่สำคัญสำหรับสภาพแวดล้อมที่ความเป็นส่วนตัวของผู้ใช้และความปลอดภัยของข้อมูลเป็นสิ่งสำคัญที่สุด ตัวอย่างได้แก่ การดูแลสุขภาพ บริการทางเงิน และแพลตฟอร์มดิจิทัลที่ข้อมูลส่วนบุคคลที่ละเอียดอ่อนได้รับการจัดการเป็นประจำ โดยนำเสนอแนวทางที่มีโครงสร้างเพื่อให้แน่ใจว่าทุกขั้นตอนตั้งแต่การป้อนข้อมูลไปจนถึงผลลัพธ์ขั้นสุดท้ายได้รับการจัด การอย่างปลอดภัยและมีประสิทธิภาพ ด้วยการใช้ประโยชน์จากการกำหนดโครงสร้างของตัวแปรนี้ ระบบจะปรับปรุงความน่าเชื่อ การปฏิบัติตาม และความโปร่งใส โดยสอดคล้องกับมาตรฐานการกำกับดูแล เช่น จีดีพีอาร์หรือพีดีพีเอ ซึ่งช่วยให้มั่นใจได้ถึงความสมดุลระหว่างการปกป้องข้อมูลของผู้ใช้และการเปิดใช้งานการใช้งานอย่างมีจริยธรรมและมีประสิทธิภาพ สามารถกำหนดโครงสร้างความสัมพันธ์ของตัวแปรต่าง ๆ ได้ดังรูปที่ 3.4 องค์ประกอบแต่ละอย่างมีความสำคัญต่อการออกแบบและการทำงานโดยรวมของระบบดังนี้

2.1) ปัจจัยนำเข้า (Input): แสดงถึงข้อมูลพื้นฐานและทรัพยากรที่เข้าสู่ระบบเพื่อเริ่มกระบวนการจัดการความยินยอม ขั้นตอนนี้มีความสำคัญเนื่องจากเป็นขั้นตอนที่จัดเตรียมข้อมูลดิบที่จำเป็นสำหรับการดำเนินการทั้งหมดที่ตามมา ข้อมูลนำเข้าจะได้ รับการจัดการอย่างระมัดระวังเพื่อให้แน่ใจว่ามีความถูกต้อง ปลอดภัย และเป็นไปตามข้อบังคับเกี่ยวกับการคุ้มครอง

ข้อมูล มีส่วนประกอบดังนี้

(1) ข้อมูลส่วนบุคคล: รวมถึงข้อมูลที่ละเอียดอ่อน เช่น ชื่อ หมายเลขประจำตัวประชาชน ที่อยู่ และรายละเอียดส่วนบุคคลอื่น ๆ ข้อมูลนำเข้าเหล่านี้มีความสำคัญต่อการระบุตัวตนของผู้ใช้และการจัดการความยินยอมของผู้ใช้ แต่ต้องมีการปกป้องอย่างเข้มงวดเพื่อให้แน่ใจว่ามีความเป็นส่วนตัวและป้องกันการใช้งานในทางที่ผิด

(2) ข้อมูลการปฏิบัติตามกฎระเบียบ: หมายถึงข้อมูลทางกฎหมายและข้อบังคับที่จำเป็นเพื่อให้แน่ใจว่ากระบวนการจัดการความยินยอมสอดคล้องกับกฎหมายคุ้มครองข้อมูล เช่น จีดีพีอาร์หรือพีดีพีเอ ซึ่งจะช่วยให้มั่นใจได้ว่าระบบทำงานภายในขอบเขตทางกฎหมายและปฏิบัติตามแนวทางปฏิบัติที่ดีที่สุดในการจัดการความเป็นส่วนตัว

(3) บทบาทของข้อมูลนำเข้า: เป็นจุดเริ่มต้นที่สำคัญสำหรับระบบการจัดการความยินยอม ระบบจะจัดหาข้อมูลที่จำเป็นในการประมวลผล วิเคราะห์และสร้างผลผลิตที่ปลอดภัยและเป็นไปตามข้อกำหนด หากขาดข้อมูลนำเข้าที่ผ่านการคัดสรรมาอย่างรอบคอบ ระบบจะไม่สามารถทำงานได้อย่างมีประสิทธิภาพ ส่งผลให้ความสามารถในการจัดการความยินยอมและปกป้องความเป็นส่วนตัวของผู้ใช้ลดลง

2.2) กระบวนการ (Process): ประกอบด้วยขั้นตอนและกิจกรรมที่มีโครงสร้างชุดหนึ่งที่มุ่งเป้าไปที่การจัดการ ติดตาม และจัดเก็บความยินยอมของผู้ใช้อย่างปลอดภัย ขั้นตอนนี้มีความสำคัญอย่างยิ่งต่อการทำให้แน่ใจว่าการโต้ตอบที่เกี่ยวกับความยินยอมทั้งหมดเป็นระบบ โปร่งใส และสอดคล้องกับกฎหมายคุ้มครองข้อมูล กระบวนการนี้ใช้เทคโนโลยีขั้นสูงและขั้นตอนการทำงานที่เน้นผู้ใช้ เพื่อรักษาความรับผิดชอบและความไว้วางใจตลอดวงจรชีวิตการจัดการความยินยอม มีขั้นตอนการทำงานดังนี้

(1) ส่งคำขอ: ผู้ใช้หรือองค์กรส่งคำขอเพื่อเข้าถึงหรือประมวลผลข้อมูลเฉพาะ คำขอนี้จะเริ่มกระบวนการจัดการความยินยม

(2) เขียนความยินยอม: ระบบจะสร้างเอกสารความยินยอม โดยระบุข้อกำหนด เงื่อนไข และวัตถุประสงค์ในการใช้ข้อมูล พร้อมทั้งให้ข้อตกลงที่ชัดเจนและมีรายละเอียดแก่ผู้ใช้

(3) แจ้งเจ้าของข้อมูล: เจ้าของข้อมูล (ผู้ใช้) จะได้รับแจ้งเกี่ยวกับคำขอความยินยอมและได้รับโอกาสในการตรวจสอบรายละเอียดที่เกี่ยวข้องทั้งหมด เพื่อให้แน่ใจว่ามีความโปร่งใส

(4) อนุมัติโดยเจ้าของข้อมูล: ผู้ใช้ประเมินคำขอความยินยอมและให้การอนุมัติหรือปฏิเสธตามความชอบและระดับความสบายใจเกี่ยวกับการใช้ข้อมูล

(5) ปรับปรุงสถานะ: ระบบจะปรับปรุงสถานะความยินยอมเพื่อสะท้อนการตัดสินใจของผู้ใช้ โดยสร้างบันทึกแบบเรียลไทม์ของกิจกรรมความยินยอม

(6) การตอบกลับ: ระบบจะส่งการตอบกลับไปยังหน่วยงานที่ร้องขอเพื่อยืนยันว่าคำขอความยินยอมได้รับการอนุมัติหรือปฏิเสธ

(7) ธุรกรรมบล็อกเชน: ข้อมูลความยินยอมจะถูกบันทึกอย่างปลอดภัยในสมุดบันทึกบล็อกเชน ขั้นตอนนี้รับรองความไม่เปลี่ยนแปลง ความโปร่งใสและการตรวจสอบย้อนกลับของบันทึกความยินยอมทั้งหมด

(8) บทบาทของกระบวนการ: รับประกันว่ากิจกรรมการจัดการความยินยอม ทั้งหมดดำเนินการอย่างเป็นระบบ โดยรักษาความปลอดภัยและความโปร่งใส นอกจากนี้ยังสร้างกรอบงานที่เชื่อถือได้ ซึ่งส่งเสริมความไว้วางใจและรับรองการปฏิบัติตามข้อบังคับด้านความเป็นส่วนตัว

2.3) ผลผลิต (Output): แสดงถึงผลลัพธ์ที่เกิดขึ้นทันทีและเป็นรูปธรรมจากระบบการจัดการความยินยอม ผลผลิตเหล่านี้ให้ข้อมูลและบันทึกที่สำคัญแก่ผู้ถือประโยชน์ ช่วยให้เกิดความโปร่งใส สามารถตรวจสอบย้อนกลับได้และปฏิบัติตามกฎระเบียบ ผลผลิตที่ได้รับการออกแบบมาให้ดำเนินการได้และน่าเชื่อถือ สะท้อนถึงประสิทธิภาพของระบบในการจัดการและปกป้องความยินยอมของผู้ใช้ มีส่วนประกอบดังนี้

(1) รายงานความยินยอม: คือเอกสารหรือบันทึกดิจิทัลที่ครอบคลุมซึ่งสรุปรายละเอียดความยินยอมที่ผู้ใช้ให้มา ซึ่งรวมถึงข้อมูลที่จำเป็น เช่น เงื่อนไขความยินยอม เวลาของการดำเนินการของผู้ใช้ และการอนุมัติหรือการปฏิเสธโดยชัดเจน รายงานนี้ทำหน้าที่เป็นข้อมูลอ้างอิงสำหรับวัตถุประสงค์ด้านความรับผิดชอบและการตรวจสอบ

(2) การนำบล็อกเชนไปใช้งาน: บันทึกความยินยอมจะถูกจัดเก็บเป็นธุรกรรมบนแพลตฟอร์มบล็อกเชน เพื่อให้แน่ใจว่าบันทึกจะไม่เปลี่ยนแปลง ไม่ถูกดัดแปลงและตรวจสอบย้อนกลับได้ ทำให้มีเส้นทางการตรวจสอบที่โปร่งใสและเชื่อถือได้สำหรับกิจกรรมที่เกี่ยวข้องกับความยินยอมทั้งหมด

(3) บทบาทของผลผลิต: จะส่งมอบผลลัพธ์ที่วัดผลได้และดำเนินการได้ให้กับผู้ถือประโยชน์ ช่วยให้ปฏิบัติตามกฎระเบียบความเป็นส่วนตัวได้ง่ายขึ้น เพิ่มความรับผิดชอบและสร้างความไว้วางใจในหมู่ผู้ใช้ด้วยการจัดทำบันทึกการจัดการความยินยอมที่ปลอดภัยและโปร่งใส

2.4) ผลลัพธ์ (Outcome): จะเน้นที่ผลกระทบและผลประโยชน์ในระยะยาวจากผลผลิตของระบบ ซึ่งแตกต่างจากผลลัพธ์ที่เกิดขึ้นทันที ผลลัพธ์จะวัดประสิทธิภาพ

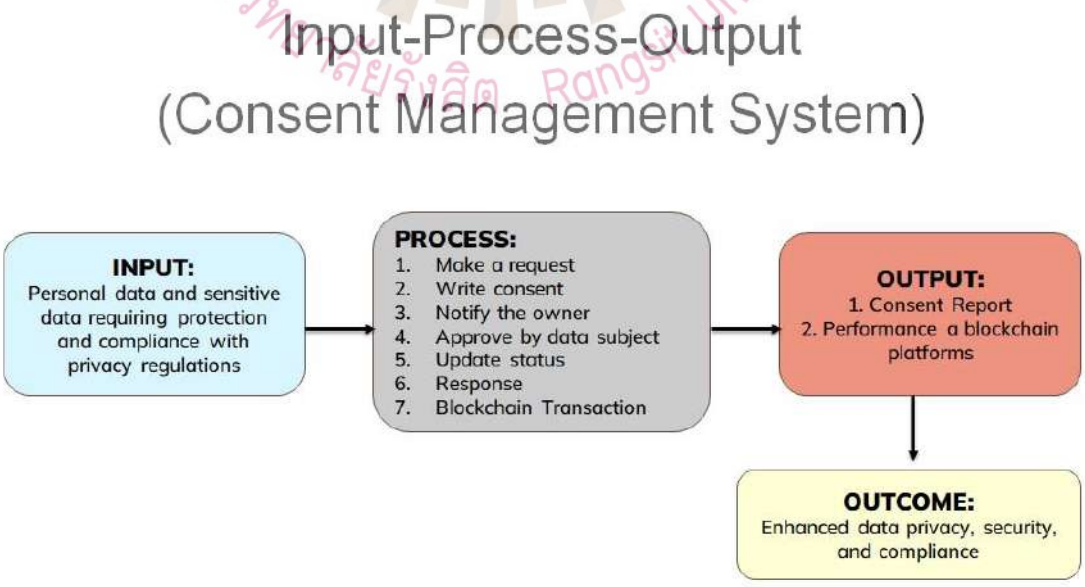
โดยรวมของระบบในการบรรลุวัตถุประสงค์ในช่วงเวลาหนึ่ง ผลลัพธ์เหล่านี้แสดงให้เห็นถึงคุณค่าของระบบในการเพิ่มความเป็นส่วนตัว ความปลอดภัย และการปฏิบัติตามข้อกำหนด ขณะเดียวกันก็ส่งเสริมความไว้วางใจระหว่างผู้ถือผลประโยชน์และผู้ใช้ มีส่วนประกอบดังนี้

(1) ความเป็นส่วนตัวของข้อมูลที่ปรับปรุง: ระบบจะรับประกันว่าข้อมูลของผู้ใช้ได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานในทางที่ผิดหรือการฝ่าฝืน โดยการใช้เทคนิคการเข้ารหัสและการทำให้เป็นข้อมูลแฝงที่แข็งแกร่ง ระบบจะรักษาความลับของข้อมูลที่ละเอียดอ่อน

(2) ความปลอดภัยที่ได้รับการปรับปรุง: ระบบจะรักษาความปลอดภัยของบันทึกความยินยอมผ่านสมุดบัญชีแยกประเภทที่ไม่เปลี่ยนแปลงของบล็อกเชน ทำให้บันทึกเหล่านั้นป้องกันการปลอมแปลงและป้องกันการฉ้อโกง ซึ่งจะช่วยเสริมความสมบูรณ์ของกระบวนการจัดการข้อมูลและป้องกันกิจกรรมที่เป็นอันตราย

(3) การปฏิบัติตามข้อบังคับ: ระบบรองรับการปฏิบัติตามข้อบังคับเกี่ยวกับการปกป้องข้อมูล เช่น จีดีพีอาร์และพีดีพีเอ โดยการรักษาบันทึกที่โปร่งใสและตรวจสอบได้ จึงลดความเสี่ยงของการไม่ปฏิบัติตามข้อบังคับและโทษทางกฎหมายที่เกี่ยวข้อง

(4) บทบาทของผลลัพธ์: สะท้อนถึงความสำเร็จของระบบในการบรรลุเป้าหมายโดยรวม ผลลัพธ์เหล่านี้ช่วยยืนยันความสามารถของระบบในการให้การปกป้องความเป็นส่วนตัวที่แข็งแกร่ง รับรองการปฏิบัติตามข้อบังคับ และสร้างความไว้วางใจและความเชื่อมั่นในระยะยาวระหว่างผู้ใช้และผู้มีส่วนได้ส่วนเสีย



รูปที่ 3.4 IPOO Model ระบบบริหารจัดการความยินยอม

3) โครงสร้างความสัมพันธ์ของตัวแปร สำหรับการแฝงข้อมูล:

การประยุกต์ใช้โครงสร้างความสัมพันธ์ของตัวแปรกับระบบการแฝงข้อมูลร่วมกับฟังก์ชันแฮช แนวทางที่มีโครงสร้างนี้ผสานเทคนิคขั้นสูงที่รักษาความเป็นส่วนตัวเพื่อปกป้องข้อมูลที่ละเอียดอ่อนในขณะที่รักษาการใช้งานและการทำงานของระบบไว้ โดยการใช้ฟังก์ชันแฮช การเข้ารหัสร่วมด้วย ระบบจะแปลงข้อมูลที่ระบุตัวตนเป็นข้อมูลแฝง ช่วยเพิ่มความเป็นส่วนตัวและลดความเสี่ยงในการเข้าถึงโดยไม่ได้รับอนุญาต กรอบงานโครงสร้างความสัมพันธ์ของตัวแปรช่วยให้เกิดการไหลอย่างเป็นระบบ ตั้งแต่การจัดการข้อมูลนำเข้าอย่างปลอดภัย การประมวลผลข้อมูลผ่านวิธีการสร้างข้อมูลแฝงที่แข็งแกร่ง การสร้างผลผลิตที่ให้ความสำคัญกับการปฏิบัติตามข้อบังคับการปกป้องข้อมูล เช่น จีดีพีอาร์หรือพีดีพีเอ ซึ่งช่วยให้เกิดความสมดุลระหว่างความปลอดภัยของข้อมูลและประสิทธิภาพการทำงาน สามารถกำหนดโครงสร้างความสัมพันธ์ของตัวแปรต่าง ๆ ได้ดังรูปที่ 3.5 องค์ประกอบแต่ละอย่างมีความสำคัญต่อการออกแบบและการทำงานโดยรวมของระบบดังนี้

3.1) ปัจจัยนำเข้า (Input): ประกอบด้วยข้อมูลดิบที่จำเป็นในการเริ่มกระบวนการแปลงข้อมูลเป็นข้อมูลแฝง โดยทั่วไปข้อมูลนี้รวมถึงข้อมูลระบุตัวตนส่วนบุคคลที่ละเอียดอ่อน (PII) ซึ่งต้องมีการจัดการและการแปลงข้อมูลอย่างปลอดภัยเพื่อปกป้องความเป็นส่วนตัวของแต่ละบุคคลและเป็นไปตามมาตรฐานการกำกับดูแล มีส่วนประกอบดังนี้

(1) ชุดข้อมูลที่มีข้อมูลระบุตัวตนส่วนบุคคล (PII): ซึ่งรวมถึงองค์ประกอบข้อมูล เช่น ชื่อ หมายเลขประกันสังคม ที่อยู่ วันเกิด และตัวระบุอื่น ๆ ที่อาจเปิดเผยตัวตนของบุคคลโดยทางตรงหรือโดยทางอ้อม

(2) บทบาทของข้อมูลนำเข้า: ทำหน้าที่เป็นข้อมูลพื้นฐานสำหรับกระบวนการแปลงข้อมูลเป็นข้อมูลแฝง โดยให้ข้อมูลที่ละเอียดอ่อนซึ่งจะต้องแปลงเป็นรูปแบบที่ไม่ระบุตัวตนหรือไม่ระบุตัวตน เพื่อให้เป็นไปตามข้อบังคับด้านความเป็นส่วนตัว เช่น จีดีพีอาร์หรือพีดีพีเอ การจัดการขั้นตอนนี้อย่างเหมาะสมถือเป็นสิ่งสำคัญในการรักษาความสมบูรณ์และความปลอดภัยของข้อมูล

3.2) กระบวนการ (Process): เกี่ยวข้องกับลำดับการทำงานที่มีโครงสร้างซึ่งออกแบบมาเพื่อใช้ข้อมูลแฝงและไม่ระบุตัวตนอย่างปลอดภัยในขณะที่ยังคงประโยชน์ในการวิเคราะห์ ขั้นตอนเหล่านี้จะช่วยให้แน่ใจว่าข้อมูลที่ละเอียดอ่อนได้รับการปกป้องและเป็นไปตามมาตรฐานความเป็นส่วนตัวโดยแปลงชุดข้อมูลเป็นรูปแบบที่ลดความเสี่ยงในการระบุตัวตนซ้ำ ประกอบด้วยขั้นตอนต่อไปนี้

(1) การทำความสะอาดข้อมูล: เตรียมชุดข้อมูลโดยระบุและแก้ไขข้อผิดพลาด ลบความไม่สอดคล้องกัน และตรวจสอบให้แน่ใจว่ารายการธุรกรรมทั้งหมดสมบูรณ์และถูกต้อง ขั้นตอนนี้มีความจำเป็นสำหรับการบรรลุผลลัพธ์การใช้ข้อมูลแฝงที่มีคุณภาพสูง

(2) สร้างรหัสประจำตัวปลอมและสร้างที่อยู่แฮช: ใช้ฟังก์ชันแฮชการเข้ารหัสเพื่อสร้างตัวระบุข้อมูลแฝงที่ไม่ซ้ำใครและไม่สามารถย้อนกลับได้สำหรับข้อมูลที่ละเอียดอ่อน โดยให้แน่ใจว่าไม่สามารถสร้างตัวระบุเดิมขึ้นมาใหม่ได้

(3) สร้างรหัสเทียม: กำหนดรหัสเทียมให้กับแอตทริบิวต์เฉพาะเพื่อปกปิดค่าจริงในขณะที่ยังคงอรรถประโยชน์เชิงวิเคราะห์ไว้สำหรับวัตถุประสงค์ทางสถิติหรือการปฏิบัติ

(4) แยกข้อมูลส่วนบุคคลที่ระบุตัวตนได้ (PII): แยกข้อมูลส่วนบุคคลที่ละเอียดอ่อนออกจากข้อมูลที่ไม่ละเอียดอ่อนเพื่อลดความเสี่ยงในการเปิดเผยข้อมูลและเพิ่มความเป็นส่วนตัว

(5) ทำให้เป็นคุณลักษณะเสมือนด้วย k-Anonymity: ใช้เทคนิคการทำให้เป็นคุณลักษณะทั่วไป เช่น การจัดกลุ่มอายุเป็นช่วงหรือสถานที่เป็นภูมิภาคที่กว้างขึ้น เพื่อให้ได้ k-Anonymity และลดโอกาสในการระบุตัวตนซ้ำ

(6) การแจกแจงคุณลักษณะย่อย: จัดประเภทคุณลักษณะข้อมูลเป็นคลาสย่อยตามกฎที่กำหนดไว้ล่วงหน้า โดยรักษาโครงสร้างของข้อมูลไว้ในขณะที่เพิ่มการปกป้องความเป็นส่วนตัว

(7) แสดงการแจกแจงคุณลักษณะเสมือน: แสดงภาพการแจกแจงของตัวระบุเสมือนในชุดข้อมูลเพื่อให้แน่ใจว่าเกณฑ์การไม่เปิดเผยข้อมูล เช่น k-Anonymity ได้รับการปฏิบัติตามอย่างเหมาะสม

(8) การประเมินประสิทธิภาพ: ประเมินประสิทธิภาพของระบบโดยวัดค่าต่าง ๆ เช่น ความเร็วในการประมวลผล ความทนทานของความปลอดภัย และความสามารถในการใช้งานข้อมูล เพื่อให้แน่ใจว่าระบบการทำให้เป็นข้อมูลแฝงบรรลุเป้าหมายที่ตั้งใจไว้

(9) บทบาทของกระบวนการ: มีบทบาทสำคัญในการทำให้ข้อมูลเป็นข้อมูลแฝงอย่างปลอดภัยในขณะที่ยังคงความสามารถในการใช้งานเพื่อการวิเคราะห์ กระบวนการนี้ช่วยลดความเสี่ยงต่อความเป็นส่วนตัวให้เหลือน้อยที่สุดโดยแปลงข้อมูลที่ละเอียดอ่อนให้เป็นรูปแบบที่ปฏิบัติตามมาตรฐานความเป็นส่วนตัวและบรรเทาความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการระบุตัวตนซ้ำ

3.3) ผลผลิต (Output): แสดงผลลัพธ์ทันทีที่เกิดจากกระบวนการแปลงข้อมูลเป็นข้อมูลแฝงและไม่ระบุชื่อ ผลลัพธ์เหล่านี้ได้รับการออกแบบมาเพื่อรักษาสมดุลระหว่างความต้องการความเป็นส่วนตัวของข้อมูลกับความสามารถในการใช้งานข้อมูลเพื่อการวิเคราะห์ โดยรับรองทั้งความสอดคล้องกับระเบียบข้อบังคับด้านความเป็นส่วนตัวและการบำรุงรักษาอรรถประโยชน์ของข้อมูล มีส่วนประกอบดังนี้

(1) ชุดข้อมูลที่ไม่ระบุตัวตนที่ใช้งานได้สำหรับการวิเคราะห์: ชุดข้อมูลที่แปลงแล้วซึ่งข้อมูลที่ระบุตัวตนได้ (PII) ได้ถูกแปลงเป็นข้อมูลแฝงหรือไม่ระบุชื่อ ชุดข้อมูลเหล่านี้มีความปลอดภัยและเหมาะสำหรับงานวิเคราะห์ โดยไม่เปิดเผยข้อมูลที่ละเอียดอ่อน

(2) การทำให้ข้อมูลไม่ระบุชื่อ: ข้อมูลที่ถูกตัดข้อมูลที่ระบุตัวตนออกไปทั้งหมด ทำให้ไม่สามารถติดตามกลับไปยังบุคคลได้ ซึ่งช่วยให้มั่นใจได้ว่าเป็นไปตามกรอบกฎหมายและข้อบังคับ เช่น จีดีพีอาร์หรือพีดีพีเอ

(3) บทบาทของผลผลิต: มีบทบาทสำคัญในการจัดเตรียมชุดข้อมูลที่รักษาความเป็นส่วนตัวซึ่งช่วยให้วิเคราะห์ข้อมูลได้อย่างปลอดภัย ชุดข้อมูลเหล่านี้ช่วยให้องค์กรสามารถดำเนินการวิจัย รับข้อมูลเชิงลึก หรือพัฒนากลยุทธ์โดยไม่กระทบต่อตัวตนของแต่ละบุคคล ทำให้มั่นใจได้ถึงประสิทธิภาพในการปฏิบัติงานและแนวทางการจัดการข้อมูลที่ถูกต้องตามจริยธรรม

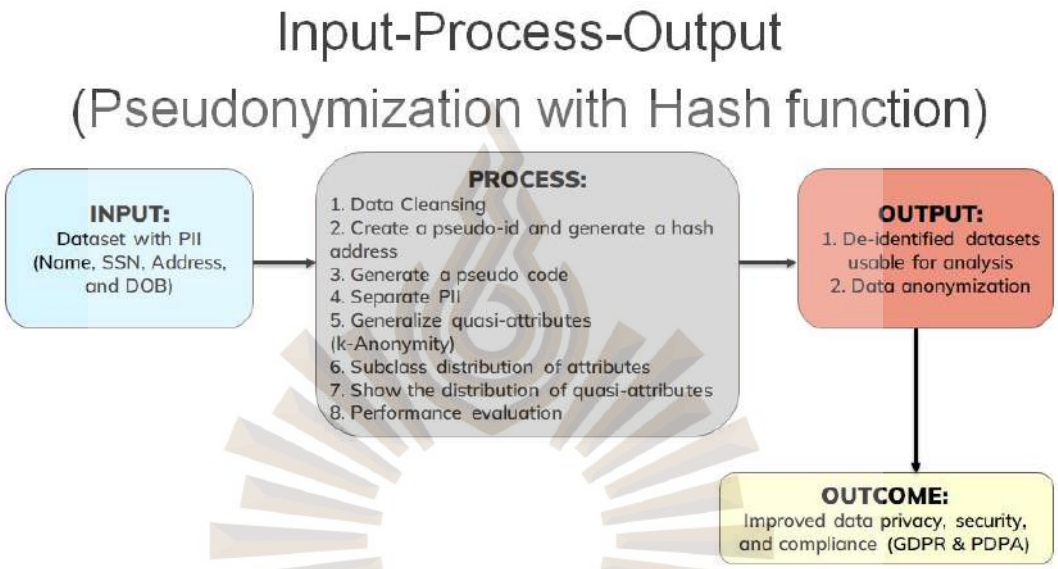
3.4) ผลลัพธ์ (Outcome): หมายถึงผลประโยชน์ในระยะยาวและผลกระทบที่กว้างขึ้นที่ได้รับจากการนำระบบการทำให้เป็นข้อมูลแฝงและการไม่เปิดเผยตัวตนมาใช้ ระบบจะเน้นย้ำถึงวิธีการที่ระบบมีส่วนสนับสนุนในการปรับปรุงความเป็นส่วนตัวของข้อมูล ความปลอดภัย และการปฏิบัติตามมาตรฐานทางกฎหมาย สร้างรากฐานของความไว้วางใจและความรับผิดชอบในแนวทางการจัดการข้อมูล มีส่วนประกอบดังนี้

(1) การปรับปรุงความเป็นส่วนตัวของข้อมูล: ช่วยให้แน่ใจว่าข้อมูลส่วนบุคคลที่ละเอียดอ่อนได้รับการปกป้องโดยทำให้ไม่สามารถเชื่อมโยงข้อมูลที่ไม่เปิดเผยตัวตนกลับไปยังบุคคลใดบุคคลหนึ่งได้ ซึ่งจะช่วยลดความเสี่ยงของการละเมิดความเป็นส่วนตัว

(2) การรักษาความปลอดภัยชั้นสูง: ใช้เทคนิคการเข้ารหัสและมาตรการไม่เปิดเผยตัวตนชั้นสูงเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การใช้ในทางที่ผิด หรือการละเมิดข้อมูล ช่วยเสริมสร้างความสมบูรณ์ของระบบ

(3) การปฏิบัติตามข้อบังคับ: ช่วยให้องค์กรปฏิบัติตามข้อกำหนดทางกฎหมายและข้อบังคับสำหรับการปกป้องข้องมูล เช่น จีดีพีอาร์หรือพีดีพีเอ ทำให้มั่นใจได้ว่าการดำเนินการสอดคล้องกับกฎหมายความเป็นส่วนตัวและมาตรฐานทางจริยธรรมในปัจจุบัน

(4) บทบาทของผลลัพธ์: บ่งชี้ถึงประสิทธิภาพของระบบในการบรรลุวัตถุประสงค์หลัก ได้แก่ การปกป้องข้อมูลที่ละเอียดอ่อน การเพิ่มความไว้วางใจของผู้ใช้ และการรับรองการปฏิบัติตามกรอบการกำกับดูแล นอกจากนี้ยังวางรากฐานสำหรับนวัตกรรมเพิ่มเติมในแนวทางการจัดการข้อมูลที่รักษาความเป็นส่วนตัวอีกด้วย



รูปที่ 3.5 IPOO Model ระบบการแฝงข้อมูล

3.2.3 ระบบที่นำเสนอ

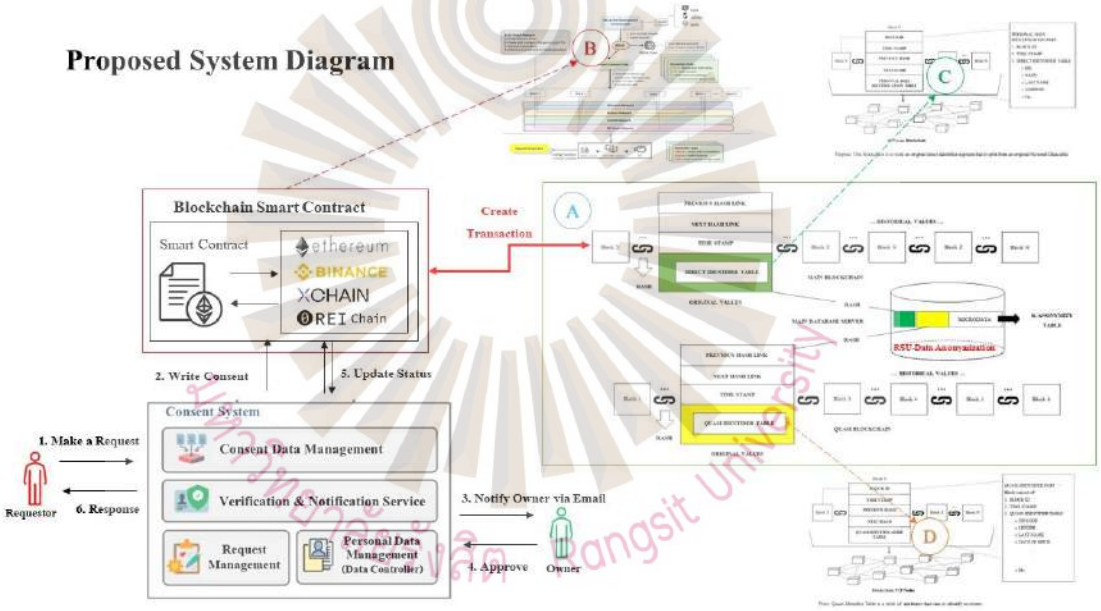
งานวิจัยฉบับนี้ผู้เขียนได้นำเสนอ “ระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล” ซึ่งเป็นระบบที่ซับซ้อนที่เกี่ยวกับเทคโนโลยีบล็อกเชนสำหรับการจัดการข้อมูลส่วนบุคคลโดยเน้นการจัดการความยินยอมและการแฝงข้อมูล เป็นระบบที่ออกแบบมาเพื่อปกป้องข้อมูลและความเป็นส่วนตัวโดยใช้ประโยชน์จากจุดแข็งของเทคโนโลยีบล็อกเชน กล่าวคือ ความไม่เปลี่ยนแปลง ความโปร่งใส และความปลอดภัยที่แข็งแกร่ง คุณสมบัติเหล่านี้มีประโยชน์อย่างยิ่งในการรับรองความสมบูรณ์และการรักษาความลับของข้อมูลส่วนบุคคล และจำเป็นต้องปฏิบัติตามกฎระเบียบการปกป้องข้อมูลส่วนบุคคลที่เข้มงวด เช่น จีดีพีอาร์หรือพีดีพีเอ ดังรูปที่ 3.6 ซึ่งงานวิจัยฉบับนี้ได้แยกการทดลองออกเป็น 2 ส่วนออกจากกัน ได้แก่

1) การใช้สัญญาอัจฉริยะบนบล็อกเชนร่วมกับระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS): ส่วนนี้เกี่ยวข้องกับการบูรณาการสัญญาอัจฉริยะบนบล็อกเชน

เข้ากับระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS) การทดลองจะทดสอบสัญญาอัจฉริยะเหล่านี้บนแพลตฟอร์มบล็อกเชนต่าง ๆ เช่น ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain) เพื่อประเมินประสิทธิภาพและความสามารถในการทำงานร่วมกันภายในเครือข่ายมหาวิทยาลัยรังสิต

2) การใช้เทคนิคการแฝงข้อมูลโดยการทดลองร่วมกับโครงการนำร่องที่ชื่อว่า RSU-Data-Anonymization โดยใช้เทคนิค k-Anonymity

การวิจัยนี้มีจุดมุ่งหมายเพื่อสาธิตการประยุกต์ใช้เทคโนโลยีบล็อกเชนในทางปฏิบัติเพื่อความเป็นส่วนตัวของข้อมูลและการจัดการความยินยอม ซึ่งสอดคล้องกับมาตรการทางกฎหมายสำหรับการปกป้องข้อมูล เช่น จีดีพีอาร์และพีดีพีเอ



รูปที่ 3.6 สถาปัตยกรรมของระบบที่นำเสนอ

รูปที่ 3.6 แสดงออกประกอบหลักของระบบที่นำเสนอ ซึ่งสามารถอธิบายรายละเอียดของแต่ละองค์ประกอบได้ดังนี้

3.2.3.1 ระบบบริหารจัดการความยินยอมที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชน:

เป็นกรอบการทำงานชั้นสูงและเป็นแนวคิดนวัตกรรมที่ออกแบบมาเพื่อบริหาร

จัดการความยินยอมของผู้ใช้สำหรับการใช้ข้อมูลในลักษณะที่ปลอดภัย โปร่งใส และมีประสิทธิภาพ ระบบนี้ได้รวมคุณสมบัติที่แข็งแกร่งของเทคโนโลยีบล็อกเชนเข้ากับความสามารถทำให้เป็นอัตโนมัติของสัญญาอัจฉริยะ เพื่อปฏิวัติวิธีการจัดการความยินยอมโดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและข้อมูลที่ละเอียดอ่อนให้รับรองการปฏิบัติตามกฎหมายและกฎระเบียบความเป็นส่วนตัวของข้อมูล เช่น จีดีพีอาร์และพีดีพีเอ แนวคิดนี้ไม่เพียงแต่เป็นการเพิ่มประสิทธิภาพที่เพิ่มขึ้นเหนือแนวทางปฏิบัติในการจัดการความยินยอมแบบดั้งเดิมเท่านั้น แต่ยังเป็นการเปลี่ยนกระบวนทัศน์ นำมาซึ่งระดับความแม่นยำ ความปลอดภัย และการเพิ่มขีดความสามารถให้กับผู้ใช้ซึ่งก่อนหน้านี้ไม่สามารถบรรลุได้ด้วยเทคโนโลยีทั่วไป ดังรูปที่ 3.7 โดยสามารถอธิบายโดยละเอียดเกี่ยวกับองค์ประกอบหลักและประโยชน์ได้ดังนี้

1) แนวทางที่ซับซ้อนในการจัดการความยินยอมของผู้ใช้: ระบบนี้แสดงความก้าวหน้าที่สำคัญเหนือวิธีการจัดการความยินยอมแบบดั้งเดิมโดยการบันทึกทุกกระทำไม่ว่าจะเป็นการให้สิทธิ์ การแก้ไข หรือการเพิกถอนความยินยอมลงในกรอบงานที่ซับซ้อน การโต้ตอบของผู้ใช้แต่ละครั้งจะได้รับการบันทึกอย่างพิถีพิถันและความสมบูรณ์ของบันทึกนี้ได้รับการปกป้องอย่างเข้มงวดจากการเปลี่ยนแปลงที่ไม่ได้รับอนุญาต แนวทางนี้ไม่ใช่แค่การจัดเก็บการตั้งค่าของผู้ใช้เท่านั้นแต่เป็นเรื่องเกี่ยวกับการจัดการและบังคับใช้การตั้งค่าเหล่านี้อย่างจริงจังในลักษณะที่ปลอดภัยและเป็นอัตโนมัติ

2) ใช้ประโยชน์จากความปลอดภัยของบล็อกเชน: การใช้เทคโนโลยีบล็อกเชนช่วยให้มั่นใจได้ว่าเมื่อมีการบันทึกข้อมูลธุรกรรมความยินยอมแต่ละรายการเข้าสู่บล็อกเชน จะได้รับการรักษาความปลอดภัยผ่านเทคนิคการเข้ารหัสทำให้ข้อมูลดังกล่าวไม่เกิดการปลอมแปลงและการฉ้อโกง คุณลักษณะด้านความปลอดภัยนี้มีความสำคัญเนื่องจากจะปกป้องความสมบูรณ์ของความยินยอมที่ได้รับจากผู้ใช้และยังเพิ่มความน่าเชื่อถือระหว่างผู้ใช้และผู้ให้บริการอย่างมีนัยสำคัญ

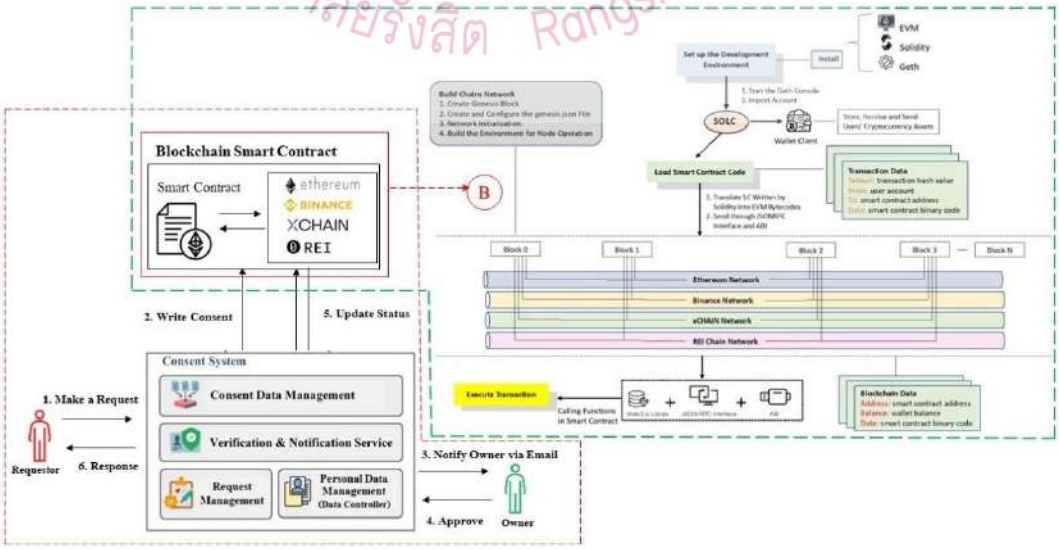
3) ใช้ประโยชน์จากความโปร่งใสของบล็อกเชน: ความโปร่งใสเป็นคุณสมบัติหลักอีกประการหนึ่งของบล็อกเชน ทุกธุรกรรมและบันทึกความยินยอมบนบล็อกเชนจะโปร่งใสและตรวจสอบได้ ซึ่งผู้ใช้และหน่วยงานกำกับดูแลสามารถติดตามและตรวจสอบความถูกต้องของการดำเนินการยินยอมได้อย่างง่ายดายและตลอดเวลาเพื่อให้มั่นใจว่ามีแนวทางที่ชัดเจนและรับผิดชอบเกี่ยวกับวิธีการใช้ข้อมูล

4) ใช้ประโยชน์จากประสิทธิภาพของสัญญาอัจฉริยะ: สัญญาอัจฉริยะทำให้การบังคับใช้และการจัดการความยินยอมเป็นไปโดยอัตโนมัติ สัญญาที่ดำเนินการด้วยตนเองมีการ

เขียนเงื่อนไขของข้อตกลงระหว่างฝ่ายต่าง ๆ ลงในรหัสโดยตรง สัญญาอัจฉริยะเหล่านี้ดำเนินการตามที่กำหนดไว้ล่วงหน้าโดยอัตโนมัติเมื่อตรงตามเงื่อนไขบางประการโดยไม่จำเป็นต้องมีคนกลาง จึงขจัดความจำเป็นในการแทรกแซงด้วยตนเอง และลดโอกาสที่จะเกิดข้อผิดพลาดของมนุษย์ ในบริบทของการจัดการความยินยอมหมายความว่าการเปลี่ยนแปลงความยินยอมของผู้ใช้จะสะท้อนให้เห็นทั่วทั้งระบบโดยอัตโนมัติ เพื่อให้มั่นใจว่าการใช้ข้อมูลจะสอดคล้องกับสถานะความยินยอมในปัจจุบันเสมอ

5) เคารพต่อการตั้งค่าและความเป็นอิสระของผู้ใช้: ระบบให้ความสำคัญอย่างมากกับการเคารพการตั้งค่าของผู้ใช้ ผู้ใช้สามารถจัดการความยินยอมของคนได้อย่างจริงจัง กำหนดเงื่อนไขในการใช้ข้อมูลของตนและสามารถแก้ไขหรือเพิกถอนความยินยอมนี้ได้อย่างง่ายดายตามต้องการและด้วยการทำให้มั่นใจว่าการตั้งค่าเหล่านี้ได้รับการปฏิบัติอย่างเคร่งครัด ระบบจะให้ความสำคัญกับความเป็นอิสระของผู้ใช้ในระดับสูง

6) ความสอดคล้องและการปฏิบัติตามกฎระเบียบด้านการคุ้มครองข้อมูล: การนำทางภูมิทัศน์ที่ซับซ้อนของกฎระเบียบด้านการปกป้องข้อมูลถือเป็นความท้าทายที่น่ากลัวสำหรับหลายองค์กร ระบบบริหารจัดการความยินยอมนี้ซึ่งมีแกนหลักเป็นบล็อกเชนและความ สามารถของสัญญาอัจฉริยะ ได้รับการออกแบบโดยธรรมชาติให้ตรงตามข้อกำหนดที่เข้มงวดของกฎหมายและกฎระเบียบ เช่น จีดีพีอาร์และพีดีพีเอ โดยให้กรอบการทำงานที่ตรวจสอบได้ ปฏิเสธไม่ได้ และเป็นไปตามข้อกำหนดสำหรับการจัดการความยินยอมของผู้ใช้ ซึ่งช่วยให้องค์กรปฏิบัติตามมาตรฐานทางกฎหมายและหลีกเลี่ยงการคว่ำบาตรที่อาจเกิดขึ้น



รูปที่ 3.7 กรอบการทำงานระบบบริหารจัดการความยินยอมเข้ากับสัญญาอัจฉริยะบนบล็อกเชน

กระบวนการการบูรณาการระบบบริหารจัดการความยินยอมเข้ากับสัญญาอัจฉริยะบนบล็อกเชน มีด้วยกัน 6 ขั้นตอน ดังรูปที่ 3.8 สามารถอธิบายรายละเอียดได้ดังต่อไปนี้

1) ขั้นตอนที่ 1 ยื่นคำร้อง: เป็นขั้นตอนแรกในกระบวนการจัดการความยินยอมภายในระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต เมื่อผู้ร้องขอทำคำขอเพื่อเข้าถึงหรือใช้ข้อมูลที่เป็นของบุคคลอื่น (เจ้าของ) มอดูลการจัดการข้อมูลคำยินยอมมีบทบาทสำคัญในกระบวน การนี้โดยการสร้างบันทึกที่มีโครงสร้าง (บล็อก) ที่จะรวบรวมรายละเอียดที่เกี่ยวข้องทั้งหมดของคำขอ ซึ่งจะช่วยอำนวยความสะดวกให้กับกระบวนการยินยอมที่มีการจัดการและตรวจสอบย้อนกลับได้ ในระบบนี้จะมีมอดูลซึ่งประกอบด้วยมอดูลที่แตกต่างกัน 4 มอดูลโดยแต่ละมอดูลทำหน้าที่เฉพาะในการจัดการข้อมูลคำยินยอม ได้แก่

1.1) มอดูลการจัดการข้อมูลคำยินยอม: มอดูลนี้มีหน้าที่รับผิดชอบในการสร้างและบำรุงรักษา บันทึกคำยินยอม เมื่อมีการเริ่มต้นการร้องขอการเข้าถึงข้อมูลหรือสิทธิ์ มอดูลนี้จะสร้างบล็อก บล็อกนี้ทำหน้าที่เป็นบันทึกภายในระบบและมีข้อมูลสำคัญหลายส่วน เช่น

(1) รหัสผู้ร้องขอ: เป็นตัวระบุที่ไม่ซ้ำกันสำหรับบุคคลหรือนิติบุคคลที่ร้องขอการเข้าถึงข้อมูล

(2) รหัสเจ้าของข้อมูล: เป็นตัวระบุที่ไม่ซ้ำกันสำหรับเจ้าของข้อมูลที่ถือสิทธิ์ในข้อมูลที่ร้องขอ

(3) รหัสความยินยอม: เป็นตัวระบุที่ไม่ซ้ำกันสำหรับธุรกรรมความยินยอม ซึ่งสามารถใช้เพื่อติดตามคำขอและการดำเนินการหรือการตอบกลับที่เกี่ยวข้อง

(4) สถานะ: สถานะปัจจุบันของคำยินยอม เช่น รอดำเนินการ อนุมัติ ปฏิเสธ หรือเพิกถอน

(5) วันที่: วันที่ที่มีการร้องขอหรือสร้างบันทึกความยินยอมหรือวันที่ที่มีการปรับปรุงสถานะ

1.2) มอดูลบริการการตรวจสอบและการแจ้งเตือน: มอดูลนี้มีแนวโน้มที่จะจัดการการตรวจสอบของฝ่ายที่เกี่ยวข้องในธุรกรรมการยินยอม และส่งการแจ้งเตือนเกี่ยวกับสถานะของคำขอความยินยอม

1.3) มอดูลการจัดการคำขอ: เป็นมอดูลที่จัดการคำขอขาเข้าและขาออกสำหรับการเข้าถึงข้อมูล เพื่อให้มั่นใจว่าคำขอเหล่านั้นได้รับการประมวลผลและตอบสนองอย่างเหมาะสม

1.4) มอดูลการจัดการข้อมูลส่วนบุคคล (ผู้ควบคุมข้อมูล): มอดูลนี้มีหน้าที่รับผิดชอบในการดูแลข้อมูลจากจุดยืนด้านกฎระเบียบและการปฏิบัติตามข้อกำหนด เพื่อให้มั่นใจว่า

การจัดการข้อมูลเป็นไปตามกฎหมายและข้อบังคับด้านการคุ้มครองข้อมูลที่เกี่ยวข้อง

2) ขั้นตอนที่ 2 บันทึกความยินยอม: ระบบบริหารจัดการความยินยอมเขียนบันทึกลงในบล็อกดังแสดงในป้ายกำกับหมายเลข 2 ตามรูปที่ 3.6 โดยผ่านกระบวนการสัญญาอัจฉริยะในขั้นตอนที่ 3 ขั้นตอนนี้ช่วยให้มั่นใจได้ว่าธุรกรรมการยินยอมไม่เพียงแต่ถูกบันทึกด้วยวิธีที่ปลอดภัยและไม่สามารถเปลี่ยนแปลงได้เท่านั้น แต่ยังช่วยให้ฝ่ายต่าง ๆ ที่เกี่ยวข้องได้รับแจ้งเกี่ยวกับธุรกรรมทันทีและเชื่อถือได้ โดยใช้ประโยชน์จากจุดแข็งของเทคโนโลยีบล็อกเชนเพื่อขอความยินยอม มีรายละเอียดของขั้นตอนนี้ดังนี้

2.1) การบันทึกความยินยอม: ระบบบริหารจัดการความยินยอมรับความยินยอมที่ได้รับจากเจ้าของข้อมูลและบันทึกลงในบล็อกเชน การดำเนินการนี้จะสร้างบันทึกธุรกรรมการยินยอมที่ไม่เปลี่ยนรูปซึ่งได้รับการอำนวยความสะดวกโดยเทคโนโลยีสัญญาอัจฉริยะ

2.2) กระบวนการสัญญาอัจฉริยะ: การใช้สัญญาอัจฉริยะถือเป็นหัวใจสำคัญ สัญญาอัจฉริยะคือสัญญาที่ดำเนินการด้วยตนเองโดยมีเงื่อนไขของข้อตกลงที่เขียนลงในชุดคำสั่งโดยตรง จะทำงานบนบล็อกเชนและเมื่อตรงตามเงื่อนไขระบบก็จะดำเนินการตามเงื่อนไขของสัญญาโดยอัตโนมัติ รวมถึงขั้นการอนุญาตการเขียนบล็อก ในบล็อกเชนโดยทั่วไปแล้วฝ่ายที่ชนะสิทธิ์ในการเพิ่มบล็อกใหม่ (ผ่านกลไกฉันทามติ) จะเป็นผู้บันทึกข้อมูล ข้อมูลความยินยอมจะถูกเขียนลงในบล็อกใหม่

2.3) ความไม่เปลี่ยนแปลงของการบันทึก: เมื่อความยินยอมถูกล็อกอินเข้าสู่บล็อกบนบล็อกเชนแล้ว จะไม่สามารถเปลี่ยนแปลงหรือแก้ไขได้ ความไม่เปลี่ยนแปลงนี้ช่วยให้แน่ใจว่าบันทึกความยินยอมมีความปลอดภัยและยังคงไม่เปลี่ยนแปลงเมื่อเวลาผ่านไป โดยให้แนวทางการตรวจสอบที่น่าเชื่อถือและตรวจสอบได้

2.4) การแจ้งเตือนการยินยอม: หลังจากบันทึกความยินยอมบนบล็อกเชนที่อยู่บล็อก (การอ้างอิงถึงตำแหน่งของบันทึกความยินยอมในบล็อกเชน) จะถูกสื่อสารไปยังเจ้าของข้อมูล การแจ้งเตือนนี้ทำได้ทั้งทางอีเมลและกระเป๋าเงินดิจิทัลของเจ้าของข้อมูล การใช้ทั้งสองวิธีทำให้มั่นใจได้ว่าเจ้าของจะได้รับแจ้งธุรกรรมอย่างเพียงพอและสามารถตรวจสอบได้โดยอิสระ

3) ขั้นตอนที่ 3 แจ้งเตือนเจ้าของผ่านทางอีเมล: เป็นการแจ้งเจ้าของข้อมูลเกี่ยวกับธุรกรรมความยินยอมผ่านทางอีเมล ขั้นตอนนี้ช่วยให้มั่นใจว่าเจ้าของข้อมูลจะได้รับแจ้งอย่างรวดเร็วและปลอดภัยเกี่ยวกับธุรกรรมที่เกี่ยวข้องกับข้อมูลของตน ซึ่งตอกย้ำหลักการความโปร่งใสและความปลอดภัยของระบบบริหารจัดการความยินยอมบนบล็อกเชนของมหาวิทยาลัยรังสิต การใช้การเข้ารหัสกุญแจสาธารณะสำหรับการสื่อสารทางอีเมลจะเพิ่มการรักษาความปลอดภัยอีกชั้นหนึ่ง ซึ่งสอดคล้องกับแนวปฏิบัติที่ดีที่สุดในการปกป้องข้อมูลและความเป็นส่วนตัว ในขั้นตอนนี้มีรายละเอียด

ดังนี้

3.1) การสร้างและการเขียนบล็อก: หลังจากสร้างบันทึกความยินยอมและเข้าสู่ระบบบล็อกเชนในขั้นตอนที่ 2 (ตามเงื่อนไขของสัญญาอัจฉริยะ) ผู้ชนะที่กำหนด (โหนดในเครือข่ายบล็อกเชนที่ได้รับสิทธิ์ในการเพิ่มบล็อกถัดไป ซึ่งมักจะผ่านกลไกฉันทามติ) เขียนบล็อกนี้ลงในบล็อกเชนอย่างเป็นทางการ บล็อกนี้มีรายละเอียดธุรกรรมที่เกี่ยวข้องกับความยินยอมที่ได้รับจากเจ้าของข้อมูล

3.2) การลงทะเบียนผู้ควบคุมข้อมูลล่วงหน้า: ก่อนการดำเนินการเหล่านี้ หน่วยงานทั้งหมดที่จะทำหน้าที่เป็นผู้ควบคุมข้อมูล (เจ้าหน้าที่ของมหาวิทยาลัย) จำเป็นต้องลงทะเบียนล่วงหน้าบนระบบบล็อกเชน ส่วนหนึ่งของขั้นตอนการลงทะเบียนนี้เกี่ยวข้องกับสร้างกระเป๋าเงินดิจิทัล ซึ่งทำหน้าที่เป็นข้อมูลประจำตัวและบัญชีบนบล็อกเชน กระเป๋าเงินดิจิทัลนี้สามารถรับและส่งธุรกรรมและเป็นส่วนสำคัญในการโต้ตอบกับบล็อกเชน

3.3) การแจ้งเตือนธุรกรรมการยินยอม: เมื่อเพิ่มบล็อกลงในบล็อกเชนเรียบร้อยแล้ว ระบบบริหารจัดการความยินยอมจะดำเนินการขั้นตอนถัดไปเพื่อแจ้งให้เจ้าของข้อมูลทราบเกี่ยวกับธุรกรรมนี้ สิ่งนี้ทำเพื่อให้แน่ใจว่าเจ้าของข้อมูลตระหนักถึงการใช้ข้อมูลของตนและรักษาความโปร่งใสในกระบวนการจัดการข้อมูล

3.4) การสื่อสารทางอีเมลที่ปลอดภัยผ่านการเข้ารหัสกุญแจสาธารณะ: การแจ้งเตือนไปยังเจ้าของข้อมูลจะถูกส่งทางอีเมลเพื่อให้มั่นใจในความปลอดภัยและการรักษาความลับของการสื่อสารนี้ อีเมลจะถูกเข้ารหัสโดยใช้การเข้ารหัสกุญแจสาธารณะ วิธีการเข้ารหัสนี้ช่วยให้แน่ใจว่าเฉพาะผู้รับที่ต้องการซึ่งมีกุญแจส่วนตัวที่เกี่ยวข้องเท่านั้นที่สามารถถอดรหัสและอ่านเนื้อหาของอีเมลได้ แนวปฏิบัตินี้จะปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตระหว่างการส่ง

4) ขั้นตอนที่ 4 อนุมัติโดยเจ้าของข้อมูล: เป็นการดำเนินการอนุมัติที่ดำเนินการโดยเจ้าของข้อมูล (บุคคลที่ข้อมูลกำลังถูกประมวลผล) ขั้นตอนนี้เป็นเรื่องเกี่ยวกับการเพิ่มขีดความสามารถของเจ้าของข้อมูลด้วยสิทธิ์เฉพาะและความสามารถในการใช้สิทธิ์เหล่านั้นผ่านการโต้ตอบกับระบบบล็อกเชน ขั้นตอนนี้เน้นย้ำถึงความมุ่งมั่นของระบบในการส่งเสริมสิทธิ์ของเจ้าของข้อมูลตามที่บัญญัติไว้ในกฎระเบียบการปกป้องข้อมูล เช่น จีดีพีอาร์และพีดีพีเอ ด้วยการทำให้เจ้าของข้อมูลสามารถอนุมัติหรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนได้อย่างเต็มที่ และรับรองว่าการกระทำเหล่านี้จะถูกบันทึกไว้ในบล็อกเชนอย่างไม่เปลี่ยนแปลง ระบบจะเพิ่มความโปร่งใส ความรับผิดชอบและการควบคุมข้อมูลส่วนบุคคล ในขั้นตอนนี้มีรายละเอียดดังนี้

4.1) การอนุมัติโดยเจ้าของข้อมูล: ในขั้นตอนนี้เจ้าของข้อมูลจะอนุมัติหรือตอบสนองต่อคำขอที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของตนอย่างจริงจิง การอนุมัตินี้ได้รับการลง

ทะเบียนโดยการปรับปรุงตัวบ่งชี้เฉพาะในบล็อกเชน จึงจะระบุถึงการตัดสินใจของเจ้าของข้อมูล การปรับปรุงส่งผลให้มีการสร้างบล็อกใหม่เพื่อให้แน่ใจว่าการดำเนินการจะถูกบันทึกอย่างไม่เปลี่ยนแปลงบนบล็อกเชน

4.2) ประเภทของสิทธิ์: ระบบจะจดจำสิทธิ์ทั้งสามประเภทที่เจ้าของข้อมูลสามารถใช้ได้ ได้แก่

(1) ประเภทที่ 1 สิทธิ์ในการได้รับแจ้ง: สิทธิ์นี้ทำให้เจ้าของข้อมูลทราบถึงวิธีการใช้ข้อมูลของตน เมื่อเจ้าของข้อมูลใช้สิทธิ์นี้ อาจเกี่ยวข้องกับการรับข้อมูลโดยละเอียดเกี่ยวกับกิจกรรมการประมวลผลข้อมูล

(2) ประเภทที่ 2 สิทธิ์ที่จะถูกลืม (การลบข้อมูล): ช่วยให้เจ้าของข้อมูลสามารถขอลบข้อมูลส่วนบุคคลของตนออกจากระบบได้ เป็นส่วนสำคัญของกฎระเบียบความเป็นส่วนตัวของข้อมูล ซึ่งช่วยให้บุคคลสามารถควบคุมการปล่อยข้อมูลของคนได้

(3) ประเภทที่ 3 สิทธิ์ในการคัดค้าน: สิทธิ์นี้อนุญาตให้บุคคลคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนภายใต้เงื่อนไขบางประการภายใต้จีดีพีอาร์และพีดีพีเอ เจ้าของข้อมูลจะได้รับสิทธิ์ในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนในสถานการณ์เฉพาะ (Bernabe, Canovas, Hernandez-Ramos, Moreno, & Skarmeta, 2019, pp.164916) ดังนี้

(3.1) หากข้อมูลส่วนบุคลได้รับการประมวลผลโดยไม่ได้รับความยินยอมและเชื่อมโยงกับกิจกรรมเพื่อประโยชน์สาธารณะหรือเป็นประโยชน์โดยชอบด้วยกฎหมาย บุคคลมีสิทธิ์ที่จะคัดค้าน

(3.2) เจ้าของข้อมูลสามารถคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนได้เมื่อใช้เพื่อวัตถุประสงค์ทางการตลาดโดยตรง

(3.3) เมื่อข้อมูลส่วนบุคคลถูกนำมาใช้เพื่อวัตถุประสงค์ทางสถิติ ประวัติศาสตร์ หรือการวิจัยทางวิทยาศาสตร์ เจ้าของข้อมูลจะรักษาสิทธิ์ในการคัดค้าน

คำขอโดยตรงไปยังผู้ควบคุมข้อมูลประเภทที่ 3 การร้องขอจะถูกส่งไปยังผู้ควบคุมข้อมูลโดยตรงโดยไม่ผ่านขั้นตอนที่ 3 (แจ้งเตือนเจ้าของผ่านทางอีเมล) และขั้นตอนที่ 4 (อนุมัติโดยเจ้าของข้อมูล) วิธีการโดยตรงนี้ช่วยปรับปรุงกระบวนการคัดค้านทำให้มั่นใจ ได้ว่าเจ้าของข้อมูลสามารถใช้สิทธิ์ในการคัดค้านได้อย่างมีประสิทธิภาพ

5) ขั้นตอนที่ 5 ปรับปรุงสถานะบนบล็อกเชน: ขั้นตอนนี้ย้ำถึงความรับผิดชอบของระบบการควบคุมข้อมูลส่วนบุคคลของตนโดยเจ้าของข้อมูล โดยทำให้แน่ใจว่าแต่ละการกระทำและสถานะผลลัพธ์นั้นได้รับการบันทึกอย่างไม่เปลี่ยนแปลงบนบล็อกเชน ระบบจะให้แนวทางการ

ตรวจสอบที่เชื่อถือได้ และเพิ่มความไว้วางใจในกระบวนการจัดการข้อมูล ในขั้นตอนนี้มีรายละเอียดดังนี้

5.1) การสร้างบล็อกใหม่พร้อมสถานะที่ปรับปรุง: หลังจากการอนุมัติหรือการตัดสินใจของเจ้าของข้อมูลในขั้นตอนก่อนหน้า ระบบจะต้องสนองโดยการสร้างบล็อกใหม่ บล็อกนี้ไม่ได้เป็นเพียงบันทึกธุรกรรมเท่านั้น แต่ยังรวมถึงสถานะที่ปรับปรุงซึ่งสะท้อนถึงการตัดสินใจของเจ้าของข้อมูลด้วย ตัวอย่างเช่น หากเจ้าของข้อมูลใช้สิทธิ์ที่จะถูกลืม การปรับปรุงสถานะ อาจสะท้อนถึงการลบหรือทำให้ข้อมูลส่วนบุคคลของพวกเขาเป็นนิรนาม

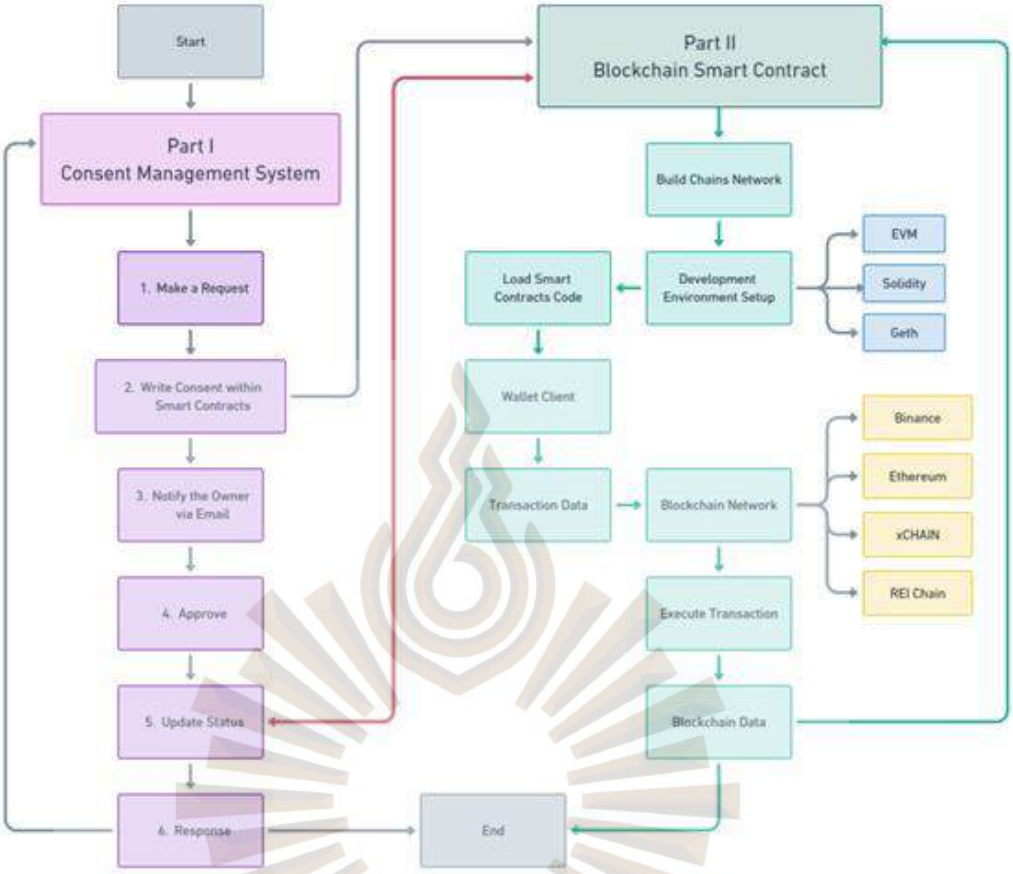
5.2) การเขียนบล็อกใหม่ไปยังบล็อกเชน: บล็อกใหม่นี้ซึ่งมีสถานะปรับปรุงจะถูกเพิ่มลงในบล็อกเชน กระบวนการเพิ่มบล็อกเป็นไปตามกลไกฉันทามติของบล็อกเชนเพื่อให้แน่ใจว่าการปรับปรุงได้รับการอนุมัติจากผู้เข้าร่วมในเครือข่ายและได้รับการบันทึกอย่างปลอดภัย

5.3) ประวัติการติดตาม: ประโยชน์ที่สำคัญอย่างหนึ่งของขั้นตอนนี้และการใช้เทคโนโลยีบล็อกเชนโดยทั่วไป คือความสามารถในการรักษาประวัติการทำธุรกรรมที่ชัดเจนและไม่เปลี่ยนรูปทุกการกระทำที่ทำโดยเจ้าของข้อมูล และทุกการตอบสนองโดยระบบจะถูกบันทึกเป็นบล็อกในบล็อกเชน นี่เป็นบัญชีแยกประเภทที่โปร่งใสและป้องกันการงัดแงะของการโต้ตอบและการปรับปรุงสถานะทั้งหมดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล

6) ขั้นตอนที่ 6 การตอบสนอง: การดำเนินการตอบสนองที่ดำเนินการโดยผู้ควบคุมข้อมูลตามสิทธิ์ที่ได้รับจากเจ้าของข้อมูล ขั้นตอนนี้เน้นความรับผิดชอบของผู้ควบคุมข้อมูลในการดำเนินการตามการตัดสินใจจากเจ้าของข้อมูลเกี่ยวกับข้อมูลส่วนบุคคลของตน ช่วยให้มั่นใจได้ว่ากระบวนการจัดการข้อมูลไม่ได้เป็นเพียงการบันทึกความยินยอมและการตัดสินใจเท่านั้น แต่ยังรวมถึงการดำเนินการตัดสินใจเหล่านี้ให้เป็นจริงด้วย ดังนั้นจึงสนับสนุนหลักการของการปกป้องข้อมูลและสิทธิ์ของบุคคลในข้อมูลส่วนบุคคลของพวกเขา บทบาทของบล็อกเชนในการจัดหาบันทึกที่โปร่งใส และไม่เปลี่ยนรูปทำให้มั่นใจได้ว่าการกระทำของผู้ควบคุมข้อมูลมีความรับผิดชอบและตรวจสอบย้อนกลับได้ ในขั้นตอนนี้มีรายละเอียดดังนี้

6.1) การดำเนินการของผู้ควบคุมข้อมูลตามการอนุญาต: หลังจากที่เจ้าของข้อมูลตัดสินใจแล้ว (เช่น การอนุมัติคำขอการใช้สิทธิ์ที่จะถูกลืมหรือการคัดค้านการประมวลผลข้อมูล) ผู้ควบคุมข้อมูล (หน่วยงานที่รับผิดชอบในการจัดการข้อมูล) ได้รับข้อมูลนี้ ผู้ควบคุมข้อมูลมีหน้าที่รับผิดชอบในการตอบสนองต่อคำขอในลักษณะที่สอดคล้องกับสิทธิ์ที่ได้รับจากเจ้าของข้อมูล

6.2) การปฏิบัติตามความยินยอมของเจ้าของข้อมูล: ผู้ควบคุมข้อมูลจะต้องดำเนินการตามความยินยอมที่ได้รับจากเจ้าของข้อมูล ซึ่งหมายความว่าการดำเนินการควรสะท้อนถึงการตัดสินใจและสิทธิ์ของเจ้าของข้อมูลตามที่บันทึกไว้และปรับปรุงในบล็อกเชน



รูปที่ 3.8 กระบวนการการบูรณาการระบบบริหารจัดการความยินยอมเข้ากับสัญญาอัจฉริยะบนบล็อกเชน

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.1 ความแตกต่างระหว่าง “ระบบการจัดการความยินยอมที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชน” และ “ระบบการจัดการความยินยอมแบบดั้งเดิม”

ความแตกต่าง	ระบบการจัดการความยินยอมที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชน	ระบบการจัดการความยินยอมแบบดั้งเดิม
1. โครงสร้างพื้นฐานทางเทคโนโลยี	ใช้เทคโนโลยีบล็อกเชนซึ่งกระจายข้อมูลผ่านเครือข่าย เพิ่มความปลอดภัยและลดความเสี่ยงของการละเมิดข้อมูลแบบรวมศูนย์ สัญญาอัจฉริยะทำให้กระบวนการที่เกี่ยวข้องกับความยินยอมเป็นไปโดยอัตโนมัติ	โดยทั่วไปจะรวมศูนย์และจัดการโดยองค์กรที่รวบรวมความยินยอมอาจใช้ฐานข้อมูลแบบดั้งเดิมเพื่อจัดเก็บบันทึกความยินยอม
2. ความโปร่งใสและไม่เปลี่ยนรูป	มีความโปร่งใสสูงและไม่เปลี่ยนรูป การดำเนินการยินยอมทุกครั้งจะถูกบันทึกไว้ในบล็อกเชนทำให้เกิดประวัติที่ถาวรและไม่เปลี่ยนแปลง ทำให้การตรวจสอบตรงไปตรงมาและเชื่อถือได้	ความโปร่งใสขึ้นอยู่กับนโยบายขององค์กร บันทึกอาจมีการเปลี่ยนแปลงได้ และเส้นทางการตรวจสอบอาจไม่มีประสิทธิภาพ
3. ความปลอดภัย	เสนอคุณสมบัติความปลอดภัยขั้นสูง ลักษณะการกระจายศูนย์ของบล็อกเชน และการป้องกันการเข้ารหัสช่วยลดความเสี่ยงของการเข้าถึงโดยไม่ได้รับอนุญาตและการดัดแปลงข้อมูลได้	การรักษาความปลอดภัยขึ้นอยู่กับโครงสร้างพื้นฐานขององค์กร อาจมีช่องโหว่ที่เกี่ยวข้องกับการรวมศูนย์และความเป็นไปได้ที่จะมีการปลอมแปลงภายใน
4. ระบบอัตโนมัติและประสิทธิภาพ	ใช้สัญญาอัจฉริยะสำหรับการตรวจสอบและการบังคับใช้ความยินยอมโดยอัตโนมัติ ลดการแทรกแซงด้วยตนเอง ลดข้อผิดพลาดและรับรองว่าการตั้งค่าความยินยอมได้รับการเคารพแบบตามเวลาจริง	กระบวนการอาจเป็นแบบกึ่งอัตโนมัติหรือแบบแมนนวล ซึ่งอาจส่งผลให้เวลาตอบสนองช้าลงและโอกาสที่จะเกิดข้อผิดพลาดจากมนุษย์สูงขึ้น

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.1 ความแตกต่างระหว่าง “ระบบการจัดการความยินยอมที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชน” และ “ระบบการจัดการความยินยอมแบบดั้งเดิม” (ต่อ)

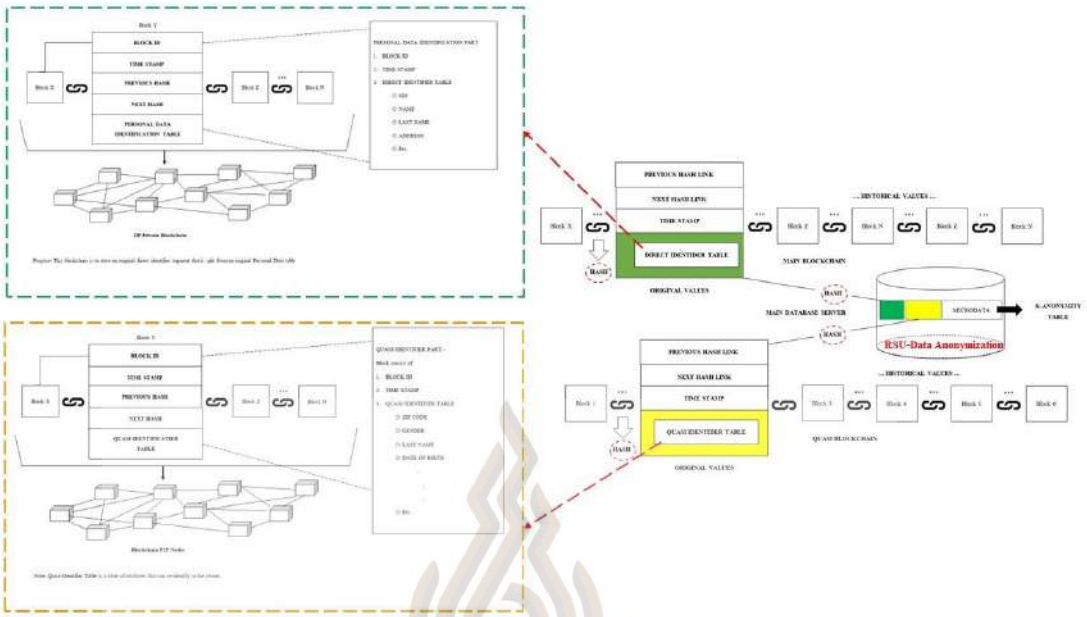
ความแตกต่าง	ระบบการจัดการความยินยอมที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชน	ระบบการจัดการความยินยอมแบบดั้งเดิม
5. การปฏิบัติตามและการรับประกันตามกฎข้อบังคับ	ธรรมชาติไม่เปลี่ยนรูปและโปร่งใสของบล็อกเชน ช่วยลดความยุ่งยากในการปฏิบัติตามกฎระเบียบการปกป้องข้อมูล เส้นทางการตรวจสอบที่ชัดเจนแสดงให้เห็นว่าความยินยอมได้รับการจัดการตามมาตรฐานทางกฎหมาย	องค์กรเป็นผู้จัดการการปฏิบัติตามกฎระเบียบและการพิสูจน์การปฏิบัติตามข้อกำหนดอาจเป็นเรื่องที่ท้าทาย โดยเฉพาะอย่างยิ่งหากบันทึกไม่ได้รับการดูแลอย่างดีหรือสามารถเปลี่ยนแปลงได้
6. การควบคุมและความน่าเชื่อถือของผู้ใช้	มอบอำนาจให้ผู้ใช้โดยให้พวกเขาควบคุมการตั้งค่าความยินยอมได้มากขึ้น และรับประกันว่าการตั้งค่าเหล่า นี้จะถูกบังคับใช้อย่างเคร่งครัด ด้วยคุณสมบัติความโปร่งใสและความปลอดภัยของระบบช่วยเพิ่มความไว้ วางใจของผู้ใช้	ผู้ใช้พึ่งพาองค์กรในการเคารพการตั้งค่าความยินยอมของตน ความน่าเชื่อถือขึ้นอยู่กับชื่อเสียงและแนวปฏิบัติขององค์กร

มหาวิทยาลัยรังสิต Rangsit University

3.2.3.2 การใช้เทคนิคการแฝงข้อมูลโดยการทดลองร่วมกับโครงการนำร่องที่ชื่อว่า RSU-Data-Anonymization โดยใช้เทคนิค k-anonymity:

โครงการนำร่องการทำข้อมูลให้เป็นนิรนามของมหาวิทยารังสิต (RSU-Data-Anonymization Pilot Project) มหาวิทยาลัยรังสิตได้ริเริ่มที่จะเปิดตัวโครงการนำร่องนี้ ความรับผิดชอบในการปกป้องข้อมูลส่วนบุคคลของนิสิตนักศึกษาทั้งหมดเป็นของศูนย์บริการเทคโนโลยีสารสนเทศ (ITSC) ซึ่งเป็นหน่วยงานในสังกัดมหาวิทยาลัยรังสิต อย่างไรก็ตามปัจจุบันไม่มีแพลตฟอร์มหรือระบบที่ได้มาตรฐานในตลาดที่สามารถตอบสนองข้อกำหนดนี้ได้อย่างเพียงพอ ดังนั้นโครงการนำร่องนี้จึงมีวัตถุประสงค์เพื่อสำรวจเทคนิคสำคัญสองประการ ได้แก่ การใช้การแฝงข้อมูล และ k-Anonymity ที่จะนำไปใช้ในการทำให้ข้อมูลเป็นนิรนาม

งานวิจัยฉบับนี้ใช้แนวคิดพื้นฐานสองแนวคิดภายในกระบวนการทำให้เป็นนิรนามซึ่งสอดคล้องกับมาตรฐานการปฏิบัติตามจีดีพีอาร์ แนวคิดแรกเกี่ยวข้องกับการทำให้เป็นลักษณะทั่วไปโดยที่อัลกอริทึม k-Anonymity จะสร้างแนวคิดการทำให้เป็นลักษณะทั่วไปที่มุ่งขยายขอบเขตบางอย่าง เช่น อายุ 16 ปี อาจสรุปเป็นช่วงอายุ 15-20 ปี แนวคิดนี้เรียกว่า “การซ่อนตัวอยู่ในฝูงชน” โดย Sweeny (2002) ซึ่งช่วยเพิ่มความเป็นส่วนตัว แนวคิดที่สองคือการใช้การแฝงข้อมูล ซึ่งเป็นส่วนเสริมล่าสุดของจีดีพีอาร์ ได้รับการออกแบบมาเพื่อบรรเทาผลกระทบจากการสูญเสียข้อมูลด้วยการใช้เทคนิคทำให้เป็นลักษณะทั่วไปและเทคนิคการแฝงข้อมูล ข้อเสียเปรียบที่เกี่ยวข้องกับอัลกอริทึม k-Anonymity อยู่ที่การสูญเสียอรรถประโยชน์ข้อมูล เมื่อใดก็ตามที่ตัวระบุเสมือนบางตัวได้รับการทำให้เป็นลักษณะทั่วไป อรรถประโยชน์ข้อมูลก็จะลดลงอย่างหลีกเลี่ยงไม่ได้ ปรากฏการณ์นี้แสดงถึงสถานการณ์การแลกเปลี่ยน เพื่อจัดการกับความท้าทายนี้ การใช้การแฝงข้อมูลจึงกลายเป็นวิธีการแก้ปัญหาที่แนะนำซึ่งได้รับการรับรองโดยจีดีพีอาร์ แนวทางที่เป็นนวัตกรรมของผู้วิจัยเกี่ยวข้องกับการใช้ประโยชน์จากเทคโนโลยีบล็อกเชนเพื่อสร้างการเชื่อมต่อระหว่าง k-Anonymity และการแฝงข้อมูล วิธีการของผู้วิจัยมุ่งหวังที่จะได้รับประโยชน์จากทั้งสองแนวทาง ในขณะเดียวกันก็บรรเทาความกังวลเรื่องข้อมูลสูญหายบางส่วนด้วย ในเทคโนโลยีบล็อกเชนนั้น ฟังก์ชันแฮชทำหน้าที่เป็นจุดเชื่อมต่อระหว่างโหนด คุณลักษณะนี้พิสูจน์ว่ามีประโยชน์สำหรับ k-Anonymity เนื่องจากที่อยู่ แฮชสามารถทำหน้าที่เป็นลิงก์ที่เชื่อมโยงฐานข้อมูลด้านหน้าและด้านหลังไฟร์วออล์ นอกจากนี้ยังสามารถใช้เป็นกุญแจหลักสำหรับแต่ละบันทึกภายในฐานข้อมูลได้อีกด้วย เมื่อผู้ควบคุมข้อมูลจำเป็นต้องสร้างบันทึกเหล่านี้ขึ้นใหม่ ที่อยู่แฮชของบล็อกเชนสามารถใช้เพื่อรวบข้อมูลเหล่านี้เข้าด้วยกันได้อย่างราบรื่น



รูปที่ 3.9 กระบวนการใช้เทคนิคการแฝงข้อมูลโดยการทดลองร่วมกับโครงการนำร่อง ที่ชื่อว่า RSU-Data-Anonymization โดยใช้เทคนิค k-anonymity

จากรูปที่ 3.9 แสดงภาพรวมที่ครอบคลุมเกี่ยวกับวิธีการรวมเทคนิคการทำข้อมูลให้เป็นนิรนามและการใช้การแฝงข้อมูลเข้ากับเทคโนโลยีบล็อกเชนเพื่อรักษาความปลอดภัยข้อมูลที่ละเอียดอ่อนอย่างมีประสิทธิภาพ มันแสดงให้เห็นถึงการใช้ฟังก์ชันแฮชและโครงสร้างที่ไม่เปลี่ยนรูปของบล็อกเชนเพื่อรับรองความเป็นส่วนตัว ความสมบูรณ์และความปลอดภัยของข้อมูล ด้วยการใช้ประโยชน์จากอัลกอริทึมการเข้ารหัส เช่น SHA-256 ระบบจะแปลงข้อมูลที่ละเอียดอ่อนเป็นรูปแบบข้อมูลแฝงหรือข้อมูลนิรนาม ทำให้ไม่สามารถย้อนกลับได้และทนทานต่อการเข้าถึงโดยไม่ได้รับอนุญาต เทคโนโลยีบล็อกเชนช่วยปรับปรุงกระบวนการนี้ให้ดียิ่งขึ้นโดยนำเสนอการกระจายอำนาจ ความไม่เปลี่ยนรูป และความโปร่งใส เมื่อข้อมูลถูกบันทึกบนบล็อกเชนแล้ว จะไม่สามารถเปลี่ยนแปลงหรือแก้ไขได้ ซึ่งเป็นรากฐานที่แข็งแกร่งสำหรับการรักษาความปลอดภัย การจัดการความยินยอม บันทึกธุรกรรม และการดำเนินการที่สำคัญอื่น ๆ การรวมกันนี้ช่วยให้องค์การสามารถปกป้องข้อมูลที่ละเอียดอ่อนในขณะที่ยังความสามารถในการใช้งานสำหรับการวิเคราะห์ การวิจัย และการตัดสินใจ นอกจากนี้ยังรับประกันการปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัว เช่น จีดีพีอาร์ และพีดีพีเอ โดยการลดความเสี่ยงของการระบุตัวตนซ้ำและการเปิดเผยโดยไม่ได้รับอนุญาต แนวทางดังกล่าวทำให้เกิดความสมดุลระหว่างการรักษาความเป็นส่วนตัวและประสิทธิภาพในการดำเนินงาน จากกรอบการทำงานนี้มีแนวคิดหลักที่เน้นองค์ประกอบที่สำคัญ 2 ประการเพื่อให้มั่นใจถึงความปลอดภัยของข้อมูลและความเป็นส่วนตัว ดังนี้

1) เทคนิคการทำให้เป็นนิรนามและการใช้การแฝงข้อมูล: ข้อมูลที่ละเอียดอ่อนได้รับการเปลี่ยนแปลงโดยใช้เทคนิคต่าง ๆ เช่น การใช้การแฝงข้อมูลและการทำให้เป็นนิรนาม ตัวอย่างเช่น ข้อมูลที่สามารถระบุตัวตนได้ เช่น ชื่อ หมายเลขประกันสังคม หรือที่อยู่ จะถูกแทนที่ด้วยข้อมูลแฝงหรือค่าแฮช กระบวนการนี้ปกป้องความเป็นส่วนตัวโดยป้องกันการเชื่อมโยงข้อมูลโดยตรงไปยังบุคคลใดบุคคลหนึ่งโดยเฉพาะ ซึ่งช่วยลดความเสี่ยงในการระบุตัวตนซ้ำอีกครั้ง เทคนิคเหล่านี้ยังคงรักษาประโยชน์ใช้สอยข้อมูล ทำให้สามารถใช้ชุดข้อมูลนิรนามเพื่อการวิเคราะห์ การตัดสินใจ หรือการปฏิบัติตามกฎหมายความเป็นส่วนตัว

2) บูรณาการกับเทคโนโลยีบล็อกเชน: ข้อมูลที่ประมวลผลจะถูกจัดเก็บไว้ในเครือข่ายบล็อกเชน ซึ่งเพิ่มความปลอดภัยผ่านความไม่เปลี่ยนรูปและความโปร่งใสโดยธรรมชาติ บล็อกเชนช่วยให้แน่ใจว่าข้อมูลเมื่อบันทึกแล้วจะไม่ถูกแก้ไขหรือเปลี่ยนแปลง ซึ่งเป็นกลไกที่แข็งแกร่งสำหรับการจัดเก็บข้อมูลที่ปลอดภัยและตรวจสอบย้อนกลับได้ การบูรณาการนี้ใช้ประโยชน์จากคุณสมบัติการเข้ารหัสของบล็อกเชนเพื่อรักษาความสมบูรณ์ของข้อมูลในขณะเดียวกันก็เปิดใช้งานการจัดการข้อมูลแบบกระจายอำนาจ ตรวจสอบได้และเป็นไปตามกฎหมายความเป็นส่วนตัว

การวิเคราะห์เปรียบเทียบเทียบ “การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน” และ “การใช้การแฝงข้อมูลแบบดั้งเดิม” โดยเฉพาะอย่างยิ่งในบริบทของการปฏิบัติกฎหมายและกฎระเบียบการปกป้องข้อมูล เช่น จีดีพีอาร์ และ พีดีพีเอ

1) ด้านความปลอดภัย: การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน สามารถให้ความปลอดภัยที่สูงขึ้นเนื่องจากมีบันทึกธุรกรรมการยินยอมที่ไม่เปลี่ยนรูป แต่ในแง่ของความยืดหยุ่นและปัญหาการปฏิบัติตามจีดีพีอาร์ที่อาจมีผลกระทบเกิดขึ้น

2) ด้านความยืดหยุ่น: การใช้การแฝงข้อมูลแบบดั้งเดิมมีความยืดหยุ่นมากกว่า เนื่องจากช่วยให้ปฏิบัติตามสิทธิ์จีดีพีอาร์ได้ง่ายกว่า เช่น การแก้ไขและการลบข้อมูล

3) ด้านต้นทุนและความซับซ้อน: การใช้การแฝงข้อมูลแบบดั้งเดิมโดยทั่วไปมีต้นทุนและความซับซ้อนที่น้อยกว่าในการดำเนินการ ในขณะที่โซลูชันที่ใช้ฟังก์ชันแฮชบนบล็อกเชน ต้องการการลงทุนด้านเทคโนโลยีและความเชี่ยวชาญมากขึ้น

4) ด้านความท้าทายในการปฏิบัติตามข้อกำหนด: การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชนนำเสนอความท้าทายที่ไม่เหมือนใครสำหรับการปฏิบัติตามจีดีพีอาร์ โดยเฉพาะอย่างยิ่งเกี่ยวกับสิทธิ์ของเจ้าของข้อมูลในการลบและการเคลื่อนย้ายข้อมูล

ตารางที่ 3.2 ความแตกต่างระหว่าง “การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน” และ “การใช้การแฝงข้อมูลแบบดั้งเดิม” โดยเฉพาะอย่างยิ่งในบริบทของการปฏิบัติตามจีดีพีอาร์

ความแตกต่าง	การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน	การใช้การแฝงข้อมูลแบบดั้งเดิม
1.คำจำกัดความ	ใช้เทคโนโลยีบล็อกเชนเพื่อเพิ่มความปลอดภัยของกระบวนการใช้การแฝงข้อมูล ข้อมูลเพิ่มเติมสำหรับการระบุตัวตนซ้ำอีกครั้งได้รับการจัดการภายในโครงสร้างพื้นฐานบล็อกเชน	การใช้การแฝงข้อมูลเป็นกระบวนที่ข้อมูลส่วนบุคคลถูกแปลงหากไม่มีข้อมูลเพิ่มเติมข้อมูลดังกล่าวจะไม่สามารถระบุแหล่งที่มาของข้อมูลเฉพาะได้
2.การย้อนกลับได้	แม้ว่าการใช้การแฝงข้อมูลจะสามารถย้อนกลับได้ แต่บล็อกเชนที่ไม่สามารถเปลี่ยนรูปสามารถทำให้การจัดการย้อนกลับนี้ซับ ซ้อนได้	สามารถย้อนกลับได้หากมีการให้ข้อมูลเพิ่มเติม (เก็บไว้แยกต่างหากและปลอดภัย) เพื่อให้สามารถระบุตัวตนของเจ้าของข้อมูลได้อีกครั้ง
3.การปฏิบัติตามจีดีพีอาร์	อาจให้การรักษาความปลอดภัยที่แข็งแกร่งยิ่งขึ้น เนื่องจากธรรมชาติของบล็อกเชนที่ไม่เปลี่ยนแปลงและการกระจาย แต่ก่อให้เกิดความท้าทายสำหรับการปฏิบัติตามจีดีพีอาร์ โดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับสิทธิ์ในการลบหรือการเคลื่อนย้ายข้อมูล	ได้รับการยอมรับภายใต้จีดีพีอาร์ว่าเป็นวิธีการในการปกป้องข้อมูลส่วนบุคคลและลดความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูล สามารถช่วยในการปฏิบัติตามพันธกรณีของจีดีพีอาร์ แต่ในตัวมันเองไม่ได้รับประกันการปฏิบัติตามข้อกำหนด
4.สิทธิ์ในข้อมูล	คุณลักษณะที่ไม่เปลี่ยนรูปของบล็อกเชนอาจขัดแย้งกับสิทธิ์จีดีพีอาร์ เช่น สิทธิ์ในการลบ (สิทธิ์ที่จะถูกลืม) เนื่องจากข้อมูลบนบล็อกเชนไม่สามารถเปลี่ยนแปลงได้เมื่อบันทึกแล้ว	เข้ากันได้กับสิทธิ์จีดีพีอาร์ สิทธิ์ในการจำกัดการประมวลผลเนื่องจากข้อมูลที่ใช้การแฝงข้อมูลสามารถแก้ไขหรือลบได้

ตารางที่ 3.2 ความแตกต่างระหว่าง “การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน” และ “การใช้การแฝงข้อมูลแบบดั้งเดิม” โดยเฉพาะอย่างยิ่งในบริบทของการปฏิบัติตามจีดีพีอาร์ (ต่อ)

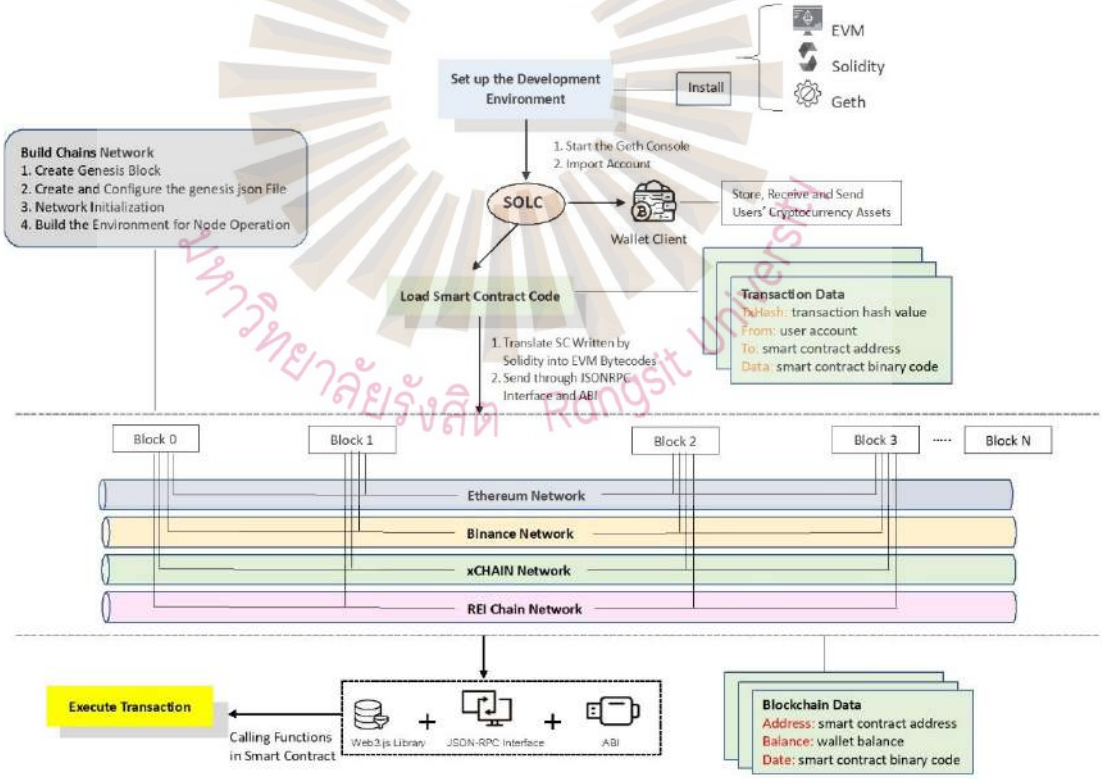
ความแตกต่าง	การใช้การแฝงข้อมูลที่บูรณาการกับฟังก์ชันแฮชบนบล็อกเชน	การใช้การแฝงข้อมูลแบบดั้งเดิม
5.การนำไปปฏิบัติ	มีความซับซ้อนมากขึ้นและอาจมีค่าใช้จ่ายสูงกว่าในการดำเนินการโดยเฉพาะในส่วนของค่าธรรมเนียมการทำธุรกรรมและค่าก๊าซ เนื่องจากความต้องการโครงสร้างพื้นฐานบล็อกเชน อาจต้องมีการเปลี่ยนแปลงที่สำคัญต่อระบบและกระบวนการที่มีอยู่	โดยทั่วไปจะง่ายกว่าและมีค่าใช้จ่ายน้อยกว่าเมื่อเทียบกับโซลูชันบล็อกเชน สามารถรวมเข้ากับระบบการจัด การข้อมูลที่มีอยู่ได้โดยไม่จำเป็นต้องใช้เทคโนโลยีบัญชีแยกประเภทแบบกระจาย
6.กรณีการใช้งาน	อาจเหมาะสมกับสถานการณ์ที่ความสมบูรณ์และการเปลี่ยนแปลงไม่ได้ของบันทึกความยินยอมเป็นสิ่งสำคัญยิ่ง และน้อยกว่าเมื่อสิทธิ์ของเจ้าของข้อมูลจำเป็นต้องมีการเปลี่ยนแปลงหรือการลบข้อมูล	เหมาะสำหรับการใช้งานที่หลากหลาย โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลอาจจำเป็นต้องได้รับการระบุอีกครั้งเพื่อวัตถุประสงค์ที่ถูกต้องตามกฎหมาย

มหาวิทยาลัยรังสิต Rangsit University

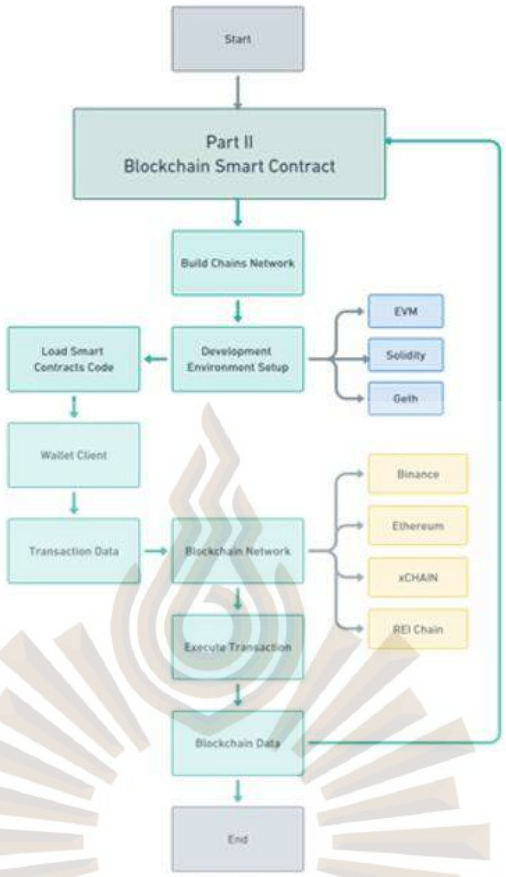
3.3 การตั้งค่าการทดลอง

3.3.1 การทดลองที่ 1: การใช้สัญญาอัจฉริยะบนบล็อกเชนร่วมกับระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS)

กระบวนการพัฒนาและการปรับใช้สัญญาอัจฉริยะภายในเทคโนโลยีบล็อกเชน ที่เขียนด้วยภาษาซอลอริตี ซึ่งเป็นภาษาโปรแกรมที่ออกแบบมาโดยเฉพาะสำหรับการสร้างสัญญาอัจฉริยะบนบล็อกเชน กระบวนการนี้เป็นกระบวนการที่เกี่ยวกับการสร้างเครือข่ายบล็อกเชน และวิธีการสร้าง ปรับใช้ และโต้ตอบกับสัญญาอัจฉริยะบนเครือข่ายบล็อกเชน โดยผู้วิจัยเน้นไปที่แพลตฟอร์มอีเธอเรียม (Ethereum) ให้เป็นแพลตฟอร์มตั้งต้นในการตั้งค่าสภาพแวดล้อมการพัฒนา นอกจากนี้ยังรวมถึงแพลตฟอร์มบล็อกเชนอื่นๆ เช่น ไบแนนซ์ (Binance) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain) กระบวนการต่าง ๆ ที่แสดงในรูปที่ 3.10 รูปที่ 3.11 และรูปที่ 3.12



รูปที่ 3.10 แผนผังกระบวนการทำงานของสัญญาอัจฉริยะบนบล็อกเชน



รูปที่ 3.11 กระบวนการทำงานของสัญญาอัจฉริยะบนบล็อกเชน

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.15;

contract Demo{

    struct Consent {
        uint id;
        address requester;
        address owener;
        uint consentId;
        uint date;
        bool status;
    }
    uint consentCount;

    constructor(){
        consentCount = 0;
    }

    mapping (uint => Consent) public consents;

    function addCosentDetail(address _requester,
                             address _owener,
                             uint _consentId) public {
        consents[consentCount] = Consent(consentCount,
                                         _requester,
                                         _owener,
                                         _consentId,
                                         block.timestamp,
                                         false);
        consentCount += 1;
    }

    function setConsentStatus(uint _id, bool _status) public {
        require(msg.sender == consents[_id].owener, "Only Owner");
        consents[_id].status = _status;
    }
}
```

รูปที่ 3.12 ตัวอย่างชุดคำสั่งของสัญญาอัจฉริยะ

จากรูปที่ 3.10 และรูปที่ 3.11 แสดงให้เห็นถึงกระบวนการทำงานของสัญญาอัจฉริยะบนบล็อกเชน เป็นกระบวนการปรับใช้และใช้งานสัญญาอัจฉริยะเพื่อจัดการความยินยอมในลักษณะที่ปลอดภัย กระจายอำนาจ และเป็นอัตโนมัติสำหรับการจัดการข้อมูลและดำเนินธุรกรรม ในขณะเดียวกันก็รับประกันความเป็นส่วนตัวและความโปร่ง ในแต่ละขั้นตอนอธิบายรายละเอียดได้ดังนี้

1) สร้างเครือข่ายเชน (Build Chains Network): เป็นกระบวนการสำคัญและเป็นขั้นตอนพื้นฐานในการเริ่มต้นระบบบล็อกเชนใหม่ โดยเริ่มต้นจากการสร้างบล็อกแรกที่เรียกว่า “บล็อกกำเนิด (Genesis Block)” ซึ่งถือเป็นจุดเริ่มต้นและจุดยึดสำหรับบล็อกทั้งหมดที่ถูกสร้างในอนาคต ไฟล์ genesis.json เป็นไฟล์กำหนดค่าที่สำคัญในการสร้างบล็อกกำเนิดนี้ โดยไฟล์ดังกล่าวระบุพารามิเตอร์ต่าง ๆ เช่น การกระจายโทเค็นเริ่มต้นที่ใช้ในเครือข่าย กลไกฉันทามติ (Consensus Algorithm) ที่ถูกใช้เพื่อประมวลผลการยืนยันธุรกรรมในเครือข่าย รวมถึงการตั้งค่าพื้นฐานอื่น ๆ เมื่อกำหนดค่าผ่านไฟล์ genesis เสร็จเรียบร้อย เครือข่ายบล็อกเชนจะถูกเริ่มต้นขึ้น นอกจากนี้ ยังมีการตั้งค่าซอฟต์แวร์และฮาร์ดแวร์สำหรับโหนด ซึ่งทำหน้าที่เป็นส่วนหนึ่งของเครือข่าย โหนดเหล่านี้ช่วยในการตรวจสอบและบันทึกธุรกรรม ทำให้ระบบบล็อกเชนสามารถทำงานได้อย่างปลอดภัยและมีเสถียรภาพในระยะยาว

2) ตั้งค่าสภาพแวดล้อมการพัฒนา (Development Environment Setup): ขั้นตอนนี้เกี่ยวข้องกับการติดตั้งเครื่องมือและซอฟต์แวร์ที่จำเป็นเพื่ออำนวยความสะดวกในการสร้าง การทดสอบและการปรับใช้สัญญาอัจฉริยะโดยเฉพาะสำหรับแพลตฟอร์มอีเธอเรียม ส่วนประกอบหลักของสภาพแวดล้อมการพัฒนาได้แก่

2.1) เครื่องเสมือนอีเธอเรียม (Ethereum Virtual Machine – EVM): สภาพแวดล้อมรันไทม์นี้มีหน้าที่รับผิดชอบในการดำเนินการสัญญาอัจฉริยะในลักษณะแบบกระจายอำนาจ เข้ากันได้กับอีเธอเรียมและบล็อกเชนที่ใช้ EVM อื่น ๆ

2.2) ซอลิดิตี (Solidity): ภาษาโปรแกรมที่ใช้สำหรับเขียนตรรกะของสัญญาอัจฉริยะ ความแข็งแกร่งช่วยให้สามารถสร้างสัญญาที่ดำเนินการด้วยตนเอง ซึ่งจะบังคับใชh ข้อกำหนดและเงื่อนไขโดยอัตมัติเมื่อเป็นไปตามเกณฑ์ที่กำหนดไว้ล่วงหน้า

2.3) โก-อีเธอเรียม (Go-Ethereum – Geth): เครื่องมือรายคำสั่งและลูกข่ายอีเธอเรียมที่ให้ส่วนต่อประสานสำหรับการโต้ตอบกับบล็อกเชนที่ใช้อีเธอเรียม Geth ใช้สำหรับ การปรับใช้สัญญาอัจฉริยะ การจัดการโหนด และการประมวลผลธุรกรรม

3) โหลดคำสั่งสัญญาอัจฉริยะ (Load Smart Contract Code): คำสั่งสัญญาอัจฉริยะ ซึ่งโดยทั่วไปจะเขียนด้วยภาษาซอลิดิตีหรือภาษาที่คล้ายกัน จะถูกโหลดลงในสภาพแวดล้อม การพัฒนา ขั้นตอนนี้รวมถึงการรวบรวมคำสั่งเพื่อระบุและแก้ไขข้อผิดพลาด เพื่อให้แน่ใจว่าสัญญาอัจฉริยะพร้อมสำหรับการใช้งาน สัญญาจะกำหนดตรรกะทางธุรกิจ เช่น ข้อกำหนด เงื่อนไข และการดำเนินการอัตโนมัติ

4) กระเป๋าเงินผู้ใช้ (Wallet Client): ถูกใช้เป็นสะพานเชื่อมระหว่างผู้ใช้และเครือข่ายบล็อกเชน มีกุญแจการเข้ารหัสที่จำเป็นสำหรับการลงนามธุรกรรมอย่างปลอดภัยและการปรับใช้สัญญาอัจฉริยะ กระเป๋าเงินผู้ใช้ยังอำนวยความสะดวกในการโต้ตอบอื่น ๆ กับบล็อกเชน เช่น การส่งข้อมูลธุรธรรม และการจัดการข้อมูลรับรองผู้ใช้

5) ข้อมูลธุรกรรม (Transaction Data): ข้อมูลที่เกี่ยวข้องกับการดำเนินการของสัญญาอัจฉริยะได้รับการจัดเตรียมและส่งไปยังบล็อกเชนเป็นข้อมูลธุรกรรม ตัวอย่างได้แก่ บันทึกความยินยอมของผู้ใช้ ธุรกรรมทางการเงิน หรือการอนุญาตในการแบ่งปันข้อมูล ธุรกรรมเหล่านี้กระตุ้นให้เกิดตรรกะของสัญญาอัจฉริยะบนบล็อกเชน

6) เครือข่ายบล็อกเชน (Blockchain Network): เครือข่ายบล็อกเชนทำหน้าที่เป็นบัญชีแยกประเภทแบบกระจายอำนาจที่มีการปรับใช้และดำเนินการสัญญาอัจฉริยะ ตรวจสอบ และประมวลผลธุรกรรมตามตรรกะที่กำหนดไว้ในสัญญาอัจฉริยะ ตัวอย่างของเครือข่ายได้แก่: ไบแนนซ์สมาร์ทเชน (Binance Smart Chain) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และ เรอิเชน (REI Chain) อีกทางเลือกแพลตฟอร์มสำหรับการดำเนินการสัญญาอัจฉริยะ

7) ดำเนินธุรกรรม (Execute Transaction): เครือข่ายบล็อกเชนจะประมวลผลและตรวจสอบธุรกรรมตามตรรกะที่กำหนดไว้ล่วงหน้าที่เข้ารหัสในสัญญาอัจฉริยะ กระบวนการนี้รวมถึงการตรวจสอบข้อมูลธุรกรรมเพื่อให้แน่ใจว่าเป็นไปตามข้อกำหนดและเงื่อนไขของสัญญา และดำเนินการตามที่ระบุไว้ในสัญญาเพื่ออำนวยความสะดวกในเรื่องนี้ ระบบจึงใช้ Web3.js ซึ่งเป็นไลบรารีสำหรับการโต้ตอบกับบล็อกเชน การสื่อสารระหว่างแอปพลิเคชันและบล็อกเชนทำได้โดยใช้ JSON-RPC เป็นส่วนต่อประสานและ ABI สำหรับการโต้ตอบสัญญาอัจฉริยะ

8) ข้อมูลบล็อกเชน (Blockchain Data): ผลลัพธ์ของธุรกรรมที่ดำเนินการจะถูกบันทึกไว้ในบัญชีแยกประเภทอย่างไม่เปลี่ยนแปลง บล็อกเชนจัดเก็บข้อมูลประเภทเฉพาะ ซึ่งรวมถึงที่อยู่ของสัญญาอัจฉริยะ ยอดคงเหลือของกระเป๋าเงิน (จำนวนสกุลเงินดิจิทัลที่มีอยู่ในนั้น) และรหัสไบนารีของสัญญาอัจฉริยะ (กฎและฟังก์ชันที่กำหนดสิ่งที่สามารถทำได้)

กระบวนการทดลองในบริบทการวิจัยครั้งนี้ การทดลองนี้เป็นการนำระบบบริหารจัดการความยินยอมโดยใช้ชุดคำสั่งสัญญาอัจฉริยะ (Smart Contracts) ที่พัฒนาด้วยภาษาซอลิดิตีมาประมวลผลบนแพลตฟอร์มบล็อกเชนต่าง ๆ ตามแผนผังกระบวนการทำงานของสัญญาอัจฉริยะบนบล็อกเชน (รูปที่ 3.10 และ 3.11) โดยงานวิจัยครั้งนี้มุ่งเน้นไปที่ 4 แพลตฟอร์มหลักได้แก่ ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xChain) และเรอิเชน (REI Chain) โดยอาศัยคุณลักษณะเด่นที่สำคัญของเทคโนโลยีบล็อกเชน เช่น ข้อมูลธุรกรรมมีความโปร่งใส ตรวจสอบได้ และข้อมูลย้อนกลับไปแก้ไขไม่ได้ ซึ่งข้อมูลที่เข้าถึงจะต้องได้ความยินยอมจากเจ้าของข้อมูลก่อนโดยผ่านระบบบริหารจัดการความยินยอม

การศึกษานี้มุ่งเน้นไปที่ผลลัพธ์ของนำระบบบริหารจัดการความยินยอมด้วยชุดคำสั่งสัญญาอัจฉริยะไปประมวลผลบนบล็อกเชนทั้ง 4 แพลตฟอร์ม ซึ่งสะท้อนถึงขอบเขตและเข้าถึงเครือข่ายบล็อกเชนที่อยู่ระหว่างการพิจารณาเพื่อปรับใช้ได้อย่างเหมาะสม การทดลองนี้เกิดขึ้นภายในสภาพแวดล้อมที่มีการควบคุมของเครือข่ายอินเทอร์เน็ตของมหาวิทยารังสิต (RSU-NET) การทดสอบบนเครือข่ายของมหาวิทยาลัยเป็นสถานการณ์จริงที่ช่วยให้นักวิจัยสามารถสังเกตได้ว่าแพลตฟอร์มบล็อกเชนเหล่านี้ทำงานอย่างไรภายใต้เงื่อนไขบางประการ การทดลองนี้มุ่งเน้นไปที่การประเมินคุณสมบัติและประสิทธิภาพของแพลตฟอร์มบนบล็อกเชนต่าง ๆ ในบริบทของงานวิจัย ดังแสดงรายละเอียดไว้ในตารางที่ 3.3

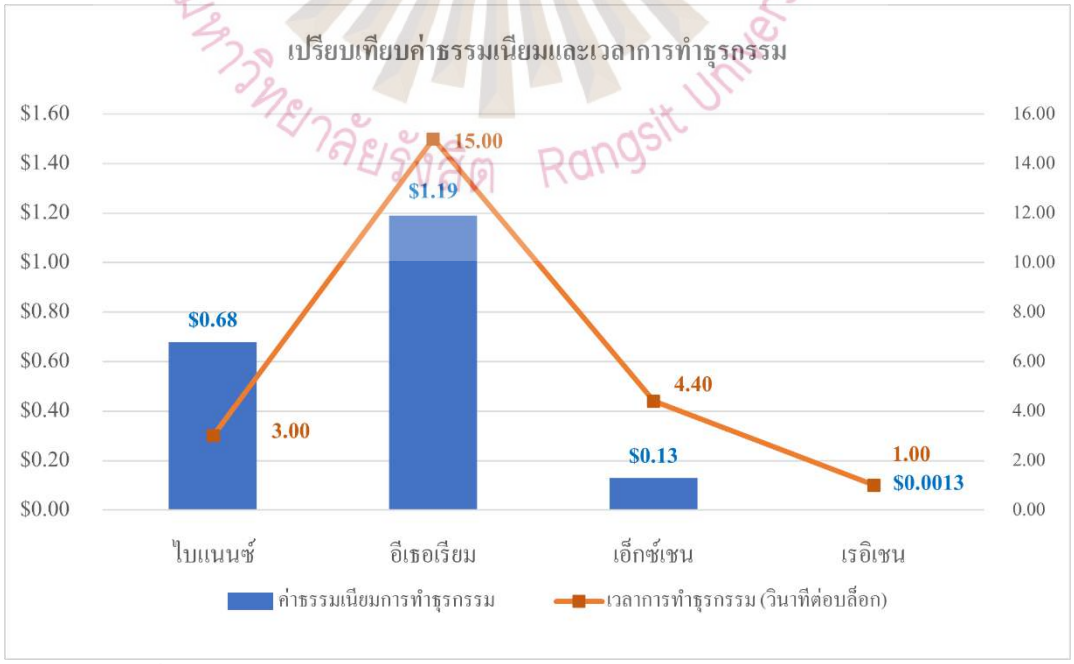
ตารางที่ 3.3 การเปรียบเทียบประสิทธิภาพของแพลตฟอร์มบล็อกเชน

พารามิเตอร์	**ไบแนนซ์**	**อีเธอเรียม**	**เอ็กซ์เชน**	**เรอิเชน**
ค่าธรรมเนียมการทำธุรกรรม	0.00210247 BNB ($0.68)	0.0007262041726249 ETH ($1.19)	0.00421894 XTH ($0.13)	0.000043822 REI ($0.0013)
เวลาทำธุรกรรม	3 วินาที	15 วินาที	4.4 วินาที	1 วินาที
ขีดจำกัดก๊าซ	420,494	46,422	421,894	65,733
ก๊าซที่ใช้ไป	420,494 (100%)	46,422 (100%)	421,894 (100%)	43,822 (66.67%)
ราคาก๊าซ	5 Gwei	15.64353 Gwei	10 Gwei	1 Gwei
กลไกฉันทามติ	PoSA	PoS	PoA	PoA
การรับส่งข้อมูลบล็อกเชนและระบบนิเวศ	4,567	3,815	4	25
การรวมศูนย์	43 สถานี	500,000+ สถานี	21 สถานี	3 สถานี

จากตารางที่ 3.3 ตารางนี้แสดงการวิเคราะห์เชิงเปรียบเทียบของแพลตฟอร์มบล็อกเชนทั้ง 4 แพลตฟอร์ม ได้แก่ ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xChain) และเรอิเชน (REI Chain) โดยมุ่งเน้นไปที่พารามิเตอร์ประสิทธิภาพหลัก เช่น ค่าธรรมเนียมการทำธุรกรรม ความเร็ว การจัดการก๊าซ กลไกฉันทามติ กิจกรรมของระบบนิเวศ การรวมศูนย์ และระดับความต้านทานต่อการโจมตี สามารถอธิบายรายละเอียดในแต่ละพารามิเตอร์ได้ดังนี้

1) ค่าธรรมเนียมการทำธุรกรรม (Transaction Frees): เรอิเชนโดดเด่นด้วยค่าธรรมเนียมการทำธุรกรรมต่ำที่สุดที่ $0.0013 ทำให้คุ้มค่าอย่างมากสำหรับธุรกรรมขนาดเล็กและการซื้อขายที่มีความถี่ เอ็กซ์เชนมอบความสมดุลระหว่างความสามารถในการจ่ายและประสิทธิภาพโดยมีค่าธรรมเนียมปานกลางที่ $0.13 ไบแนนซ์มีค่าธรรมเนียม $0.68 สะท้อนถึงโครงสร้างที่มีประสิทธิภาพแต่มีศูนย์กลางในระดับปานกลาง ในขณะที่ อีเธอเรียมซึ่งมีค่าธรรมเนียมสูงสุดอยู่ที่ $1.19 เผชิญกับค่าใช้จ่ายที่สูงขึ้นเนื่องจากความแออัดของเครือข่ายและความต้องการในการคำนวณแบบใช้ก๊าซ

2) เวลาการทำธุรกรรม (Transaction Time): เรอิเชนเป็นผู้นำด้วยเวลาการทำธุรกรรมที่เร็วที่สุด 1 วินาที ทำให้เหมาะสมสำหรับการใช้งานแบบเรียลไทม์ ไบแนนซ์ตามมาใน 3 วินาที ทำให้ความเร็วสมดุลกับความน่าเชื่อถือ เอ็กซ์เชนประมวลผลธุรกรรมภายใน 4.4 วินาที ตอบสนองความต้องการความเร็วปานกลาง ในขณะที่ อีเธิเรียมซึ่งมีเวลาการทำธุรกรรมช้าที่สุด15 วินาที สะท้อนถึงลักษณะการกระจายอำนาจและโหลดเครือข่ายที่สูงขึ้น



รูปที่ 3.13 เปรียบเทียบค่าธรรมเนียมการทำธุรกรรมและเวลาการทำธุรกรรม

3) การจัดการก๊าซ (Gas Management: Limit, Used, and Price): ไบแนนซ์และเอ็กเชนรองรับขีดจำกัดก๊าซสูงถึง 420,494 ช่วยให้การทำธุรกรรมที่ซับซ้อนพร้อมการใช้งานเต็มรูปแบบเพื่อประสิทธิภาพ อีเธอเรียมซึ่งมีขีดจำกัดก๊าซต่ำสุด 46,422 อาจจำกัดการดำเนินการที่ซับซ้อนสูงแต่บรรลุการใช้งาน 100% ซึ่งบ่งชี้ถึงการใช้งานที่มีประสิทธิภาพ เรอิเชนมีขีดจำกัดก๊าซปานกลางที่ 65,777 โดยใช้ไป 66.67% อาจเนื่องมาจากความซับซ้อนของธุรกรรมหรือการเพิ่มประสิทธิภาพที่ลดลง ในส่วนค่าก๊าซที่แตกต่างกันอย่างกันอย่างมาก โดยเรอิเชน (1 Gwei) และไบแนนซ์ (5 Gwei) มีความคุ้มค่า ในขณะที่ เอ็กซ์เชน (10 Gwei) และอีเธอเรียม (15.64 Gwei) มีราคาสูงกว่าเมื่อเปรียบเทียบกัน

4) กลไกฉันทามติ (Consensus Mechanism): อีเธอเรียมใช้การพิสูจน์การเดิมพัน (Proof of Stake – PoS) โดยจัดลำดับความสำคัญด้านความปลอดภัยและการกระจายอำนาจ แม้ว่าประสิทธิภาพจะลดลงก็ตาม ไบแนนซ์และเอ็กซ์เชนใช้ประโยชน์จากการพิสูจน์การมีอำนาจเดิมพัน (Proof of Staked Authority – PoSA) และการพิสูจน์การมีอำนาจ (Proof of Authority – PoA) ตามลำดับซึ่งให้ประสิทธิภาพที่มากกว่าแต่ลดการกระจายอำนาจลง ส่วนเรดิเชนยังใช้การพิสูจน์การมีอำนาจ (Proof of Authority – PoA) โดยเน้นที่ความเร็วและความคุ้มค่าทำให้ไม่เหมาะกับการใช้งานที่ต้องการความปลอดภัยสูง

5) การรับส่งข้อมูลบล็อกเชนและกิจกรรมระบบนิเวศ (Blockchain Traffic and DApps Ecosystem): ไบแนนซ์เป็นผู้นำในกิจกรรมระบบนิเวศด้วย 4,567 DApps แสดงให้เห็นการนำไปใช้ที่แข็งแกร่งและความสามารถรอบด้าน ตามมาด้วยอีเธอเรียมที่มี 3.816 DApps สะท้อนให้เห็นถึงระบบนิเวศที่แข็งแกร่งและหลากหลาย ในทางตรงกันข้าม เรอิเชนและเอ็กซ์เชนมีการนำไปใช้เพียงเล็กน้อย โดยมีเพียง 25 และ 4 DApps ตามลำดับ ซึ่งเน้นย้ำถึงการพัฒนาระบบนิเวศที่จำกัด

6) การรวมศูนย์ (Centralize): อีเธอเรียมมีการกระจายอำนาจอย่างสูงด้วยโหนดมากกว่า 500,000+ โหนด รับประกันความปลอดภัยที่เหนือกว่าและต้านทานการโจมตี ไบแนนซ์ที่มี 43 โหนด และเอ็กซ์เชนที่มี 21 โหนด ทำให้เกิดความสมดุลระหว่างการกระจายอำนาจและประสิทธิภาพ ในทางตรงกันข้าม เรอิเชนซึ่งมีเพียง 3 โหนด มีการรวมศูนย์ไว้สูง ทำให้เสี่ยงต่อการถูกโจมตีหรือการสมรู้ร่วมคิดของผู้ตรวจสอบความถูกต้อง

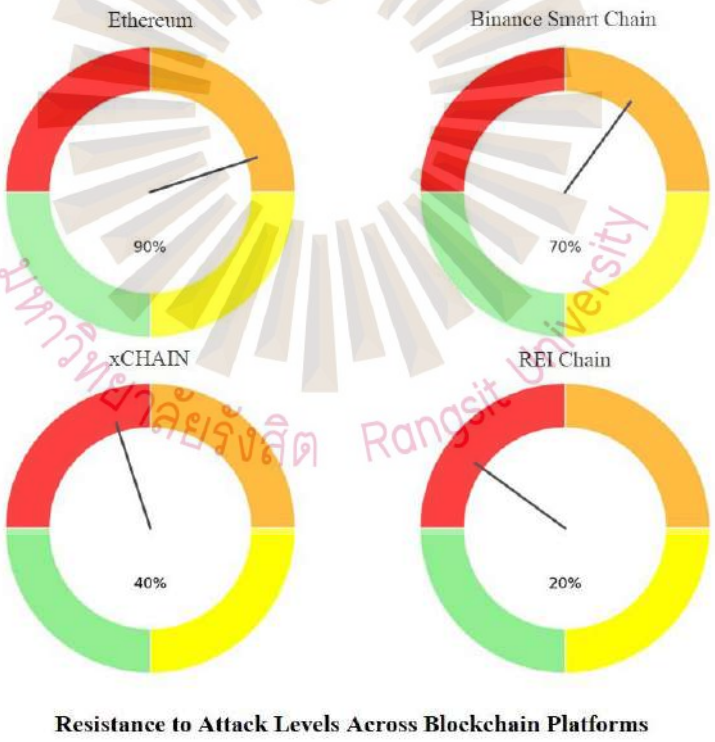
7) ระดับความต้านทานต่อการโจมตี (Level of Resistance to Attack): ระดับความต้านทานต่อการโจมดีในเครือข่ายบล็อกเชนถูกกำหนดโดยปัจจัยต่าง ๆ เช่น การกระจายอำนาจ กลไกฉันทามติ และการรับส่งข้อมูลเครือข่าย ในบริบทของงานวิจัย แต่ละแพลตฟอร์มบล็อกเชนมีระดับความต้านทานต่อการโจมดีที่แตกต่างกันในระดับต่าง ๆ ดังรูปที่ 3.14

7.1) อีเธอเรียม: มีความต้านทานสูง การกระจายอำนาจ (500,000+ โหนด) และกลไกฉันทามติแบบ PoS ให้ความปลอดภัยที่แข็งแกร่ง การนำไปใช้อย่างกว้างขวางและปริมาณการรับส่งข้อมูลที่สูงยังช่วยเพิ่มความแข็งแกร่งต่อการโจมตีอีกด้วย

7.2) ไบแนนซ์: มีความต้านทานปานกลาง ด้วยโหนด 43 โหนดและกลไกฉันทามติแบบ PoSA การกระจายอำนาจในระดับหนึ่งแต่ยังคงอ่อนแอต่อการสมรู้ร่วมคิดระหว่างผู้ตรวจสอบความถูกต้อง กิจกรรม DApps สูงจะเพิ่มความยืดหยุ่น

7.3) เอ็กซ์เชน: มีความต้านทานต่ำ การรวมศูนย์ 21 โหนดและกลไกฉันทามติแบบ PoA ลดความปลอดภัย การนำ DApps มาใช้และการรับส่งข้อมูลอย่างจำกัดทำให้กำหนดเป้าหมายได้ง่าย

7.4) เรอิเชน: ความต้านทานต่ำมาก การรวมศูนย์ที่รุนแรง 3 โหนด และกลไกฉันทามติแบบ PoA ทำให้มีความเสี่ยงสูง กิจกรรมของระบบนิเวศที่จำกัดยิ่งทำให้ความต้านทานต่อการโจมตีลดลงอีกด้วย



รูปที่ 3.14 เปรียบเทียบระดับความต้านทานต่อการโจมตี

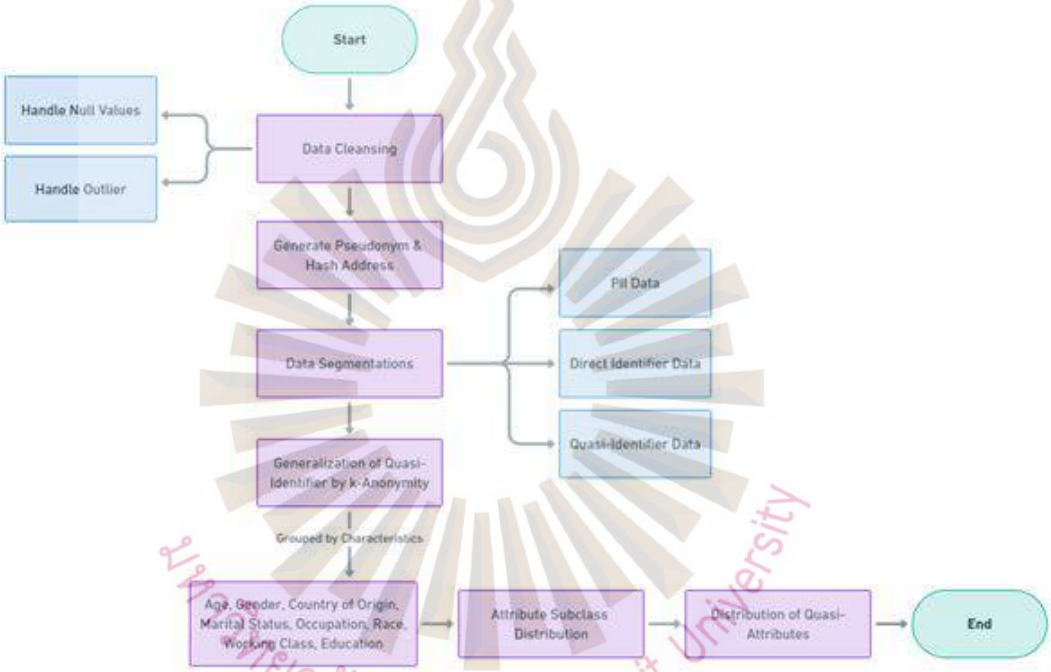
ตารางที่ 3.4 สรุปจุดแข็งและจุดอ่อนของแต่ละแพลตฟอร์ม

แพลตฟอร์มบล็อกเชน	จุดแข็ง	จุดอ่อน
ไบแนนซ์	- ค่าธรรมเนียมการทำธุรกรรมต่ำ - เวลาการทำธุรกรรมที่รวมเร็ว - ขีดจำกัดก๊าซสูงสำหรับการดำเนินการที่ซับซ้อน - ระบบนิเวศ DApps ที่แข็งแกร่ง	- การรวมศูนย์ระดับปานกลางด้วย 43 โหนด - การพึ่งพาผู้ตรวจสอบความถูกต้องจำนวนน้อยกว่า
อีเธอเรียม	- มีการกระจายอำนาจสูงด้วยโหนดมากกว่า 500,000+ โหนด - การยอมรับระบบนิเวศอย่างกว้างขวาง - กลไกฉันทามติที่ปลอดภัย	- ค่าธรรมเนียมการทำธุรกรรมสูง - เวลาการทำธุรกรรมช้า - ข้อจำกัดของก๊าซ จำกัดการดำเนินงานที่ซับซ้อน
เอ็กซ์เชน	- ค่าธรรมเนียมการทำธุรกรรมปานกลาง - ความเร็วการทำธุรกรรมที่เหมาะสม - ขีดจำกัดก๊าซสูงสำหรับการสนับสนุนธุรกรรมที่ซับซ้อน	- กิจกรรมระบบนิเวศ DApps ต่ำ - การรวมศูนย์ระดับปานกลางด้วย 21 โหนด
เรอิเชน	- ค่าธรรมเนียมการทำธุรกรรมต่ำสุด - เวลาการทำธุรกรรมที่เร็วที่สุด	- การรวมศูนย์ขั้นสูงสุดด้วย 3 โหนดเท่านั้น - การพัฒนาระบบนิเวศ DApps มีจำกัด - ขีดจำกัดของก๊าซที่ต่ำกว่า ลดความเหมาะสมในการทำธุรกรรมที่ซับซ้อน

3.3.2 การทดลองที่ 2: การใช้เทคนิคการแฝงข้อมูลโดยการทดลองร่วมกับโครงการนำร่องที่ชื่อว่า RSU-Data-Anonymization โดยใช้เทคนิค k-anonymity

กระบวนการทดลองนี้มีขั้นตอนการทำงานของการใช้เทคนิคการแฝงข้อมูลและทำให้

เป็นลักษณะทั่วไป ขั้นตอนการทำงานโดยละเอียดนี้ดังรูปที่ 3.15 จะอธิบายขั้นตอนและวิธีการสำหรับการใช้เทคนิคการแฝงข้อมูลและการกำหนดชุดข้อมูลลักษณะทั่วไปเพื่อปกป้องความเป็นส่วนตัวในขณะที่ยังคงรักษาอรรถประโยชน์ข้อมูลไว้ด้วยการใช้เทคนิคต่าง ๆ เช่น การแฝงข้อมูล การแฮช และ k-Anonymity ให้การป้องกันที่แข็งแกร่งต่อความเสี่ยงในการระบุตัวตนซ้ำ แนวทางนี้ช่วยให้มั่นใจว่าจะปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัวและเพิ่มความปลอดภัยของข้อมูล ขั้นตอนการทำงานนี้จะสมดุลระหว่างความต้องการความเป็นส่วนตัวกับความสำคัญของการรักษาการใช้ข้อมูลได้อย่างมีประสิทธิภาพ แต่ละขั้นตอนมีรายละเอียดนี้



รูปที่ 3.15 ขั้นตอนการทำงานของการทดลองที่ 2

ชุดข้อมูลที่มีชื่อเสียงชื่อ “Adult.csv” นี่คือชุดข้อมูลที่รู้จักกันดีในชุมชนการเรียนรู้ของเครื่อง ซึ่งมักใช้เพื่อสาธิตการประมวลผลข้อมูลและเทคนิคการเรียนรู้ของเครื่องต่าง ๆ พร้อมใช้งานผ่าน UCI Machine Learning Repository ซึ่งเป็นแหล่งข้อมูลยอดนิยมสำหรับชุดข้อมูลที่ใช้ในสถาบันการศึกษาและการวิจัย โดยทั่วไปชุดข้อมูล “Adult.csv” จะประกอบด้วยคุณลักษณะต่าง ๆ เช่น ระดับการศึกษา อายุ เพศ และอาชีพ ซึ่งมีอิทธิพลโดยสัญชาตญาณในการกำหนดรายได้ของแต่ละบุคคล เพื่อวัตถุประสงค์ของการทดลองนี้ ได้มีการเสริมกับข้อมูลส่วนบุคคลเพิ่มเติม เช่น หมายเลขประกันสังคม ชื่อ นามสกุล และที่อยู่ ชุดข้อมูลใหม่มีชื่อว่า “Full-Adult-dataset.csv” ซึ่งชุดข้อมูลใหม่นี้แสดงถึงเวอร์ชันเสริมของชุดข้อมูล “Adult.csv” ดั้งเดิม ประกอบด้วยข้อมูลส่วนบุคคลที่

สามารถระบุตัวตนได้ (PII) มากขึ้น ทำให้เป็นต้นแบบที่แข็งแกร่งสำหรับการสาธิตเทคนิคการทำให้ข้อมูลเป็นนิรนามในงานวิจัยนี้ การทดลองใช้ประโยชน์จากเครื่องมือยอดนิยมในชุมชนการเรียนรู้ของเครื่อง โดยเฉพาะไพทอนและไลบรารี่ Scikit-learn สำหรับการจัดระเบียบชุดข้อมูลออกเป็น 3 ส่วนที่แตกต่างกันได้แก่ ส่วนตัวระบุโดยตรง ส่วนตัวระบุเสมือน และส่วนที่เป็นนิรนาม

3.3.2.1 ขั้นตอนที่ 1 การทำความสะอาดข้อมูล:

ขั้นตอนการทำความสะอาดข้อมูลมุ่งเน้นไปที่การสร้างข้อมูลที่สะอาด แม่นยำ และ สม่ำเสมอ ซึ่งจำเป็นสำหรับการรักษาคุณภาพของข้อมูลและทำให้การวิเคราะห์เชื่อถือได้ ในขั้นตอนนี้ เกี่ยวข้องกับงานหลักสองส่วนคือ การจัดการค่า Null (Handing Null Values) และการจัดการค่าผิดปกติ (Managing Outliers) ด้วยขั้นตอนเหล่านี้ข้อมูลจะได้รับการปรับปรุงให้มีความถูกต้อง สม่ำเสมอ และพร้อมสำหรับการประมวลผลหรือการวิเคราะห์ในขั้นตอนต่อไป

1) การจัดการค่า Null (Handing Null Values): ค่าที่หายไปหรือเป็นค่าว่างในชุดข้อมูลอาจทำให้เกิดความไม่ถูกต้องหรือขัดขวางการวิเคราะห์เพิ่มเติม เพื่อแก้ไขปัญหานี้ ค่าที่หายไป จะถูกระบุและประมวลผลผ่านวิธีการต่าง ๆ หรือลบออก โดยมีวิธีการดังนี้

จากรูปที่ 3.16 แสดงชุดคำสั่งการทำความสะอาดข้อมูลด้วยการจัดการค่าว่างหรือค่าที่หายไปสำหรับชุดข้อมูลที่มีข้อมูลส่วนบุคคล (PII) เริ่มต้นโดยนำเข้าชุดข้อมูลที่ชื่อ “adult_with_pii.csv” ลงในดาต้าเฟรม (df) มีการเรียกใช้ไลบรารี NumPy และ Pandas คอลัมน์เฉพาะที่ใช้จัดการกับค่าที่หายไป ได้แก่ country, workclass และ occupation พบว่ามีอักขระพิเศษ (?) ที่บ่งชี้ค่าที่หายไป อักขระเหล่านี้จะถูกแทนที่ด้วยค่า NaN แถวที่มีค่า NaN ในคอลัมน์ใด ๆ จะถูกลบออกจากชุดข้อมูลเพื่อให้แน่ใจว่าไม่มีข้อมูลที่ไม่สมบูรณ์เหลืออยู่หลังจากการดำเนินการนี้ ชุดข้อมูลจะลดลงเหลือ 30,162 รายการ ซึ่งบ่งชี้ว่ามีการลบออกไป 2,399 รายการเนื่องจากพบค่าที่หายไป ชุดข้อมูลที่ทำการลบค่าที่หายไปออกแล้วจะถูกบันทึกเป็นไฟล์ใหม่ชื่อ “adult_with_pii_null.csv”

```python
# Import libraries
import numpy as np  # for linear algebra
import pandas as pd  # for data processing
# Load the dataset
df = pd.read_csv('adult_with_pii.csv')
print('Total Row', df.shape[0], 'rows')

df1 = df
# Replace special characters with NaN
df1['Country'] = df1['Country'].replace('?', np.nan)
df1['Workclass'] = df1['Workclass'].replace('?', np.nan)
df1['Occupation'] = df1['Occupation'].replace('?', np.nan)
# Drop rows with any NaN values
df1.dropna(how='any', inplace=True)

print('Total Row without null', df1.shape[0], 'rows')

# Saving output to csv file
df1.to_csv('adult_with_pii_null.csv', index=False)

# Display the first 7 rows of the dataframe
df1.head(7)
```

```
Total Row 32561 rows
Total Row without null 30162 rows
```

	Name	DOB	SSN	Zip	Age	Workclass	fnlwgt	Education	Education-Num	Marital Status	Occupation
0	Karrie Trusslove	9/7/1967	732-14-6110	64152	39	State-gov	77516	Bachelors	13	Never-married	Adm-clerical
1	Brandise Tripony	6/7/1988	150-19-2766	61523	50	Self-emp-not-inc	83311	Bachelors	13	Married-civ-spouse	Exec-managerial
2	Brenn McNeely	8/6/1991	725-59-9860	95668	38	Private	215646	HS-grad	9	Divorced	Handlers-cleaners
3	Dorry Poter	4/6/2009	659-57-4974	25503	53	Private	234721	11th	7	Married-civ-spouse	Handlers-cleaners
4	Dick Honnan	9/16/1951	220-93-3811	75387	28	Private	338409	Bachelors	13	Married-civ-spouse	Prof-specialty

รูปที่ 3.16 ขั้นตอนการจัดการค่าที่หายไป

2) การจัดการค่าผิดปกติ (Managing Outliers): ค่าผิดปกติซึ่งเป็นจุดข้อมูลที่รุนแรงหรือผิดปกติ สามารถบิดเบือนผลลัพธ์การวิเคราะห์หรือก่อให้เกิดความเสี่ยงในบริบทที่ละเอียดอ่อนต่อความเป็นส่วนตัว ค่าเหล่านี้ได้รับการระบุอย่างระมัดระวัง และลบออกหรือเปลี่ยนรูปขึ้นอยู่กับข้อกำหนดในการวิเคราะห์ โดยมีวิธีการดังนี้

จากรูปที่ 3.17 แสดงวิธีการระบุค่าผิดปกติในชุดข้อมูลโดยใช้วิธีช่วงระหว่างควอร์ไทล์ (Interquartile Range – IQR) การตรวจจับค่าผิดปกติเป็นสิ่งสำคัญในการรับรองคุณภาพของข้อมูลและป้องกันการวิเคราะห์ที่บิดเบือนซึ่งเกิดจากค่าที่มากเกินไปหรือผิดปกติ เริ่มต้นด้วยการนำเข้าและอ่านชุดข้อมูล “adult_with_pii_null.csv” โดยข้อมูลจะถูกจัดเรียงตามคอลัมน์ ‘Age’ จากมากไปน้อย การคำนวณหาค่า IQR จะกำหนดให้ควอร์ไทล์แรก (Q1) คำนวณที่เปอร์เซ็นไทล์ที่ 20 ของคอลัมน์ตัวเลข และควอร์ไทล์ที่สาม (Q3) คำนวณที่เปอร์เซ็นไทล์ที่ 80 วิธีการนี้ค่อนข้างแปลก

เล็กน้อยเนื่องจากโดยทั่วไปแล้วค่า Q1 และ Q3 ถูกกำหนดไว้ที่เปอร์เซ็นไทล์ที่ 25 และ 75 ในที่นี้ผู้วิจัยได้พิจารณาข้อมูลตรงกลาง 60% แทนที่จะเป็นข้อมูลตรงกลางมาตรฐาน 50% (เพราะผู้วิจัยพิจารณาถึงความเหมาะสมและความสมบูรณ์ของข้อมูลหลังจากได้ทำการทดลองกำหนดค่า Q1 และ Q3 หลายครั้งจนได้ค่าที่เหมาะสมสำหรับชุดข้อมูลนี้) การกำหนดขอบเขตค่าผิดปกติคือ ค่าผิดปกติจะถูกกำหนดให้เป็นค่าที่ต่ำกว่า = Q1- 1.5*IQR หรือค่าที่สูงกว่า = Q3+1.5*IQR ขอบเขตเหล่านี้เรียกว่าขอบเขตล่างและบน ค่าที่อยู่นอกขอบเขตเหล่านี้ถือเป็นค่าผิดปกติและจะถูกลบออกจากชุดข้อมูลเพื่อหลีกเลี่ยงผลกระทบที่อาจเกิดขึ้นกับการวิเคราะห์เพิ่มเติม

```
# Sort the dataframe by 'age' in descending order and reset the index
df = pd.read_csv('adult_with_pii_null.csv')
df1 = df.sort_values(by=['Age'], ascending=False).reset_index()

# Calculate the first quartile (Q1) and third quartile (Q3)
Q1 = df2.quantile(0.2,numeric_only=True)
Q3 = df2.quantile(0.8,numeric_only=True)

# Calculate the Interquartile Range (IQR)
IQR = Q3 - Q1
IQR
```

```
# Calculate the upper and lower bounds for outliers
UpperBound = Q3 + 1.5 * IQR
LowerBound = Q1 - 1.5 * IQR
print("Upper Bound:",UpperBound),
print("Lower Bound:",LowerBound)
```

```
Upper Bound: index       55263.2
Zip                     170839.7
Age                         86.0
fnlwgt                  491402.7
Education-Num               19.0
Capital Gain                 0.0
Capital Loss                 0.0
Hours per week              71.0
dtype: float64
Lower Bound: index      -22671.2
Zip                     -70372.3
Age                       -10.0
fnlwgt                 -124825.3
Education-Num               3.0
Capital Gain                0.0
Capital Loss                0.0
Hours per week             15.0
dtype: float64
```

รูปที่ 3.17 แสดงวิธีการระบุค่าผิดปกติโดยใช้วิธีช่วงระหว่างควอร์ไทล์ (IQR)

เมื่อได้ขอบเขตค่าผิดปกติดังกล่าวแล้วจากนั้นก็ทำการลบค่าผิดปกติออกจากคอลัมน์ ‘Age’ และ ‘Hours per week’ ของชุดข้อมูลโดยใช้วิธีช่วงระหว่างควอร์ไทล์ (IQR) ค่าผิดปกติถูกระบุตามขอบเขตบนและล่างที่คำนวณได้ หลังจากทำการจัดการค่าหายไปชุดข้อมูลมี 30,162 รายการ เมื่อกรองคอลัมน์ ‘Age’ จะตรวจพบค่าผิดปกติเล็กน้อย ส่งผลให้จำนวนรายลดลงเหลือเพียง 30,123 รายการ อย่างไรก็ตามคอลัมน์ ‘Hours per week’ แสดงค่าที่ผิดปกติจำนวนมากขึ้น ส่งผลให้ขนาดชุดข้อมูลลดลงอย่างมากเหลือ 28,618 รายการหลังผ่านการทำความสะอาด ชุดข้อมูลที่ทำความสะอาดแล้วจะถูกบันทึกลงไฟล์ใหม่ชื่อ “adult_with_pii_null_outliers.csv” เพื่อใช้งานต่อไป เพื่อให้มั่นใจว่าข้อมูลมีคุณภาพและความน่าเชื่อถือที่ดีขึ้น รายละเอียดดังรูปที่ 3.18

```
# Correcting the quotation marks around 'Age'
drop_outlier1 = df1[(df1['Age'] < UpperBound['Age']) & (df1['Age'] > LowerBound['Age'])]
print("New Shape without outlier in 'Age Column': ", drop_outlier1.shape[0], "rows")
drop_outlier1.to_csv('adult_with_pii_null_outliers.csv', index=False)

# Correcting the quotation marks around 'Hours per week'
df2 = pd.read_csv('adult_with_pii_null_outliers.csv')
df3 = df2.sort_values(by=['Hours per week'], ascending=False).reset_index()
drop_outlier2 = df2[(df2['Hours per week'] < UpperBound['Hours per week']) & (df2['Hours per week'] > LowerBound['Hours per week'])]

print("New Shape without outlier in 'Hours per week Column': ", drop_outlier2.shape[0], "rows")

# Saving output to csv file
# Display the first 7 rows of the dataframe

drop_outlier2.to_csv('adult_with_pii_null_outliers.csv', index=False)

# Display the first 7 rows of the dataframe
drop_outlier2.head(7)
```

```
Total Row of Original Data: 30162 rows
Total Row without null:  30162 rows
New Shape without outlier in 'Age Column':  30123 rows
New Shape without outlier in 'Hours per week Column':  28618 rows
```

รูปที่ 3.18 แสดงการลบค่าผิดปกติออกจากชุดข้อมูล

ตารางที่ 3.5 ผลกระทบจากการทำความสะอาดข้อมูล

ชนิด	จำนวนแถว
รายการค่าที่หายไปลดลง	2,399
รายการที่มีค่าผิดปกติลดลง	1,544

จากตารางที่ 3.5 สรุปผลจากการทำความสะอาดข้อมูล รายงานว่ามีการลบข้อมูล 2,399 แถวที่มีค่าที่หายไป และ 1,544 แถวที่มีค่าผิดปกติออกจากชุดข้อมูล การทำความสะอาดข้อมูลลดชุดข้อมูลดั้งเดิมลงทั้งหมด 3,910 แถว ส่งผลให้ชุดข้อมูลสุดท้ายเหลือ 28,618 แถว การทำความสะอาดข้อมูลเป็นส่วนสำคัญของการเตรียมข้อมูล โดยเฉพาะอย่างยิ่งก่อนดำเนินการวิเคราะห์ทางสถิติหรืองานการเรียนรู้ของเครื่อง การลบค่าที่หายไปออกช่วยให้แน่ใจว่าชุดข้อมูลไม่มีข้อมูลที่ไม่สมบูรณ์ ซึ่งอาจบิดเบือนการวิเคราะห์ได้ การกำจัดค่าผิดปกติเป็นสิ่งสำคัญในการป้องกันค่าที่ผิดปกติอย่างยิ่งจากการบิดเบือน

3.3.2.2 ขั้นตอนที่ 2 สร้างข้อมูลแฝงและที่อยู่แฮช:

กระบวนการสร้างข้อมูลแฝงและที่อยู่แฮช เป็นวิธีการที่สำคัญในการปกป้องข้อมูลที่ละเอียดอ่อน ในขณะเดียวกันก็ทำให้มั่นใจได้ว่าข้อมูลดังกล่าวยังคงมีประโยชน์สำหรับการวิเคราะห์และการประมวลผล มีการนำไปใช้อย่างกว้างขวางในอุตสาหกรรมต่าง ๆ เพื่อให้เป็นไปตามกฎระเบียบการปกป้องข้อมูลส่วนบุคคล เช่น จีดีพีอาร์และพีดีพีเอ กระบวนการนี้เกี่ยวข้อง

กับสองขั้นตอนหลักดังนี้

3) การสร้างข้อมูลแฝง (Pseudonym Generation): ข้อมูลแฝงแทนที่ตัวระบุโดยตรง เช่น ชื่อ หมายเลขประกันสังคม หรือรายละเอียดส่วนบุคคลอื่น ๆ ด้วย ID ที่สร้างขึ้นแบบสุ่มหรือกำหนดอย่างเป็นระบบ ข้อมูลแฝงเหล่านี้จะกำจัดการเชื่อมโยงโดยตรงไปยังแต่ละบุคคล เพื่อให้มั่นใจถึงความเป็นส่วนตัว ในขณะเดียวกันค่าการวิเคราะห์ของข้อมูลก็ยังคงอยู่ ข้อมูลแฝงมีประโยชน์อย่างยิ่งเมื่อไม่จำเป็นต้องใช้ตัวระบุดั้งเดิมอีกต่อไป แต่การรักษาความสมบูรณ์ของชุดข้อมูลถือเป็นสิ่งสำคัญ

จากรูปที่ 3.19 แสดงกระบวนการสร้างข้อมูลแฝงซึ่งเป็นวิธีการทำให้ข้อมูลเป็นนิรนามที่ใช้ไพทอน ซึ่งออกแบบมาเพื่อแทนที่ตัวระบุที่ละเอียดอ่อน เช่น แทนชื่อด้วยข้อมูลแฝงที่ไม่ซ้ำกัน เพื่อให้ความมั่นใจถึงความเป็นส่วนตัว ใช้ไลบรารี pandas, random และ string เพื่อจัดการชุดข้อมูลและสร้างข้อมูลแฝงที่เป็นตัวอักษรและตัวเลขแบบสุ่ม กระบวนการนี้เกี่ยวข้องกับฟังก์ชันหลักสองฟังก์ชันคือ Generate_alphanumeric_id (ซึ่งสร้างข้อมูลแฝงที่ไม่ซ้ำกันโดยการรวมตัวอักษรและตัวเลขแบบสุ่ม) และ Pseudonymize_column (ซึ่งแทนที่ค่าที่ไม่ซ้ำกันทั้งหมดในคอลัมน์ที่ระบุด้วยข้อมูลแฝงเหล่านี้) หลังจากโหลดข้อมูลแล้วคอลัมน์ใหม่ชื่อ “Pseudonym_ID” จะถูกสร้างขึ้นเพื่อจัดเก็บข้อมูลแฝง โดยแทนที่ค่าละเอียดอ่อนเดิมในคอลัมน์ “Name” ชุดข้อมูลที่แทนค่าแล้วจะถูกบันทึกลงในไฟล์ใหม่ชื่อ “adult_pii_pseudonym.csv” เพื่อใช้ในอนาคต กระบวนการนี้ทำให้มั่นใจได้ถึงความเป็นส่วนตัวโดยการทำให้ข้อมูลแฝงไม่สามารถย้อนกลับได้ ในขณะเดียวกันก็รักษาคอลัมน์อื่น ๆ ไว้ครบถ้วนเพื่อวัตถุประสงค์ในการวิเคราะห์ วิธีการนี้จะทำให้ข้อมูลไม่เปิดเผยตัวตนสมดุลกับประโยชน์ข้อมูลช่วยให้ชุดข้อมูลยังคงมีประโยชน์สำหรับการวิจัยหรือการวิเคราะห์โดยไม่เปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อน

```python
import pandas as pd
import random
import string

#Define the RNG Pseudonymization Function
def generate_alphanumeric_id(length=10):
    """Generate a random alphanumeric ID."""
    characters = string.ascii_letters + string.digits  # Include both letters and digits
    return ''.join(random.choice(characters) for _ in range(length))

def pseudonymize_column(data, column_name):
    unique_values = data[column_name].unique()
    pseudonyms_id = {value: generate_alphanumeric_id() for value in unique_values}
    return data[column_name].map(pseudonyms_id)

# Load the dataset
data = pd.read_csv('adult_with_pii_null_outliers.csv')

# Replace 'ColumnName' with the name of the column you want to pseudonymize
data.insert(0, 'Pseudonym_ID', range(1, len(data) + 1))
data['Pseudonym_ID'] = pseudonymize_column(data, 'Name')

# Save the updated DataFrame back to a CSV (optional)
data.to_csv('adult_pii_pseudonym.csv', index=False)
data.head()
```

	Pseudonym_ID	Name	DOB	SSN	Zip	Age	Workclass	fnlwgt	Education	Education-Num	Marital Status	Occupation
0	GV69daktNi	Jamill Elphey	4/3/2004	820-46-7127	14029	85	Self-emp-not-inc	166027	HS-grad	9	Widowed	Sales
1	WflMSma1GS	Lenette Summerson	2/8/1962	443-69-4786	46412	85	Private	115364	HS-grad	9	Widowed	Sales
2	mENJQ8Kxjc	Sigrid Addington	1/8/2007	863-26-2416	88641	84	Local-gov	163685	HS-grad	9	Widowed	Exec-managerial
3	vpx6m9VpqO	Appolonia Winear	4/11/1987	549-44-4855	21017	84	Private	241065	Masters	14	Never-married	Prof-specialty

รูปที่ 3.19 แสดงการสร้างข้อมูลแฝง

4) การสร้างที่อยู่แฮช: ที่อยู่แฮชถูกสร้างขึ้นโดยใช้ฟังก์ชันแฮชที่เข้ารหัส เช่น SHA-256 ฟังก์ชันเหล่านี้แปลงข้อมูลที่ละเอียดอ่อนให้เป็นค่าแฮชที่มีความยาวคงที่ ปลอดภัยและไม่สามารถย้อนกลับได้ แฮชแต่ละรายการมีเอกลักษณ์เฉพาะสำหรับข้อมูลนำเข้า ทำให้มั่นใจได้ถึงการรักษาความลับของข้อมูล ในขณะเดียวกันก็ช่วยให้สามารถตรวจสอบหรือจับคู่ชุดข้อมูลต่าง ๆ ได้โดยไม่ต้องเปิดเผยข้อมูลต้นฉบับ สิ่งนี้ทำให้มั่นใจได้ถึงการปกป้องความเป็นส่วนตัวที่แข็งแกร่ง

กระบวนการสร้างที่อยู่แฮช ดังรูปที่ 3.20 เป็นเทคนิคการทำให้ข้อมูลเป็นนิรนามที่ใช้ฟังก์ชันแฮชที่เข้ารหัส SHA-256 เพื่อสร้างค่าแฮชที่ไม่ซ้ำกันและไม่สามารถย้อนกลับได้สำหรับแต่ละแถวในชุดข้อมูล กระบวนการเริ่มต้นด้วยการนำเข้าไลบรารีที่จำเป็นรวมถึง pandas และ hashlib ฟังก์ชันที่ใช้กำหนดเองคือ “Generate_hash” ได้รับการกำหนดให้แปลงแต่ละแถวเป็นสตริง เข้ารหัส และใช้อัลกอริทึม SHA-256 โดยส่งคืนแฮชเลขฐานสิบหกที่ไม่ซ้ำกันสำหรับเนื้อหาของแถวหลังจากโหลดชุดข้อมูล (รวมถึงข้อมูลแฝงจากขั้นตอนก่อนหน้า) ฟังก์ชันแฮชจะถูกนำไปใช้กับแต่ละแถว โดยเพิ่มคอลัมน์แฮชใหม่ลงในชุดข้อมูล คอลัมน์นี้แสดงถึงแต่ละแถวโดยไม่ซ้ำ

กันด้วยวิธีที่ปลอดภัยและไม่สามารถย้อนกลับได้ จากนั้นชุดข้อมูลที่มีการปรับปรุงจะถูกบันทึกเป็นไฟล์ใหม่ชื่อ “adult_pii_pseudonym_hash.csv” เพื่อใช้งานต่อไป วิธีการนี้ช่วยเพิ่มความปลอดภัยของข้อมูลโดยการไม่ระบุชื่อทั้งแถวในขณะที่ยังคงรักษาความสมบูรณ์สำหรับการวิเคราะห์หรือการเชื่อมโยงโดยไม่เปิดเผยรายละเอียดที่ละเอียดอ่อน

```python
import pandas as pd
import hashlib

def generate_hash(row):
    """Generate SHA-256 hash for a given row of data."""
    row_string = row.to_string(header=False, index=False)
    hash_object = hashlib.sha256(row_string.encode())
    return hash_object.hexdigest()

# Load the dataset
#file_path = '/path/to/your/file.csv'
data = pd.read_csv('adult_pii_pseudonym.csv')

# Apply the hash function to each row
data['Hash'] = data.apply(generate_hash, axis=1)

# Save the updated DataFrame back to a CSV (optional)
data.to_csv('adult_pii_pseudonym_hash.csv', index=False)

data.head()
```

	Pseudonym_ID	Hash	Name	DOB
0	GV69daktNi	ceacb309adbd1dbcff85df4e050a95704fbdde41014f29...	Jamill Elphey	4/3/2004
1	WflMSma1GS	ddc805df0042f37c1eaf76ad025f17833d8b3e22be717e...	Lenette Summerson	2/8/1962
2	mENJQ8Kxjc	3e9e620dd337dc2a6eec573f8ac41815771ed3ae5db5b6...	Sigrid Addington	1/8/2007
3	vpx6m9VpqO	79779086325954324ae42c5ccb44f86cd118eef1579cb2...	Appolonia Winear	4/11/1987

รูปที่ 3.20 แสดงการสร้างที่อยู่แฮช

3.3.2.3 ขั้นตอนที่ 3 การแบ่งส่วนข้อมูล:

การแบ่งส่วนข้อมูลเป็นกระบวนการจัดหมวดหมู่ชุดข้อมูลออกเป็นกลุ่มเล็ก ๆ ที่มีความหมายหรือตามลักษณะเฉพาะ แนวทางนี้ใช้กันอย่างแพร่หลายในการจัดการข้อมูล การวิเคราะห์ และแนวปฏิบัติด้านความเป็นส่วนตัวเพื่อปรับปรุงการจัดระเบียบข้อมูล ปรับปรุง การวิเคราะห์ และรับประกันการปฏิบัติตามกฎระเบียบการปกป้องข้อมูล เช่น จีดีพีอาร์หรือพีดีพีเอ ด้วยการจัดกลุ่มข้อมูลตามความอ่อนไหวและศักยภาพในการระบุตัวตน การแบ่งส่วนช่วยให้สามารถกำหนดมาตรการรักษาความปลอดภัยและการควบคุมความเป็นส่วนตัว จำแนกหมวดหมู่หลัก ได้ดังนี้

1) ข้อมูลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information – PII): ซึ่งรวมถึงข้อมูลที่ระบุตัวบุคคลโดยตรง เช่น ชื่อ หมายเลขประกันสังคม วันเกิด หรือที่อยู่อีเมล PII เป็นข้อมูลที่ละเอียดอ่อนที่สุดและมักอยู่ภายใต้กฎระเบียบที่เข้มงวด การปกป้อง PII เป็นสิ่งสำคัญในการป้องกันการโจรกรรมข้อมูลส่วนบุคคลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

2) ข้อมูลตัวระบุโดยตรง (Direct Identifier Data): หมวดหมู่ย่อยของ PII ประกอบด้วยข้อมูลที่ระบุตัวบุคคลได้อย่างชัดเจนและไม่ซ้ำกัน เช่น หมายเลขประกันสังคม หมายเลขหนังสือเดินทาง หรือหมายเลขโทรศัพท์ โดยทั่วไปตัวระบุโดยตรงจะถูกลบออก ใช้ข้อมูลแฝงหรือเข้ารหัสเพื่อปกป้องความเป็นส่วนตัว

3) ข้อมูลตัวระบุเสมือน (Quasi-Identifier Data): หมวดหมู่นี้ประกอบด้วยตัวระบุทางอ้อม เช่น อายุ เพศ รหัสไปรษณีย์ หรืออาชีพ แม้ว่าจะไม่เปิดเผยทันที แต่เมื่อรวมกับตัวระบุเสมือนหรือชุดข้อมูลอื่น ๆ ข้อมูลนี้สามารถระบุตัวบุคคลได้อีกครั้ง

4) ข้อมูลที่ไม่สามารถระบุตัวตนได้ (Non-Identifiable Data): ข้อมูลในหมวดหมู่นี้ไม่สามารถใช้ระบุตัวบุคคลได้ ตัวอย่างเช่น สถิติที่ไม่ระบุชื่อ ข้อมูลรวมหรือผลการวิจัยที่ไม่ระบุตัวตน ข้อมูลที่ไม่สามารถระบุตัวตนได้ถือว่ามีความเสี่ยงต่ำและมักได้รับการยกเว้นจากกฎระเบียบด้านความเป็นส่วนตัวที่เข้มงวด

จากรูปที่ 3.21 แสดงกระบวนการแบ่งส่วนข้อมูลโดยละเอียดที่ออกแบบมาเพื่อจัดการข้อมูลที่ละเอียดอ่อนและไม่ละเอียดอ่อนอย่างปลอดภัยและมีประสิทธิภาพ เริ่มต้นด้วยการโหลดชุดข้อมูล “adult_pii_pseudonym_hash.csv” ที่มีข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลที่สามารถตัวบุคคลได้ (PII) คอลัมน์ที่ไม่ระบุตัวตน ตัวระบุเสมือน และข้อมูลที่ไม่ละเอียดอ่อน คอลัมน์ในชุดข้อมูลแบ่งออกเป็น 4 กลุ่มที่แตกต่างกันคือ (1) คอลัมน์ PII ซึ่งรวมถึงตัวระบุโดยตรงเช่น Name, DOB, SSN, และ Zip ที่ระบุตัวบุคคลโดยไม่ซ้ำกันและมีความละเอียดอ่อนสูง (2) ตัวระบุ เช่น pseudonyms หรือ hash values ซึ่งใช้เพื่อแทนที่ตัวระบุที่ละเอียดอ่อน ในขณะที่ยังคงรักษาความสมบูรณ์ของชุดข้อมูลสำหรับการวิเคราะห์ (3) ตัวระบุเสมือน เช่น Age, Sex, Education และ Occupation ที่ไม่ใช้ตัวระบุโดยตรงแต่อาจเปิดเผยตัวตนของบุคคลเมื่อรวมกับข้อมูลอื่น ๆ และ (4) คอลัมน์ที่ไม่ละเอียดอ่อนซึ่งมีข้อมูลทั่วไปหรือข้อมูลรวม เช่น fnlwgt, Capital Gain และ Target จะถูกบันทึกเป็นไฟล์ csv แยกต่างกัน (pii_data_anonymized_csv, deid_data_generalized.csv, qi_data_generalized.csv และ “non_pii_data.csv”) เพื่อการจัดเก็บและการประมวลผลที่ปลอดภัย นอกจากนี้ยังเอาที่แบ่งส่วนทั้งหมดรวมกันใหม่เป็นการประมวลผลเดียวและบันทึกเป็นไฟล์ใหม่ชื่อ “processed_data.csv” เพื่อการวิเคราะห์เพิ่มเติม มีการรวมขั้นตอนการทำงานทางเลือกที่จะลบคอลัมน์ PII ออกจากชุดข้อมูล ทั้งหมด และบันทึกข้อมูลที่

ผ่านขั้นตอนแล้วเป็นไฟล์ชื่อ “adult_without_pii.csv” วิธีการแบ่งส่วนนี้สนับสนุนการปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัว เช่น จีดีพีอาร์และพีดีพีเอ โดยการแยกข้อมูลที่ละเอียดอ่อนและลดความเสี่ยงในการระบุตัวตนซ้ำ

```python
import pandas as pd

# Assuming the file has been successfully uploaded and is named 'adult_pii_new2.csv'
data = pd.read_csv('adult_pii_pseudonym_hash.csv')

# Direct identifiers
pii_columns = ['Name', 'DOB', 'SSN', 'Zip']
# De-identifiers
deid_columns = ['Pseudonym_ID', 'Hash']
# Quasi-identifiers that can be used in linkage attacks
qi_columns = [
    'Age', 'Workclass','Education', 'Education-Num', 'Marital Status', 'Occupation',
    'Relationship', 'Race', 'Sex' , 'Country']
# Non-sensitive information
non_pii_columns = ['fnlwgt', 'Capital Gain', 'Capital Loss', 'Hours per week', 'Target']

# Create DataFrames for each type of data
pii_data = data[pii_columns]
deid_data = data[deid_columns]
qi_data = data[qi_columns]
non_pii_data = data[non_pii_columns]

# Save the segregated data
pii_data.to_csv('pii_data_anonymized.csv', index=False)
deid_data.to_csv('deid_data_generalized.csv', index=False)
qi_data.to_csv('qi_data_generalized.csv', index=False)
non_pii_data.to_csv('non_pii_data.csv', index=False)

# Or combine them back into one DataFrame and save
processed_data = pd.concat([pii_data, deid_data, qi_data, non_pii_data], axis=1)
processed_data.to_csv('processed_data.csv', index=False)
```

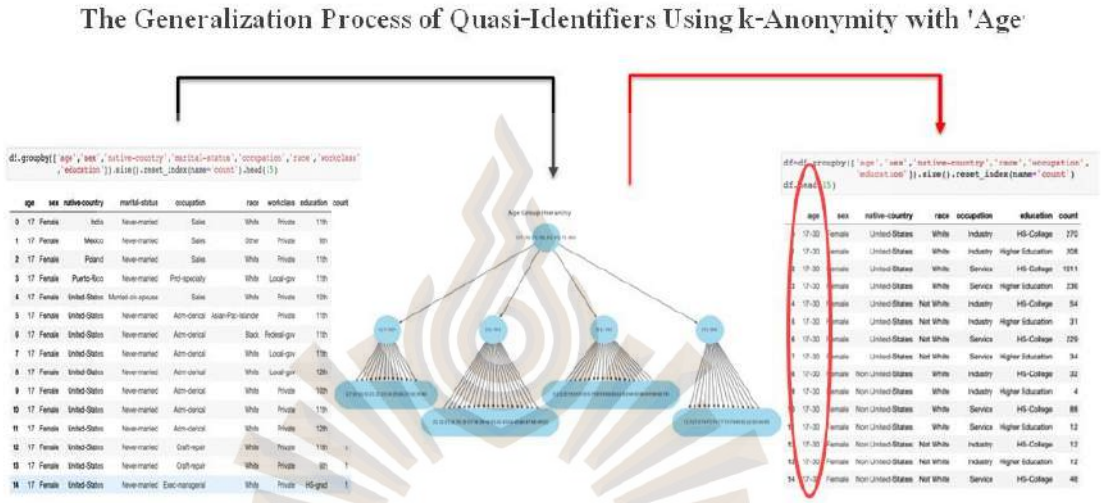
```python
import pandas as pd

# Assuming the file has been successfully uploaded and is named 'adult_pii_new2.csv'
non_pii_data = pd.read_csv('adult_pii_pseudonym_hash.csv')
non_pii_data.drop(['Name', 'DOB', 'SSN', 'Zip'], axis=1, inplace=True)

# Saving output to csv file
non_pii_data.to_csv('adult_without_pii.csv', index=False)
```

รูปที่ 3.21 แสดงกระบวนการแบ่งส่วนข้อมูล

3.3.2.4 ขั้นตอนที่ 4 ทำให้ตัวระบุเสมือนเป็นลักษณะทั่วไปด้วย k-Anonymity:

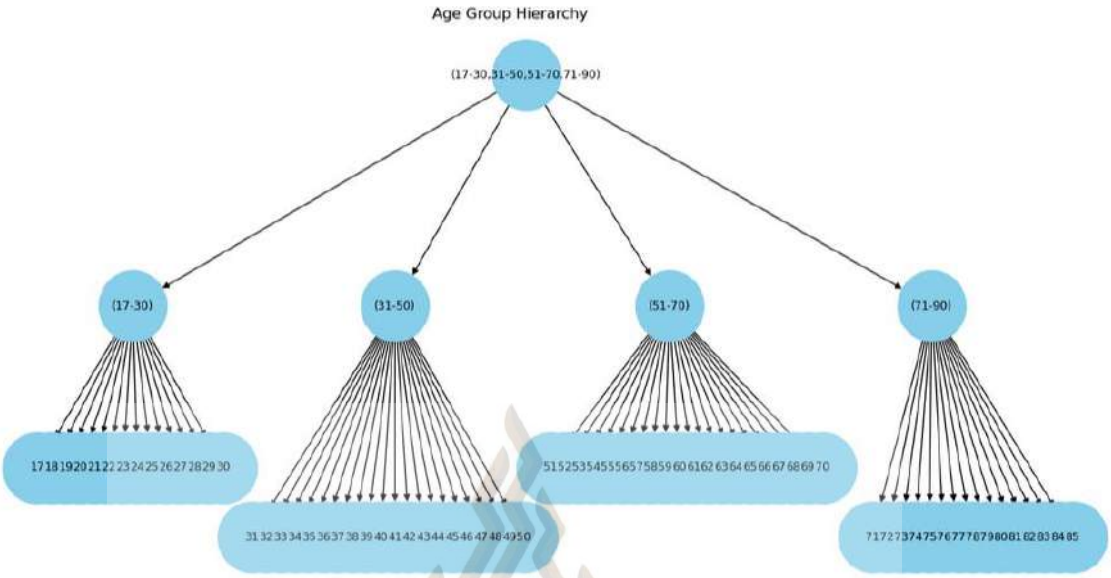
ขั้นตอนนี้เป็นเทคนิคการทำให้ข้อมูลเป็นนิรนามที่สำคัญซึ่งรับประกันความเป็นส่วนตัวของบุคคลในชุดข้อมูลโดยการแก้ไขตัวระบุเสมือน ซึ่งเป็นคุณลักษณะเช่น Age, Sex หรือ ZIP ที่สามารถระบุตัวบุคคลทางอ้อมได้ วิธีการนี้รับประกันได้ว่าแต่ละรายการในชุดข้อมูลจะแยกไม่ออกจากรายการอื่น ๆ อย่างน้อย “k” ตามคุณลักษณะเหล่านี้ ซึ่งก่อตัวเป็นกลุ่มที่ไม่เปิดเผยตัวตน เพื่อให้บรรลุเป้าหมายตัวระบุเสมือนจึงได้รับการสรุปหรือจัดกลุ่มเป็นหมวดหมู่ที่กว้างขึ้นและ

เจาะจงน้อยลง ตัวอย่างเช่น อายุที่แน่นอน อาจถูกสรุปเป็นช่วงอายุเช่น 20-30 หรือ 30-40 วิธีการนี้จะลดรายละเอียดลงในขณะที่ยังคงรักษาค่าการวิเคราะห์ของข้อมูลไว้ ด้วยเทคนิค k-Anonymity ชุดข้อมูลสามารถรักษาอรรถประโยชน์สำหรับการวิเคราะห์ ในขณะเดียวกันก็ลดความเสี่ยงในการเปิดเผยตัวตนของแต่ละบุคคลผ่านตัวระบุทางอ้อม ดังรูปที่ 3.22

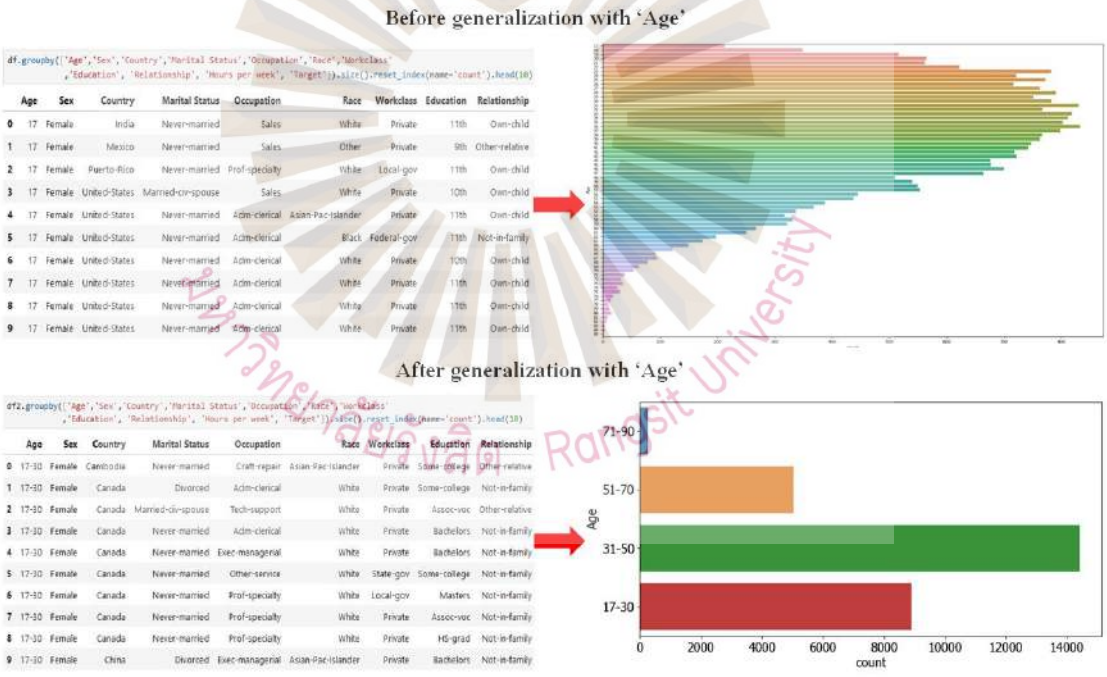


รูปที่ 3.22 กระบวนการทำให้ตัวระบุเสมือนเป็นลักษณะทั่วไปโดยใช้ k-Anonymity กับ ‘อายุ’

กระบวนการทำให้ตัวระบุเสมือนเป็นลักษณะทั่วไปโดยใช้ k-Anonymity กับ ‘อายุ’ ช่วยให้มั่นใจในความเป็นส่วนตัวโดยการจัดกลุ่มค่าอายุที่เฉพาะเจาะจงออกเป็นหมวดหมู่ที่กว้างขึ้น ช่วยลดความเสี่ยงของการระบุตัวตนซ้ำในขณะที่ยังคงรักษาอรรถประโยชน์ข้อมูลไว้ ดังรูปที่ 3.23 ‘อายุ’ จะแสดงตามลำดับชั้น โดยระดับบนสุดแสดงช่วงอายุกว้าง ๆ 4 ช่วง (17-30, 31-50, 51-70 และ 71-90) ช่วงเหล่านี้จะแบ่งย่อยออกเป็นแต่ละช่วงอายุในระดับล่าง เช่น อายุ 17-30 ปี จะถูกขยายเป็นค่าเฉพาะ (เช่น 17, 18, 19) กระบวนการนี้เริ่มต้นด้วยการระบุ ‘Age’ เป็นตัวระบุเสมือนและใช้กฎเพื่อให้แน่ใจว่าแต่ละกลุ่มอายุมีบุคคลอย่างน้อย k คน หากค่าอายุไม่ตรงตามเกณฑ์นี้ ค่าต่าง ๆ จะถูกกำหนดให้เป็นช่วงที่กว้างขึ้นเพื่อรักษาสมดุลระหว่างความเป็นส่วนตัวและรายละเอียดของข้อมูล การรวมกลุ่มนี้ป้องกันไม่ให้ผู้โจมตีแยกบุคคลตามอายุที่ไม่ซ้ำกัน ในขณะที่ยังคงให้การวิเคราะห์ที่มีความหมายภายในชุดข้อมูล อย่างไรก็ตามมีข้อเสียระหว่างความเป็นส่วนตัวและอรรถประโยชน์: ลักษณะทั่วไปที่สูงขึ้นจะช่วยเพิ่มความเป็นส่วนตัวแต่ลดความแม่นยำของข้อมูล ในขณะที่ลักษณะทั่วไปที่ต่ำกว่ายังคงรักษาข้อมูลเชิงลึกโดยละเอียดแต่เพิ่มความเสี่ยงด้านความเป็นส่วนตัว



รูปที่ 3.23 การทำให้ตัวระบุเสมือนเป็นลักษณะทั่วไปโดยใช้ k-Anonymity กับ ‘อายุ’



รูปที่ 3.24 การกระจายของ ‘อายุ’ ก่อนและหลังทำให้เป็นลักษณะทั่วไป

จากรูปที่ 3.24 เป็นภาพรวมเชิงลึกเกี่ยวกับลักษณะทั่วไปของแอตทริบิวต์ ‘อายุ’ ก่อนและหลังการเปลี่ยนแปลง แสดงให้เห็นถึงการประยุกต์ใช้ k-Anonymity กับ แอตทริบิวต์ ‘อายุ’ ในชุดข้อมูล ซึ่งแสดงให้เห็นว่าค่าอายุถูกแปลงเป็นช่วงอายุที่กว้างขึ้นเพื่อปรับปรุงความเป็นส่วนตัวอย่างไร ด้วยการสรุปอายุที่เฉพาะเจาะจงให้เป็นช่วงเวลา กระบวนการนี้จะช่วยลดความเสี่ยง

ในการระบุตัวบุคคลในขณะที่ยังคงรักษาค่าการวิเคราะห์ของชุดข้อมูลไว้ การเปรียบเทียบเน้นย้ำถึงการเปลี่ยนแปลงเชิงโครงสร้างและภาพในข้อมูลก่อนและหลังการทำให้เป็นภาพรวม โดยเน้นความสมดุลระหว่างการปกป้องข้อมูลที่ละเอียดอ่อนและการรักษาความสามารถในการใช้งานสำหรับการวิเคราะห์ สามารถอธิบายรายละเอียดก่อนและหลังทำเป็นลักษณะทั่วไปของแอตทริบิวต์ 'อายุ' ดังนี้

1) ก่อนทำเป็นลักษณะทั่วไป: ชุดข้อมูลจะแสดงค่า 'อายุ' ที่เป็นข้อมูลดิบและมีความเฉพาะเจาะจงสูง เช่น 17, 18, 19, 20 ควบคู่ไปกับตัวระบุเสมือนอื่น ๆ เช่น เพศ ประเทศ สถานภาพการสมรส อาชีพ และชนชั้นแรงงาน แผนภูมิแท่งแสดงแต่ละช่วงอายุเป็นแถบแนวนอนแยกกัน โดยเน้นรายละเอียดที่ละเอียดและความแม่นยำของข้อมูล แม้ว่ารายละเอียดระดับนี้จะมีคุณค่าสำหรับการวิเคราะห์ระดับจุลภาคและข้อมูลเชิงลึกที่แม่นยำ แต่ก็ยังเพิ่มความเสี่ยงในการระบุตัวตนซ้ำได้อย่างมาก ค่าอายุที่ไม่ซ้ำหรือค่าอายุที่หายาก เมื่อรวมกับตัวระบุเสมือนอื่น ๆ อาจเปิดเผยตัวตนของบุคคล ซึ่งเป็นการละเมิดกฎระเบียบด้านความเป็นส่วนตัว เช่น จีดีพีอาร์และพีดีพีเอ แม้ว่าชุดข้อมูลจะมีรายละเอียดมากมายและมีข้อมูลสูงแต่ก็ไม่เป็นไปตามมาตรฐาน k-Anonymity ซึ่งกำหนดให้แต่ละคนต้องแชร์แอตทริบิวต์กับผู้อื่นอย่างน้อย k-1 ด้วยเหตุผลนี้ แม้ว่าจะแม่นยำแต่การนำเสนอ 'อายุ' แบบดิบนี้ทำให้เกิดช่องโหว่ด้านความเป็นส่วนตัว โดยเฉพาะอย่างยิ่งในชุดข้อมูลที่มีขนาดเล็กกว่าขนาดตัวอย่างหรือกลุ่มประชากรเฉพาะ

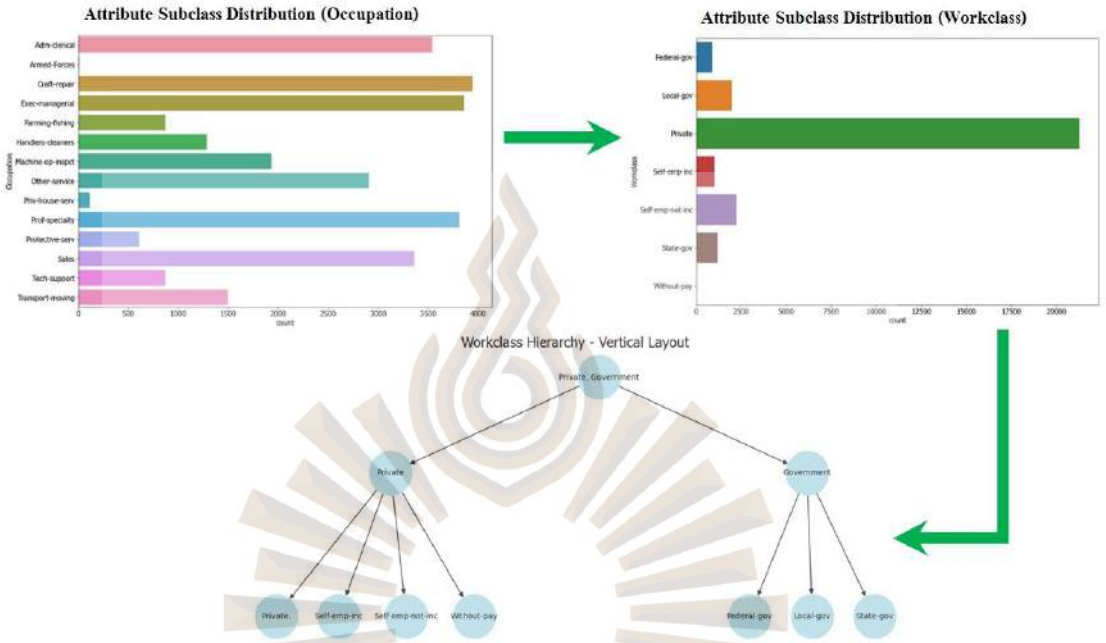
2) หลังทำเป็นลักษณะทั่วไป: ค่า 'อายุ' แต่ละรายการจะถูกแทนที่ด้วยช่วงอายุที่กว้างขึ้น เช่น 17-30, 31-50, 51-70 และ 71-90 การเปลี่ยนแปลงนี้จะลดความละเอียดของข้อมูลโดยจัดกลุ่มบุคคลเป็นหมวดหมู่ที่ใหญ่ขึ้นและกว้างขึ้น ขณะเดียวกันก็รักษาตัวระบุเสมือนอื่น ๆ เช่น เพศ ประเทศ สถานภาพการสมรส อาชีพ และชนชั้นแรงงาน แผนภูมิแท่งสะท้อนถึงกลุ่มอายุทั่วไปเหล่านี้โดยรวมแท่งแต่ละแท่งออกเป็นส่วนที่น้อยลงและใหญ่ขึ้นซึ่งแสดงถึงช่วงอายุรวม กระบวนการนี้ทำให้แน่ใจได้ถึงการปฏิบัติตาม k-Anonymity เนื่องจากแต่ละกลุ่มอายุมีบุคคลอย่างน้อย k คน ซึ่งช่วยลดความเสี่ยงในการระบุตัวตนซ้ำได้อย่างมาก แม้ว่าความแม่นยำของข้อมูลบางส่วนจะลดลง แต่ชุดข้อมูลยังคงรักษาค่าการวิเคราะห์ไว้สำหรับการศึกษาข้อมูลประชากรระดับมหภาคและข้อมูลเชิงลึกทางสถิติ การแลกเปลี่ยนระหว่างความเป็นส่วนตัวและอรรถประโยชน์ทำให้มั่นใจได้ว่าจะปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัว เช่น จีดีพีอาร์และพีดีพีเอ ทำให้สามารถแบ่งปันข้อมูลได้อย่างปลอดภัยและมีความรับผิดชอบ การทำให้เป็นลักษณะทั่วไปกลายเป็นกลยุทธ์การทำให้ไม่เปิดเผยตัวตนที่สำคัญโดยสร้างความสมดุลระหว่างการปกป้องความเป็นส่วนตัวและการใช้งานข้อมูลทั่วทั้งโดเมนการวิจัย การดูแลสุขภาพ และการวิเคราะห์

3.3.2.5 ขั้นตอนที่ 5 การกระจายคลาสย่อยของแอตทริบิวต์:

ขั้นตอนนี้เป็นการแสดงทางสถิติของหมวดหมู่หรือกลุ่มย่อยต่าง ๆ ภายในแอตทริบิวต์ชุดข้อมูลเฉพาะ เช่น อาชีพหรือการศึกษา โดยเน้นย้ำถึงวิธีการกระจายจุดข้อมูลระหว่างคลาสย่อย การเปิดเผยรูปแบบ ความไม่สมดุล และแนวโน้ม เครื่องมือแสดงภาพ (เช่น แผนภูมิแท่งและแผนภูมิวงกลม) ช่วยแสดงการแจกแจงเหล่านี้เพื่อความชัดเจนยิ่งขึ้น การวิเคราะห์นี้มีความสำคัญอย่างยิ่งต่อการระบุหมวดหมู่ที่มีการนำเสนอมากเกินไปหรือน้อยเกินไป การตรวจจับค่าผิดปกติ และรับประกันการนำเสนอที่สมดุลในแบบจำลองการเรียนรู้ของเครื่อง นอกจากนี้ยังสนับสนุนเทคนิคการรักษาความเป็นส่วนตัว เช่น k-Anonymity โดยการจัดการคลาสย่อยที่มีประชากรกระจัดกระจาย ลดความเสี่ยงในการระบุตัวตนซ้ำ และดูแลรักษาอรรถประโยชน์ข้อมูลสำหรับการวิเคราะห์และการตัดสินใจ

1) การกระจายคลาสย่อยของแอตทริบิวต์ ‘คลาสงาน’: รูปที่ 3.25 แสดงให้เห็นว่าข้อมูลอาชีพแบบละเอียดสามารถรวมเป็นหมวดหมู่ที่กว้างขึ้นได้อย่างไร โดยใช้เทคนิคการทำเป็นลักษณะทั่วไปเพื่อให้ได้ k-Anonymity ขณะเดียวกันก็รักษาสมดุลของความเป็นส่วนตัวของข้อมูลและอรรถประโยชน์ แผนภูมิแท่งแนวนอนด้านซ้ายบนแสดงคลาสย่อยโดยละเอียดของอาชีพ เช่น Adm-clerical, Exec-managerial, Craft-repair, Armed-Forces, Sales, Tech-support และ Transport-moving โดยมีจำนวนแสดงการกระจายตัวในชุดข้อมูล หมวดหมู่บางหมวดหมู่ เช่น Exec-managerial และ Other-service มีตัวแทนที่สูงกว่า ในขณะที่กลุ่มเล็ก ๆ เช่น Farming-fishing และ Armed-Forces มีความเสี่ยงในการระบุตัวตนซ้ำสูงกว่าเนื่องจากมีเอกลักษณ์เฉพาะ เป็นแผนภูมิแท่งแนวตั้งด้านขวาบนจะรวมอาชีพเหล่านี้ไว้ในหมวดหมู่ชนชั้นแรงงานที่กว้างขึ้น ได้แก่ Private, Self-emp-inc, Self-emp-not-inc, Federal-gov, State-gov และ Without-pay หมวดหมู่เอกชนมีความโดดเด่นโดยมีตัวแทนสูงสุด ในขณะที่กลุ่มเล็ก ๆ เช่น Without-pay และ State-gov แสดงตัวแทนที่ต่ำกว่าอย่างเห็นได้ชัด ลักษณะทั่วไปนี้ลดรายละเอียดและปรับปรุงการปกป้องความเป็นส่วนตัวในขณะที่ยังคงความสามารถในการใช้งานสำหรับการวิเคราะห์ระดับมหภาค แผนภาพต้นไม้ลำดับชั้นด้านล่างยังแบ่งหมวดหมู่ระดับงานเหล่านี้ออกเป็นโครงสร้างที่ชัดเจน ลำดับชั้นนี้สนับสนุนกระบวนการทำเป็นลักษณะทั่วไปโดยผสานคลาสย่อยที่มีขนาดเล็กลงและมีความเสี่ยงเป็นกลุ่มที่กว้างขึ้น (เช่น เอกชนหรือภาครัฐ) เพื่อให้มั่นใจว่าสอดคล้องกับมาตรฐาน k-Anonymity และป้องกันการระบุตัวตนซ้ำ แม้ว่าการทำเป็นลักษณะทั่วไปจะเสียสละความแม่นยำของข้อมูลบางส่วน แต่จะรักษาข้อมูลเชิงลึกที่สำคัญสำหรับแนวโน้มทางประชากรศาสตร์ การวิเคราะห์กำลังคน และการวางแผนนโยบาย กระบวนการนี้สร้าง

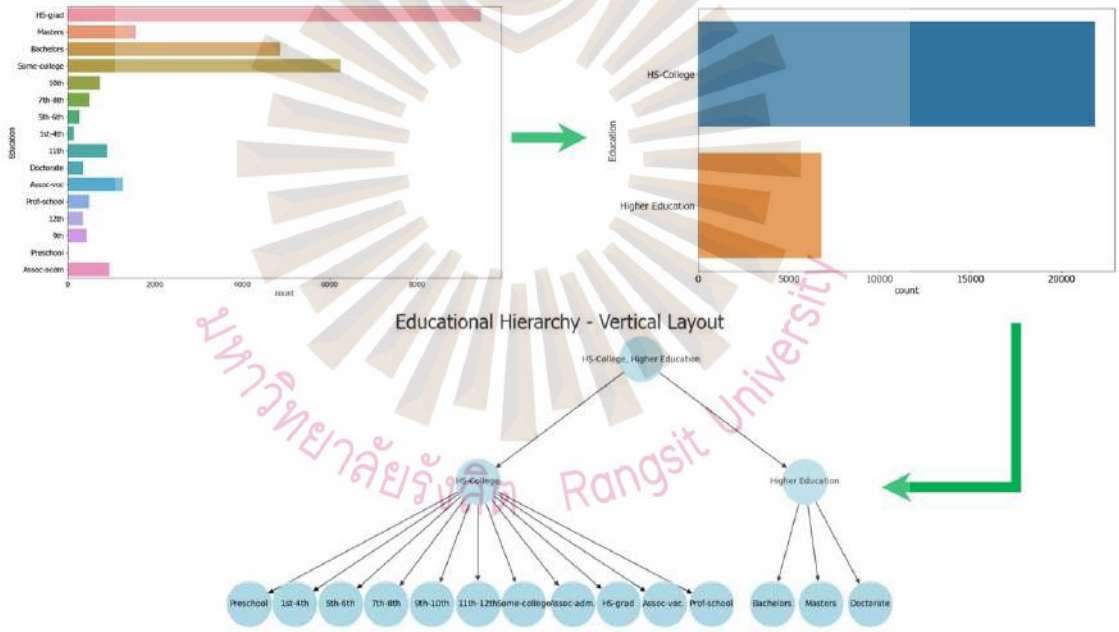
ความสมดุลระหว่างความเป็นส่วนตัวด้วยอรรถประโยชน์ข้อมูล ซึ่งสอดคล้องกับกฎระเบียบด้านความเป็นส่วนตัว เช่น จีดีพีอาร์และพีดีพีเอ ทำให้ชุดข้อมูลมีความปลอดภัยสำหรับการแบ่งปันและการวิเคราะห์ในภาคส่วนต่าง ๆ เช่น การดูแลสุขภาพ การวิจัย และรายงานของรัฐบาล



รูปที่ 3.25 การกระจายคลาสย่อยของแอตทริบิวต์ ‘คลาสงาน’

2) การกระจายคลาสย่อยของแอตทริบิวต์ ‘การศึกษา’: รูปที่ 3.26 ซึ่งแสดงให้เห็นว่าข้อมูลการศึกษาโดยละเอียดสามารถสรุปเป็นหมวดหมู่ที่กว้างขึ้นได้อย่างไรเพื่อให้บรรลุถึง k-Anonymity โดยรับประกันการปกป้องความเป็นส่วนตัวในขณะที่ยังรักษาอรรถประโยชน์ข้อมูลไว้ แผนภูมิแท่งแนวนอนด้านซ้ายบนจะแสดงระดับการศึกษาแบบละเอียด เช่น HS-grad, Some-college, Bachelors, Masters, Doctorate, Assoc-voc, Assoc-acdm, Prof-school และ Preschool พร้อมด้วยหมวดหมู่เกรดเฉพาะ เช่น 1^{st}-4^{th}, 5^{th}-6^{th}, 7^{th}-8^{th}, 9^{th}-10^{th} และ 11^{th}-12^{th} หมวดหมู่ต่าง ๆ เช่น HS-grad และ Some-college มีความแพร่หลายอย่างมากในชุดข้อมูลในขณะที่กลุ่มที่พบได้น้อยกว่า เช่น Doctorate และ Preschool มีความเสี่ยงในการระบุตัวตนซ้ำได้สูงกว่าเนื่องจากมีเอกลักษณ์เฉพาะตัว ในแผนภูมิแท่งแนวตั้งด้านขวาบนจะแสดงให้เห็นว่าระดับการศึกษาโดยละเอียดเหล่านี้จะรวมกันเป็นกลุ่มระดับ ที่สูงกว่าสองกลุ่มคือ HS-College และ Higher-Education กลุ่ม HS-College ประกอบด้วยผู้สำเร็จการศึกษาระดับมัธยมปลาย ผู้สำเร็จการศึกษาระดับวิทยาลัย และผู้สำเร็จการศึกษาระดับอนุปริญญา ในขณะที่กลุ่ม Higher-Education ครอบคลุมระดับปริญญาตรี โท เอก และศาสตราจารย์ การรวมกลุ่มนี้ลดรายละเอียดลง เพิ่มประสิทธิภาพการปกป้องความเป็นส่วนตัวในขณะ

ที่ยังคงรักษาการวิเคราะห์ข้อมูลเชิงลึกที่มีความหมายไว้ แผนภาพต้นไม้ลำดับชั้นด้านล่างแสดงภาพกระบวนการทำเป็นลักษณะทั่วไปเพิ่มเติม โดยแบ่งการศึกษาออกเป็นสองกลุ่มหลัก คือ HS-College และ Higher Education มีการแจกแจงข้อมูลในแต่ละกลุ่มอย่างละเอียด ลำดับชั้นที่มีโครงสร้างนี้สนับสนุนกระบวนการทำเป็นลักษณะทั่วไป โดยรวบรวมกลุ่มเล็ก ๆ ที่มีความเสี่ยงให้เป็นหมวดหมู่ที่ใหญ่ขึ้น เพื่อให้มั่นใจว่าสอดคล้องกับมาตรฐาน k-Anonymity และความเสี่ยงในการระบุตัวตนซ้ำให้เหลือน้อยที่สุด แม้ว่าความแม่นยำจะลดลงแต่ข้อมูลเชิงลึกที่มีความหมายเกี่ยวกับแนวโน้มทางการศึกษาจะยังคงอยู่ โดยคงคุณค่าของชุดข้อมูลไว้สำหรับการวิเคราะห์ทางประชากรศาสตร์ การวางแผนนโยบาย และการวิจัยทางสถิติ การทำเป็นลักษณะทั่วไปนี้ทำให้เกิดความสมดุลระหว่างความเป็นส่วนตัวของข้อมูลและอรรถประโยชน์ โดยรับประกันการปฏิบัติตามกฎระเบียบด้านความเป็นส่วนตัว เช่น จีดีพีอาร์และพีดีพีเอ ขณะเดียวกันก็อนุญาตให้ชุดข้อมูลยังคงมีคุณค่าในการวิเคราะห์สำหรับภาคส่วนต่าง ๆ



รูปที่ 3.26 การกระจายคลาสย่อยของแอตทริบิวต์ ‘การศึกษา’

ชุดคำสั่งในรูปที่ 3.27 มุ่งเน้นไปที่การจัดทำดัชนี การแบ่งพาร์ติชัน และการจัดกลุ่มข้อมูลหมวดหมู่ใหม่ภายในชุดข้อมูล สำหรับงานต่าง ๆ เช่น ข้อมูลนิรนาม การจัดกลุ่ม และการแสดงภาพแบบมีโครงสร้าง ฟังก์ชัน re_indexes จะจับคู่ค่าหมวดหมู่ที่ไม่ซ้ำกับดัชนีจำนวนเต็มเพื่อความสอดคล้องและการจัดการข้อมูลได้ง่ายขึ้น ฟังก์ชัน gether_new ปรับและจัดระเบียบพาร์ติชันใหม่แบบไดนามิกโดยใช้ออฟเซ็ต เพื่อให้มั่นใจว่ามีการจัดกลุ่มที่ชัดเจนและเป็นตรรกะ ฟังก์ชัน

regroup_main จะประมวลผลพาร์ติชันเหล่านี้ซ้ำ ๆ โดยใช้การปรับออฟเซ็ตส่วนเพิ่ม เพื่อรักษาความชัดเจนในการแสดงภาพหรือเค้าโครง และฟังก์ชัน equal_attributes จะรวมกระบวนการเหล่านี้เข้าด้วยกันโดยการจัดทำดัชนีใหม่และจัดกลุ่มแอตทริบิวต์ตัวระบุเสมือนใหม่ เพื่อให้มั่นใจว่ามีการแบ่งพาร์ติชันที่มีโครงสร้างและการจัดแนวทั่วทั้งชุดข้อมูล แนวทางนี้สร้างความสมดุลระหว่างการรักษาความเป็นส่วนตัวและอรรถประโยชน์ข้อมูล เพื่อให้มั่นใจว่ามีการจัดการองค์กรที่ชัดเจนและการแสดงโครงสร้างข้อมูลแบบลำดับชั้นหรือแบบแบ่งพาร์ติชันอย่างมีประสิทธิภาพ

```
def re_indexes(df):
    indexes = {}
    for column in categorical:
        values = sorted(df[column].unique())
        indexes[column] = { x : y for x, y in zip(values, range(len(values)))}
    return indexes

def gether_new(df, column, partition, indexes, offset=0.1):
    if column in categorical:
        sv = df[column][partition].sort_values()
        l, r = indexes[column][sv[sv.index[0]]], indexes[column][sv[sv.index[-1]]]+1.0
    else:
        sv = df[column][partition].sort_values()
        next_value = sv[sv.index[-1]]
        larger_values = df[df[column] > next_value][column]
        if len(larger_values) > 0:
            next_value = larger_values.min()
        l = sv[sv.index[0]]
        r = next_value
    # we add some offset to make the partitions more easily visible
    l -= offset
    r += offset
    return l, r

def regroup_main(df, partitions, column_x, column_y, indexes, offsets=[0.1, 0.1]):
    rects = []
    for partition in partitions:
        xl, xr = gether_new(df, column_x, partition, indexes, offset=offsets[0])
        yl, yr = gether_new(df, column_y, partition, indexes, offset=offsets[1])
        rects.append(((xl, yl),(xr, yr)))
    return rects

# Regroup all quasi-attributes
indexes = re_indexes(df)
column_x, column_y = feature_columns[:2]
rects = regroup_main(df, finished_partitions, column_x, column_y, indexes, offsets=[0.0, 0.0])
```

รูปที่ 3.27 แสดงชุดคำสั่งการจัดกลุ่มแอตทริบิวต์ตัวระบุเสมือนใหม่

3.3.2.6 ขั้นตอนที่ 6 การกระจายของแอตทริบิวต์เสมือน:

จะแสดงการกระจายตัวหรือการกระจุกตัวของข้อมูลในแอตทริบิวต์ที่ไม่สามารถระบุตัวตนได้โดยตรง แต่สามารถใช้ร่วมกับข้อมูลอื่นเพื่อระบุตัวตนบุคคลได้ การกระจายของแอตทริบิวต์เสมือนมีบทบาทสำคัญในการประเมินความเสี่ยงในการระบุตัวตนของข้อมูลบุคคล กระบวนการนี้ช่วยรักษาสมดุลระหว่างการรักษาความปลอดภัยของข้อมูลและคงไว้ซึ่งประสิทธิภาพในการวิเคราะห์ข้อมูล ทำให้มั่นใจได้ว่าชุดข้อมูลมีความปลอดภัยสำหรับการเผยแพร่และการใช้งานต่อไป จากรูปที่ 3.22 แสดงภาพรวมของชุดข้อมูลที่ผ่านการประยุกต์ใช้เทคนิค k-Anonymity ซึ่งเป็นเทคนิคสำคัญในการปกป้องความเป็นส่วนตัวของข้อมูล ขณะเดียวกันก็ยังคงรักษาประโยชน์ในการ

วิเคราะห์ข้อมูลเอาไว้ โดยเทคนิคนี้ช่วยให้ข้อมูลที่อาจระบุตัวตนได้ถูกแปลงเป็นรูปแบบที่ความปลอดภัยมากขึ้น ผ่านการจัดกลุ่มและการแทนค่าที่มีความเฉพาะเจาะจงด้วยหมวดหมู่ที่กว้างขึ้นหรือช่วงครอบคลุมมากขึ้น เช่น การแสดงช่วงอายุแทนที่ตัวเลขอายุที่เจาะจง หรือการจัดกลุ่มอาชีพเป็นหมวดหมู่ที่กว้างขึ้น กระบวนการนี้ทำให้ข้อมูลในชุดเป็นลักษณะทั่วไปมากขึ้น ลดความเสี่ยงจากการระบุตัวตนของบุคคลจากข้อมูลที่เหลืออยู่ รูปที่ 3.23 รูปที่ 3.25 และรูปที่ 3.26 แสดงให้เห็นอย่างชัดเจนว่าค่าเฉพาะของแอตทริบิวต์เสมือนถูกแปลงเป็นหมวดหมู่หรือช่วงที่กว้างขึ้นได้อย่างไร เพื่อให้มั่นใจว่าข้อมูลที่เปิดเผยออกไปนั้นไม่สามารถใช้ในการระบุตัวตนได้โดยตรง ขณะเดียวกันก็ยังคงรักษาความสัมพันธ์ และโครงสร้างข้อมูลไว้สำหรับการวิเคราะห์ข้อมูลเชิงลึก นอกจากนี้รูปที่ 3.28 ยังเป็นผลลัพธ์จากกระบวนการประมวลผลคำสั่งที่อธิบายไว้รูปที่ 3.27 ซึ่งแสดงให้เห็นถึงวิธีการจัดกลุ่มใหม่ของแอตทริบิวต์เสมือนเป็นหมวดหมู่ที่กว้างขึ้น กระบวนการนี้แปลงข้อมูลดิบให้อยู่รูปแบบที่สามารถนำไปเผยแพร่หรือใช้งานในการวิเคราะห์ได้อย่างปลอดภัย โดยไม่เสี่ยงต่อการเปิดเผยข้อมูลที่อาจระบุตัวตนบุคคลได้ รูปนี้สะท้อนถึงความสามารถในการใช้เทคนิค k-Anonymity เพื่อสร้างข้อมูลที่ปลอดภัยต่อความเป็นส่วนตัว พร้อมทั้งยังรักษาประโยชน์ของข้อมูลไว้สำหรับการใช้งานจริงอย่างมีประสิทธิภาพและโปร่งใส

```
dfn.sort_values('age')
```

	age	education-num	income	count
0	[17.0]	[7.200598802395209]	<=50k	334
120	[17.0]	[9.0]	<=50k	14
43	[17.0]	[10.0]	<=50k	5
469	[17.0]	[3.0]	<=50k	3
615	[17.0]	[4.0]	<=50k	5
...	...	...	...	...
746	[90.0]	[9.0]	>50k	4
818	[90.0]	[14.0]	<=50k	2
819	[90.0]	[14.0]	>50k	3
804	[90.0]	[6.5]	<=50k	4
750	[90.0]	[10.545454545454545]	<=50k	9

822 rows × 4 columns

รูปที่ 3.28 การทำเป็นลักษณะทั่วไปโดยการแบ่งพาร์ติชันแอตทริบิวต์เสมือน

3.3.2.7 ขั้นตอนที่ 7 ทดสอบและประเมินผลแบบจำลองการเรียนรู้ของเครื่อง:

ขั้นตอนนี้ถือเป็นขั้นตอนที่มีความสำคัญอย่างยิ่ง เนื่องจากเป็นช่วงเวลา

ที่ต้องตรวจสอบและวัดผลการทำงานของแบบจำลองที่สร้างขึ้นอย่างละเอียด โดยเฉพาะการวัดประสิทธิภาพในการทำนาย การตรวจสอบการสูญเสียข้อมูล (Data Loss) และการประเมินความเสี่ยงจากการถูกโจมตีเพื่อระบุตัวตนซ้ำอีกครั้ง (Risk of Re-identification Attacks) กระบวนการนี้รวมถึงการประยุกต์ใช้เทคนิคการทำให้ข้อมูลเป็นลักษณะทั่วไป (Generalization Technique) ด้วยเทคนิค k-Anonymity เพื่อรักษาความเป็นส่วนตัวของข้อมูลโดยครอบคลุมถึงแบบจำลองการเรียนรู้ของเครื่องทั้ง 7 แบบได้แก่ Gradient Boosting (GB), Gaussian Naïve Bayes (GNB), Logistic Regression (LR), Random Forest (RF), Support Vector Classifier (SVC), Decision Tree (DT) และK-Nearest Neighbor (KNN) ซึ่งจะทำการวัดค่าตัวชี้วัดเพิ่มเติมเช่น Area Uder the Curve (AUC & Receiver Operating Characteristic (ROC) Curve ทั้งก่อนและหลังการประยุกต์ใช้ k-Anonymity วัตถุประสงค์หลักของการทดสอบและประเมินผลนี้ประกอบด้วยการวัดประสิทธิภาพการสูญเสียข้อมูลเพื่อประเมินผลกระทบที่เกิดจากการทำให้ข้อมูลเป็นลักษณะทั่วไปต่อความแม่นยำและประสิทธิภาพของแบบจำลอง ประเมินความเสี่ยงของการระบุตัวตนซ้ำอีกครั้งเพื่อให้มั่นใจว่าข้อมูลที่ผ่านการประยุกต์ใช้ k-Anonymity มีความปลอดภัยเพียงพอในการป้องกันการโจมตีที่พยายามระบุตัวตนของบุคคลจากข้อมูลที่เป็นลักษณะทั่วไป รวมถึงการวัดค่าตัวชี้วัดเพิ่มเติมเช่น AUC และ ROC Curve เพื่อประเมินความสามารถของแบบจำลองในการแยกแยะระหว่างคลาสต่าง ๆ และวิเคราะห์ความแม่นยำในการทำนาย การประเมินทั้งด้านการสูญเสียข้อมูลและความเสี่ยงของการระบุตัวตนซ้ำอีกครั้งนี้ช่วยให้สามารถปรับปรุงและพัฒนาแบบบจำลองให้มีความแม่นยำสูงขึ้นและปลอดภัยในการใช้งานจริง โดยมีวิธีการทดสอบและประเมินผลดังนี้

1) การเตรียมข้อมูลและแบบจำลอง:

1.1) ชุดข้อมูลต้นฉบับ (Raw Data): ในขั้นตอนแรกจะใช้ชุดข้อมูลที่ยังไม่ได้ถูกประยุกต์ใช้เทคนิค k-Anonymity ซึ่งหมายถึงข้อมูลดิบที่ยังคงรายละเอียดครบถ้วนและไม่ผ่านการปรับเปลี่ยนใด ๆ ก่อนการฝึกและทดสอบแบบจำลอง การใช้ข้อมูลดิบเป็นพื้นฐานช่วยให้แบบจำลองสามารถเรียนรู้จากข้อมูลที่มีความสามารถหลากหลายและซับซ้อนได้อย่างเต็มที่ ส่งผลให้การทำนายหรือการจำแนกข้อมูลมีความแม่นยำและมีประสิทธิภาพสูง ดังแสดงในรูปที่ 3.29

```
import pandas as pd
from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score

import pandas as pd
df=pd.read_csv('adult_without_pii.csv',index_col=0)

def cleandata(dataset):
    for column in dataset.columns:
        if dataset[column].dtype == type(object):
            le = LabelEncoder()
            dataset[column]=le.fit_transform(dataset[column])
    return dataset

df=cleandata(df)
```

รูปที่ 3.29 การเตรียมข้อมูลตั้งต้น

1.2) ชุดข้อมูลที่ผ่านการทำให้เป็นลักษณะทั่วไป (Generalized Data): นำชุดข้อมูลต้นฉบับมาทำให้เป็นลักษณะทั่วไปโดยเทคนิค k-Anonymity (ดังขั้นตอนที่ 4) กระบวนการนี้รวมถึงการเลือกคุณลักษณะเฉพาะที่ต้องการมาทำให้เป็นลักษณะทั่วไป เช่น การแปลงค่าตัวเลขให้เป็นช่วงหรือการใช้วิธีการอื่น ๆ เพื่อปกป้องข้อมูลส่วนบุคคล การทำให้ข้อมูลเป็นลักษณะทั่วไปช่วยลดความเสี่ยงในการระบุตัวตนของบุคคลในชุดข้อมูล ในขณะเดียวกันยังคงรักษาความสามารถในการวิเคราะห์และการเรียนรู้ของแบบจำลองได้อย่างมีประสิทธิภาพ ดังรูปที่ 3.30

```
import pandas as pd
from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score

import pandas as pd
df=pd.read_csv('adult_generalize_PDPA.csv',index_col=0)

def cleandata(dataset):
    for column in dataset.columns:
        if dataset[column].dtype == type(object):
            le = LabelEncoder()
            dataset[column]=le.fit_transform(dataset[column])
    return dataset

df=cleandata(df)
```

รูปที่ 3.30 การเตรียมข้อมูลที่ผ่านการทำให้เป็นลักษณะทั่วไป

2) การฝึกและทดสอบแบบจำลอง:

2.1) ก่อนการประยุกต์ใช้ k-Anonymity: มีการนำแบบจำลองการเรียนรู้ของเครื่องทั้ง 7 แบบมาใช้ ชุดข้อมูลถูกแบ่งออกเป็นชุดฝึกและชุดทดสอบโดยใช้ train_test_split เพื่อให้แน่ใจว่าการกระจายคลาสมีความสมดุลด้วยการแบ่งชั้นและการทำซ้ำได้ด้วย random_state=66

แต่ละแบบจำลองได้รับการฝึกจากข้อมูลฝึกและประเมินโดยใช้ข้อมูลการทดสอบ โดยคำนวณคะแนนความแม่นยำโดยใช้ Accuracy_score ผลลัพธ์ความแม่นยำนั้นเหมือนกันทั้ง 7 แบบจำลอง โดยให้ค่า 0.778197 ซึ่งบ่งชี้ว่าชุดข้อมูลสามารถเรียนรู้ได้อย่างเท่าเทียมกันในสถาปัตยกรรมแบบจำลองที่แตกต่างกัน ดังรูปที่ 3.31 ทำการทดสอบและประเมินแบบจำลองการเรียนรู้ของเครื่องดังรูปที่ 3.32

```
from sklearn.neighbors import KNeighborsClassifier
from sklearn.svm import SVC
from sklearn.linear_model import LogisticRegression
from sklearn.tree import DecisionTreeClassifier
from sklearn.naive_bayes import GaussianNB
from sklearn.ensemble import RandomForestClassifier
from sklearn.ensemble import GradientBoostingClassifier
from sklearn.model_selection import train_test_split
from sklearn.model_selection import train_test_split
from sklearn.model_selection import cross_val_score
from sklearn.metrics import accuracy_score
from sklearn.model_selection import train_test_split

logReg = LogisticRegression(solver='lbfgs', max_iter=3000)
X_train, X_test, y_train, y_test = train_test_split(df.loc[:, df.columns != 'Target']
                                                    , df['Target'], stratify=df['Target'], random_state=66)

models = []
models.append(('KNN', KNeighborsClassifier()))
models.append(('SVC', SVC()))
models.append(('LR', LogisticRegression()))
models.append(('DT', DecisionTreeClassifier()))
models.append(('GNB', GaussianNB()))
models.append(('RF', RandomForestClassifier()))
models.append(('GB', GradientBoostingClassifier()))
```

```
#Before k-anonymity
names = []
scores = []
for name, model in models:
    model=LogisticRegression(max_iter=3000)
    model.fit(X_train, y_train)
    y_pred = model.predict(X_test)
    scores.append(accuracy_score(y_test, y_pred))
    names.append(name)

kf_cross_val = pd.DataFrame({'Name': names, 'Score': scores})
kf_cross_val
```

	Name	Score
0	KNN	0.778197
1	SVC	0.778197
2	LR	0.778197
3	DT	0.778197
4	GNB	0.778197
5	RF	0.778197
6	GB	0.778197

รูปที่ 3.31 การฝึกและทดสอบแบบจำลองการเรียนรู้ของเครื่องก่อนใช้ k-Anonymity

```python
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = LogisticRegression(random_state=42,max_iter=3000)
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.797871  0.940967  0.863531      5336
           1   0.634571  0.300715  0.408057      1819

    accuracy                       0.778197      7155
   macro avg   0.716221  0.620841  0.635794      7155
weighted avg   0.756355  0.778197  0.747737      7155
```

```python
from sklearn.neighbors import KNeighborsClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = KNeighborsClassifier()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.783296  0.928036  0.849545      5336
           1   0.539016  0.246839  0.338612      1819

    accuracy                       0.754857      7155
   macro avg   0.661156  0.587437  0.594079      7155
weighted avg   0.721193  0.754857  0.719652      7155
```

```python
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = RandomForestClassifier(n_estimators=5, max_depth=2)
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.759465  1.000000  0.863291      5336
           1   1.000000  0.070918  0.132444      1819

    accuracy                       0.763802      7155
   macro avg   0.879732  0.535459  0.497867      7155
weighted avg   0.820616  0.763802  0.677489      7155
```

```python
from sklearn.ensemble import GradientBoostingClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = GradientBoostingClassifier()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.872580  0.945840  0.907734      5336
           1   0.789205  0.594832  0.678370      1819

    accuracy                       0.856604      7155
   macro avg   0.830892  0.770336  0.793052      7155
weighted avg   0.851383  0.856604  0.849423      7155
```

```python
from sklearn.svm import SVC
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = SVC(random_state=42)
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.776274  0.999438  0.873833      5336
           1   0.989474  0.155030  0.268061      1819

    accuracy                       0.784766      7155
   macro avg   0.882874  0.577234  0.570947      7155
weighted avg   0.830475  0.784766  0.719829      7155
```

```python
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = GaussianNB()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.800063  0.947901  0.867730      5336
           1   0.666267  0.305113  0.418552      1819

    accuracy                       0.784486      7155
   macro avg   0.733165  0.626507  0.643141      7155
weighted avg   0.766048  0.784486  0.753537      7155
```

```python
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = DecisionTreeClassifier()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.868268  0.867129  0.867698      5336
           1   0.611720  0.614074  0.612894      1819

    accuracy                       0.802795      7155
   macro avg   0.739994  0.740601  0.740296      7155
weighted avg   0.803046  0.802795  0.802920      7155
```

รูปที่ 3.32 ทดสอบและประเมินแบบจำลองการเรียนรู้ของเครื่องก่อนใช้ k-Anonymity

จากผลการทดสอบและประเมินแบบจำลองสามารถสรุปและแสดงภาพกราฟการวิเคราะห์เชิงเปรียบเทียบของแบบจำลองการเรียนรู้ของเครื่องได้ดังรูปที่ 3.33 ซึ่งเป็นการวิเคราะห์เชิงเปรียบเทียบของแบบจำลองการเรียนรู้ของเครื่องทั้ง 7 แบบ โดยอิงตามความแม่นยำความถูกต้อง การเรียกคืน และคะแนนเอฟวัน สำหรับคลาส 0 และคลาส 1 ได้ดังนี้

(1) ความแม่นยำของแบบจำลอง (Model Accuracy): จากการประเมินแบบจำลอง Gradient Boosting (GB) มีค่าความแม่นยำสูงสุดที่ประมาณ 0.8566 ซึ่งแสดงถึงความสามารถที่ในการสรุปข้อมูลทั่วไปที่แข็งแกร่งทั่วทั้งชุดข้อมูล ส่วน Decision Tree (DT) ตามมาด้วยค่าความแม่นยำที่ค่อนข้างสูงที่ประมาณ 0.8028 ซึ่งสะท้อนถึงความสามารถในการจับรูปแบบข้อมูลได้อย่างมีประสิทธิภาพ ในทางกลับกัน Random Forest (RF) และ K-Nearest Neighbors (KNN) มีคะแนนความแม่นยำที่ต่ำกว่าโดยอยู่ที่ประมาณ 0.7638 และ 0.7548 ตามลำดับ ซึ่งบ่งบอกถึงความท้าทายในการจัดการกับความซับซ้อนของชุดข้อมูลและความไม่สมดุลของคลาส

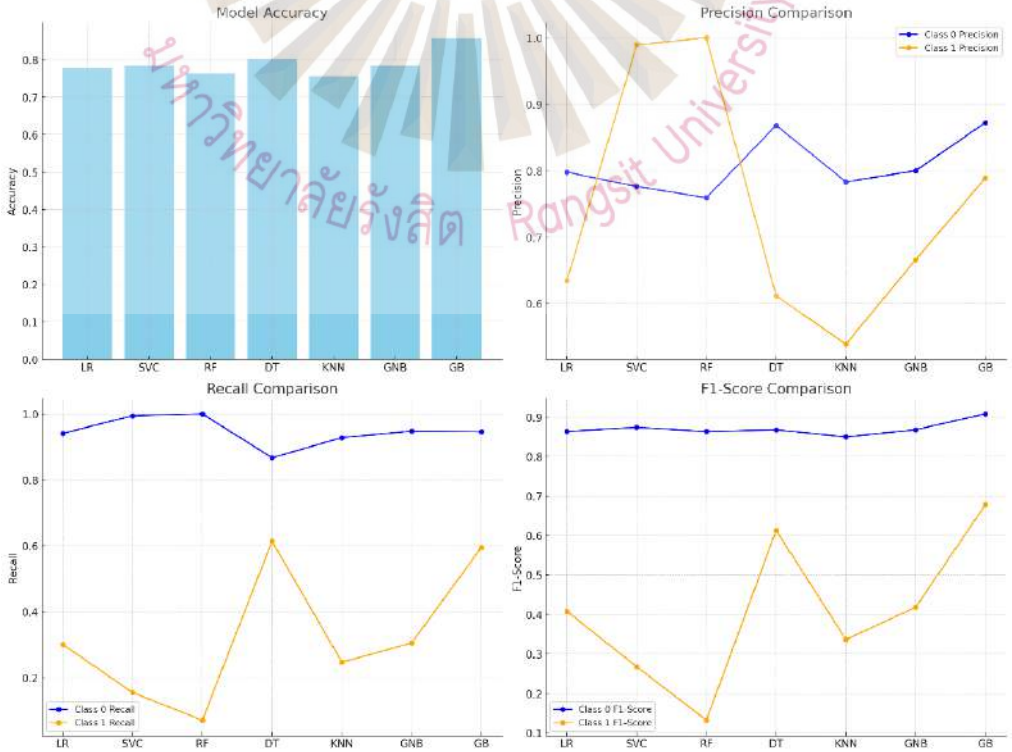
(2) การเปรียบเทียบความถูกต้อง (Precision Comparison): ในแง่ของความถูกต้องของคลาส 0 แบบจำลองส่วนใหญ่ประสิทธิภาพที่เสถียร โดยที่ Gradient Boosting (GB) และ Decision Tree (DT) ถือเป็นตัวแสดงประสิทธิภาพสูงสุด เนื่องจากระดับความถูกต้องที่สม่ำเสมอ อย่างไรก็ตาม ความถูกต้องของคลาส 1 แสดงให้เห็นถึงความแปรปรวนที่เห็นได้ชัดในแต่ละแบบจำลอง Random Forest (RF) และ Support Vector Classifier (SVC) ให้ความถูกต้องที่เกือบสมบูรณ์โดยโดดเด่นในการลดค่าบวกปลอมให้เหลือน้อยที่สุด ในทางกลับกัน K-Nearest Neighbors (KNN) และ Decision Tree (DT) แสดงให้เห็นถึงความถูกต้องที่ต่ำกว่าอย่างเห็นได้ชัดสำหรับคลาส 1 ซึ่งสะท้อนถึงความท้าทายในการระบุตัวอย่างเชิงบวกโดยไม่มีค่าบวกปลอมได้อย่างแม่นยำ

(3) การเปรียบเทียบการเรียกคืน (Recall Comparison): สำหรับการเรียกคืนคลาส 0 แบบจำลองส่วนใหญ่แสดงให้เห็นถึงประสิทธิภาพที่แข็งแกร่งอย่างสม่ำเสมอ โดย Random Forest (RF) ประสบความสำเร็จในการเรียกคืนอย่างสมบูรณ์แบบ โดยสามารถระบุอินสแตนซ์ทั้งหมดของคลาส 0 ได้สำเร็จโดยไม่มีการละเว้นใด ๆ อย่างไรก็ตาม การเรียกคืนคลาส 1 นั้นแตกต่างกันอย่างมากในแต่ละแบบจำลอง Decision Tree (DT) และ Gradient Boosting (GB) มีประสิทธิภาพค่อนข้างดีโดยจับตัวอย่างเชิงบวกได้มากกว่า ในขณะที่ Support Vector Classifier (SVC) และ K-Nearest Neighbors (KNN) แสดงคะแนนการเรียกคืนที่ต่ำอย่างเห็นได้ชัด โดยมักจะจำแนกอินสแตนซ์เชิงบวกเป็นเชิงลบอย่างไม่ถูกต้อง ความไม่สอดคล้องกันนี้เน้นย้ำถึงความยากลำบากที่แบบจำลองเหล่านี้เผชิญในการระบุตัวอย่างคลาสชนกลุ่มน้อยอย่างแม่นยำ

(4) การเปรียบเทียบคะแนนเอฟวัน (F1-Score Comparison): สำหรับคะแนนเอฟวันของคลาส 0 แบบจำลองทั้งหมดจะรักษาค่าสูงอย่างสม่ำเสมอ แสดงให้เห็นถึงความ

เสถียรและความน่าเชื่อถือในการทำนายคลาสส่วนใหญ่ด้วยความถูกต้องและการเรียกคืนที่สมดุล อย่างไรก็ตาม คะแนนเอฟวันของคลาส 1 จะแตกต่างกันอย่างมากในแต่ละแบบจำลอง Gradient Boosting (GB) และ Decision Tree (DT) โดดเด่นด้วยคะแนนเอฟวันที่สูงกว่า ซึ่งแสดงให้เห็นถึงความสมดุลระหว่างความถูกต้องและการเรียกคืนสำหรับการทำนายคลาสส่วนน้อย ในทางกลับกัน Support Vector Classifier (SVC) และ K-Nearest Neighbors (KNN) แสดงคะแนนเอฟวันที่ต่ำลงอย่างเห็นได้ชัด ซึ่งแสดงให้เห็นถึงความยากลำบากในการสร้างสมดุลระหว่างความถูกต้องและการเรียกคืนเมื่อระบุอินสแตนซ์คลาส 1

(5) ข้อสังเกตที่สำคัญ: Gradient Boosting (GB) โดดเด่นในฐานะแบบจำลองที่มีประสิทธิภาพที่สูงสุดโดยให้ผลลัพธ์ที่แข็งแกร่งอย่างสม่ำเสมอในทุกเกณฑ์วัดในขณะที่รักษาประสิทธิภาพที่สมดุลระหว่างทั้งสองคลาส Decision Tree (DT) ยังทำงานได้ดีโดยรวม แต่แสดงให้เห็นถึงความแปรปรวนในความถูกต้องและการเรียกคืนเฉพาะคลาส ในทางตรงกันข้าม Support Vector Classifier (SVC) และ K-Nearest Neighbors (KNN) ประสบปัญหาอย่างมากกับคลาส 1 โดยเน้นย้ำถึงความยากลำบากในการจัดการการทำนายคลาสชนกลุ่มน้อย ในขณะเดียวกัน Random Forest (RF) โดดเด่นในการเรียกคืนคลาส 0 ด้วยผลลัพธ์ที่เกือบสมบูรณ์แบบ แต่ล้มเหลวในการเรียกคืนคลาส 1 ซึ่งส่งผลต่อความแม่นำโดยรวมและความสมดุลของคลาสใน



รูปที่ 3.33 การวิเคราะห์เชิงเปรียบเทียบแบบจำลองการเรียนรู้ของเครื่องก่อนใช้ k-Anonymity

2.2) หลังการประยุกต์ใช้ k-Anonymity: หลังจากนำ k-Anonymity ไปใช้กับชุดข้อมูลแล้ว ได้มีการฝึกและประเมินแบบจำลองการเรียนรู้ของเครื่อง 7 แบบจำลอง โดยชุดข้อมูลจะผ่านกระบวนการก่อนการประมวลผล ซึ่งรวมถึงการเข้ารหัสป้ายกำกับสำหรับตัวแปรตามหมวดหมู่ และการแยกเป็นชุดฝึกและทดสอบโดยใช้การสุ่มแบบชั้น แต่ละแบบจำลองจะได้รับการฝึกทดสอบ และประเมินโดยใช้คะแนนความแม่นยำ แบบจำลองทั้งหมดได้รับคะแนนความแม่นยำที่เท่ากันคือประมาณ 0.782949 ซึ่งบ่งชี้ว่าเทคนิค k-Anonymity อาจทำให้ชุดข้อมูลมีความเป็นเนื้อเดียวกันซึ่งช่วยลดความแปรปรวนในประสิทธิภาพของแบบจำลอง ความสม่ำเสมอนี้บ่งชี้ถึงการสูญเสียรูปแบบเฉพาะในข้อมูลเนื่องจากการสรุปผล ซึ่งผลต่อแต่ละแบบจำลองเท่า ๆ กัน ดังรูปที่ 3.34 ทำการทดสอบและประเมินแบบจำลองการเรียนรู้ของเครื่องดังรูปที่ 3.35

```python
#Dataset : https://www.kaggle.com/uciml/adult-census-income
import pandas as pd
from sklearn.preprocessing import LabelEncoder
from sklearn.model_selection import train_test_split
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score

import pandas as pd
df=pd.read_csv('adult_generalize_PDPA.csv',index_col=0)

def cleandata(dataset):
    for column in dataset.columns:
        if dataset[column].dtype == type(object):
            le = LabelEncoder()
            dataset[column]=le.fit_transform(dataset[column])
    return dataset

df=cleandata(df)
```

```python
from sklearn.neighbors import KNeighborsClassifier
from sklearn.svm import SVC
from sklearn.linear_model import LogisticRegression
from sklearn.tree import DecisionTreeClassifier
from sklearn.naive_bayes import GaussianNB
from sklearn.ensemble import RandomForestClassifier
from sklearn.ensemble import GradientBoostingClassifier
from sklearn.model_selection import train_test_split
from sklearn.model_selection import train_test_split
from sklearn.model_selection import cross_val_score
from sklearn.metrics import accuracy_score
from sklearn.model_selection import train_test_split

logReg = LogisticRegression(solver='lbfgs', max_iter=3000)
X_train, X_test, y_train, y_test = train_test_split(df.loc[:, df.columns != 'Target']
                                   , df['Target'], stratify=df['Target'], random_state=66)
models = []
models.append(('KNN', KNeighborsClassifier()))
models.append(('SVC', SVC()))
models.append(('LR', LogisticRegression()))
models.append(('DT', DecisionTreeClassifier()))
models.append(('GNB', GaussianNB()))
models.append(('RF', RandomForestClassifier()))
models.append(('GB', GradientBoostingClassifier()))
```

```python
#After k-anonymity
names = []
scores = []
for name, model in models:
    model=LogisticRegression(max_iter=3000)
    model.fit(X_train, y_train)
    y_pred = model.predict(X_test)
    scores.append(accuracy_score(y_test, y_pred))
    names.append(name)

kf_cross_val = pd.DataFrame({'Name': names, 'Score': scores})
kf_cross_val
```

	Name	Score
0	KNN	0.782949
1	SVC	0.782949
2	LR	0.782949
3	DT	0.782949
4	GNB	0.782949
5	RF	0.782949
6	GB	0.782949

รูปที่ 3.34 การฝึกและทดสอบแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity

```python
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = LogisticRegression(random_state=42,max_iter=3000)
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.805722  0.934220  0.865226      5336
           1   0.637397  0.339197  0.442770      1819

    accuracy                       0.782949      7155
   macro avg   0.721559  0.636709  0.653998      7155
weighted avg   0.762929  0.782949  0.757826      7155
```

```python
from sklearn.svm import SVC
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = SVC(random_state=42)
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6, zero_division=0))
```

```
              precision    recall  f1-score   support

           0   0.745772  1.000000  0.854375      5336
           1   0.000000  0.000000  0.000000      1819

    accuracy                       0.745772      7155
   macro avg   0.372886  0.500000  0.427188      7155
weighted avg   0.556176  0.745772  0.637169      7155
```

```python
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = RandomForestClassifier(n_estimators=5, max_depth=2)
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.803937  0.956709  0.873695      5336
           1   0.713043  0.315558  0.437500      1819

    accuracy                       0.793711      7155
   macro avg   0.758490  0.636134  0.655598      7155
weighted avg   0.780829  0.793711  0.762802      7155
```

```python
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = DecisionTreeClassifier()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.849195  0.889618  0.868936      5336
           1   0.623642  0.536559  0.576832      1819

    accuracy                       0.799860      7155
   macro avg   0.736419  0.713088  0.722884      7155
weighted avg   0.791853  0.799860  0.794675      7155
```

```python
from sklearn.neighbors import KNeighborsClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = KNeighborsClassifier()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.859735  0.852324  0.856014      5336
           1   0.577480  0.592084  0.584691      1819

    accuracy                       0.786164      7155
   macro avg   0.718608  0.722204  0.720352      7155
weighted avg   0.787978  0.786164  0.787036      7155
```

```python
from sklearn.naive_bayes import GaussianNB
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = GaussianNB()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.866998  0.784295  0.823576      5336
           1   0.505584  0.647059  0.567639      1819

    accuracy                       0.749406      7155
   macro avg   0.686291  0.715677  0.695607      7155
weighted avg   0.775117  0.749406  0.758510      7155
```

```python
from sklearn.ensemble import GradientBoostingClassifier
from sklearn.metrics import accuracy_score
from sklearn.metrics import classification_report

model = GradientBoostingClassifier()
model.fit(X_train, y_train)
y_pred = model.predict(X_test)
print(classification_report(y_test, y_pred, digits=6))
```

```
              precision    recall  f1-score   support

           0   0.850751  0.922976  0.885393      5336
           1   0.699122  0.525014  0.599686      1819

    accuracy                       0.821803      7155
   macro avg   0.774936  0.723995  0.742540      7155
weighted avg   0.812203  0.821803  0.812759      7155
```

รูปที่ 3.35 ทดสอบและประเมินแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity

จากผลการทดสอบและประเมินแบบจำลองสามารถสรุปและแสดงภาพกราฟการวิเคราะห์เชิงเปรียบเทียบของแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity ได้ดังรูปที่ 3.36 ซึ่งเป็นการวิเคราะห์เชิงเปรียบเทียบของแบบจำลองการเรียนรู้ของเครื่องทั้ง 7 แบบ โดยอิงตามความแม่นยำความถูกต้อง การเรียกคืน และคะแนนเอฟวัน สำหรับคลาส 0 และคลาส 1 ได้ดังนี้

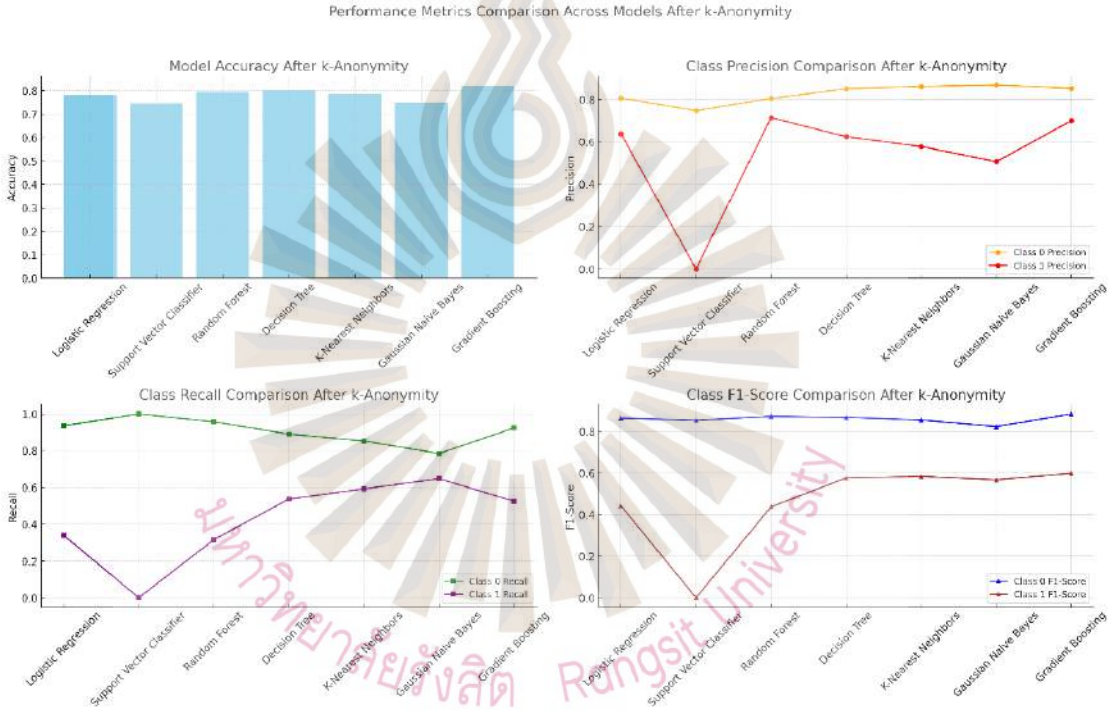
(1) ความแม่นยำของแบบจำลอง (Model Accuracy): จากการประเมินแบบจำลองหลังจากใช้ k-Anonymity พบว่า Gradient Boosting (GB) แสดงให้เห็นถึงความแม่นยำสูงสุดมีค่า 0.821803 ซึ่งแสดงให้เห็นถึงความสามารถในการปรับตัวที่แข็งแกร่งกับชุดข้อมูลทั่วไป ส่วนDecision Tree (DT) และ Random Forest (RF) ก็ทำงานได้ดีเช่นกัน โดยได้รับคะแนนความแม่นยำที่ค่อนข้างสูงเช่นกัน ในทางกลับกัน Support Vector Classifier (SVC) มีปัญหาในการบันทึกข้อมูลทั่วไปโดยบันทึกความแม่นยำต่ำสุดอยู่ที่ 0.745772 และบ่งชี้ถึงความท้าทายในการเรียนรู้จากชุดข้อมูลที่เป็นนิรนามอย่างมีประสิทธิภาพ

(2) การเปรียบเทียบความถูกต้อง (Precision Comparison): แบบจำลองส่วนใหญ่แสดงให้เห็นถึงความถูกต้องสูงอย่างสม่ำเสมอสำหรับคลาส 0 โดยที่ Gradient Boosting (GB) และ Gaussian Naïve Bayes (GNB) มีประสิทธิภาพสูงสุด อย่างไรก็ตามความถูกต้องของคลาส 1 ลดลง อย่างมีนัยสำคัญในหลายแบบจำลอง โดยที่ Support Vector Classifier (SVC) ได้ค่าความถูกต้องเป็น 0 ซึ่งบ่งชี้ว่าไม่สามารถทำนายคลาส 1 ได้อย่างมีประสิทธิภาพ ในขณะที่ Random Forest (RF) และ Gradient Boosting (GB) ประสบความสำเร็จในค่าความถูกต้องที่ดีกว่าสำหรับคลาส 1

(3) การเปรียบเทียบการเรียกคืน (Recall Comparison): แบบจำลองส่วนใหญ่แสดงคะแนนการเรียกคืนข้อมูลที่แข็งแกร่งสำหรับคลาส 0 โดยที่ Support Vector Classifier (SVC) ประสบความสำเร็จที่สมบูรณ์แบบในการเรียกคืน อย่างไรก็ตาม การเรียกคืนข้อมูลในคลาส 1 แสดงให้เห็นถึงความแปรปรวนอย่างมาก ในขณะที่แบบจำลองเช่น Gradient Boosting (GB) และ Gaussian Naïve Bayes (GNB) มีประสิทธิภาพปานกลาง Support Vector Classifier (SVC) และ Random Forest (RF) ประสบปัญหาโดยบันทึกค่าการเรียกคืนข้อมูลที่ต่ำกว่าอย่างมีนัยสำคัญ

(4) การเปรียบเทียบคะแนนเอฟวัน (F1-Score Comparison): แบบจำลองส่วนใหญ่มีประสิทธิภาพดีอย่างสม่ำเสมอสำหรับคลาส 0 ซึ่งบ่งชี้ถึงความสมดุลระหว่างความถูกต้องและการเรียกคืน อย่างไรก็ตาม คะแนนเอฟวันของคลาส 1 แสดงให้เห็นถึงความแปรปรวนอย่างมีนัยสำคัญ Gradient Boosting (GB) และ Decision Tree (DT) ได้รับคะแนนที่สูงกว่าเมื่อเทียบกัน ในขณะที่ Support Vector Classifier (SVC) แสดงให้เห็นถึงประสิทธิภาพที่อ่อนแอที่สุด ซึ่งสะท้อนถึงความยากลำบากในการรักษาสมดุลระหว่างความถูกต้องและการเรียกคืนสำหรับคลาส 1

(5) ข้อสังเกตที่สำคัญ: Gradient Boosting (GB) กลายเป็นแบบจำลองที่มีความสมดุลและเชื่อถือได้มากที่สุดหลังจากใช้ k-Anonymity โดยมอบประสิทธิภาพที่แข็งแกร่งอย่างสม่ำเสมอในเกณฑ์ประเมินทั้งหมด ความสามารถในการรักษาความแม่นยำ ความถูกต้อง การเรียกคืนและคะแนนเอฟวัน เน้นย้ำถึงความสามารถในการปรับตัวให้เข้ากับชุดข้อมูลทั่วไป Decision Tree (DT) และ Random Forest (RF) ยังแสดงผลลัพธ์ที่มั่นคงโดยตามหลัง Gradient Boosting (GB) อย่างใกล้ชิดในด้านประสิทธิภาพโดยรวม ในทางกลับกัน Support Vector Classifier (SVC) ประสบปัญหาอย่างเห็นได้ชัด โดยเฉพาะในการทำนายคลาส 1 ซึ่งเน้นย้ำถึงข้อจำกัดในการจัดการข้อมูลทั่วไปและข้อมูลนิรนามอย่างมีประสิทธิภาพ



รูปที่ 3.36 การวิเคราะห์เชิงเปรียบเทียบแบบจำลองการเรียนรู้ของเครื่องหลังใช้ k-Anonymity

3) การวัดประสิทธิภาพการสูญเสียข้อมูล: การนำเทคนิค k-Anonymity ไปใช้นั้นมุ่งหวังที่จะปรับปรุงความเป็นส่วนตัวของข้อมูลโดยทำให้ข้อมูลที่ละเอียดอ่อนเป็นนิรนามหรือเป็นลักษณะทั่วไป ซึ่งจะช่วยลดความเสี่ยงในการระบุตัวตนของบุคคลได้ แม้ว่าวิธีนี้จะช่วยปกป้องความเป็นส่วนตัวได้อย่างมีประสิทธิภาพแต่ก็มักจะทำให้เกิดการสูญเสียข้อมูลโดยทำให้รายละเอียดไม่ชัดเจน การสูญเสียข้อมูลนี้อาจส่งผลกระทบอย่างมากต่อประสิทธิภาพการทำนายของแบบจำลองการเรียนรู้ของเครื่อง โดยเฉพาะอย่างยิ่งในสถานการณ์ที่ต้องใช้ความถูกต้องและการเรียกคืนข้อมูลสูง ดังนั้นการแลกเปลี่ยนระหว่างความเป็นส่วนตัวและความแม่นยำของแบบจำลอง

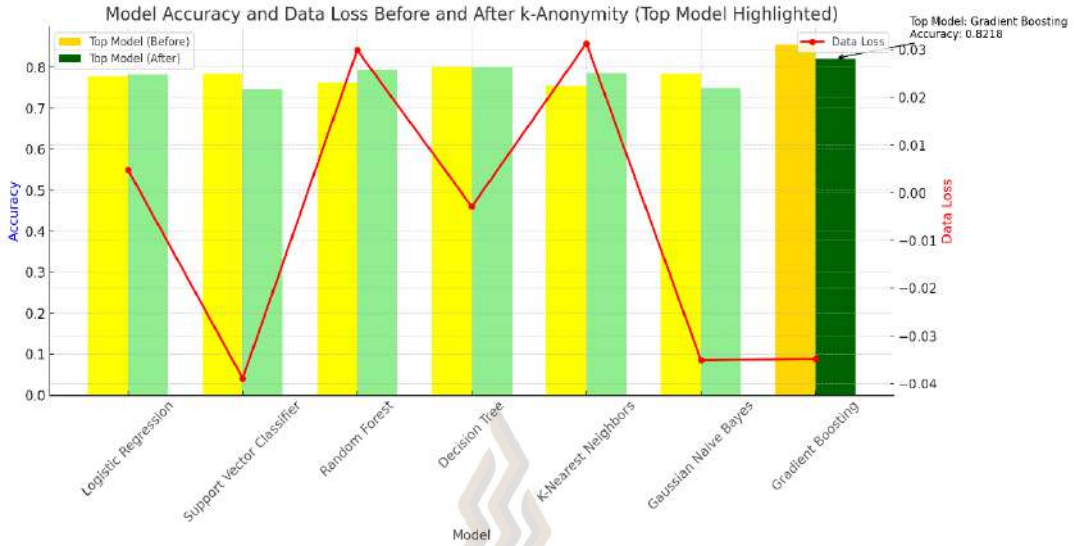
กลายเป็นปัญหาสำคัญ รายละเอียดด้านล่างเป็นการวิเคราะห์ผลกระทบของเทคนิค k-Anonymity ต่อประสิทธิภาพแบบจำลองโดยอิงตามตัวชี้วัดการประเมินที่สำคัญ ดังนี้

3.1) การเปรียบเทียบค่าความแม่นยำ: ความแม่นยำแสดงถึงอัตราส่วนของผลลัพธ์ที่คาดการณ์ได้อย่างถูกต้องเมื่อเทียบกับผลลัพธ์ที่คาดการณ์ทั้งหมด ความแม่นยำทำหน้าที่เป็นตัวชี้วัดพื้นฐานในการทำความเข้าใจผลกระทบต่อประสิทธิภาพโดยรวมอันเนื่องมาจากการทำให้ข้อมูลเป็นนิรนาม ดังรายละเอียดข้อมูลในตารางที่ 3.6

ตารางที่ 3.6 การเปรียบเทียบความแม่นยำของแบบจำลองก่อนและหลังใช้ k-Anonymity

Model	Accuracy		Data Loss
	Before k-Anonymity	After k-Anonymity	
Logistic Regression (LR)	0.778197	0.782949	0.004752
Support Vector Classifier (SVC)	0.784766	0.745772	-0.038994
Random Forest (RF)	0.763802	0.793711	0.029909
Decision Tree (DT)	0.802795	0.799860	-0.002935
K-Nearest Neighbors (KNN)	0.754857	0.786164	0.031307
Gaussian Naïve Bayes (GNB)	0.784486	0.749406	-0.035080
Gradient Boosting (GB)	0.856604	0.821803	-0.034801

จากรูปที่ 3.37 แสดงการเปรียบเทียบความแม่นยำของแบบจำลองก่อนและหลังใช้เทคนิค k-Anonymity โดยเน้นที่ความแม่นยำและการสูญเสียข้อมูล พบว่า Gradient Boosting เป็นแบบจำลองที่มีประสิทธิภาพสูงสุด โดยคงความแม่นยำสูงสุดทั้งก่อน (0.856604) และหลัง (0.821803) ใช้ k-Anonymity โดยมีการสูญเสียข้อมูลน้อยที่สุด (-0.034801) ส่วน Random Forest และ K-Nearest Neighbors แสดงการปรับปรุงความแม่นยำเพียงเล็กน้อยหลังใช้ k-Anonymity โดยเพิ่มขึ้น 0.029909 และ 0.031307 ตามลำดับ ในทางตรงกันข้าม แบบจำลองอย่าง Gaussian Naïve Bayes และ Support Vector Classifier ประสบปัญหาความแม่นยำที่ลดลงอย่างเห็นได้ชัด โดยมีการสูญเสียข้อมูล -0.035080 และ -0.038994 สิ่งนี้เน้นย้ำถึงผลกระทบที่แตกต่างกันของ k-Anonymity ต่อประสิทธิภาพของแบบจำลอง โดยที่บางแบบจำลองมีความยืดหยุ่นมากกว่าแบบจำลองอื่น ๆ



รูปที่ 3.37 การเปรียบเทียบความแม่นยำของแบบจำลองการเรียนรู้ของเครื่อง ก่อนและหลังใช้ k-Anonymity

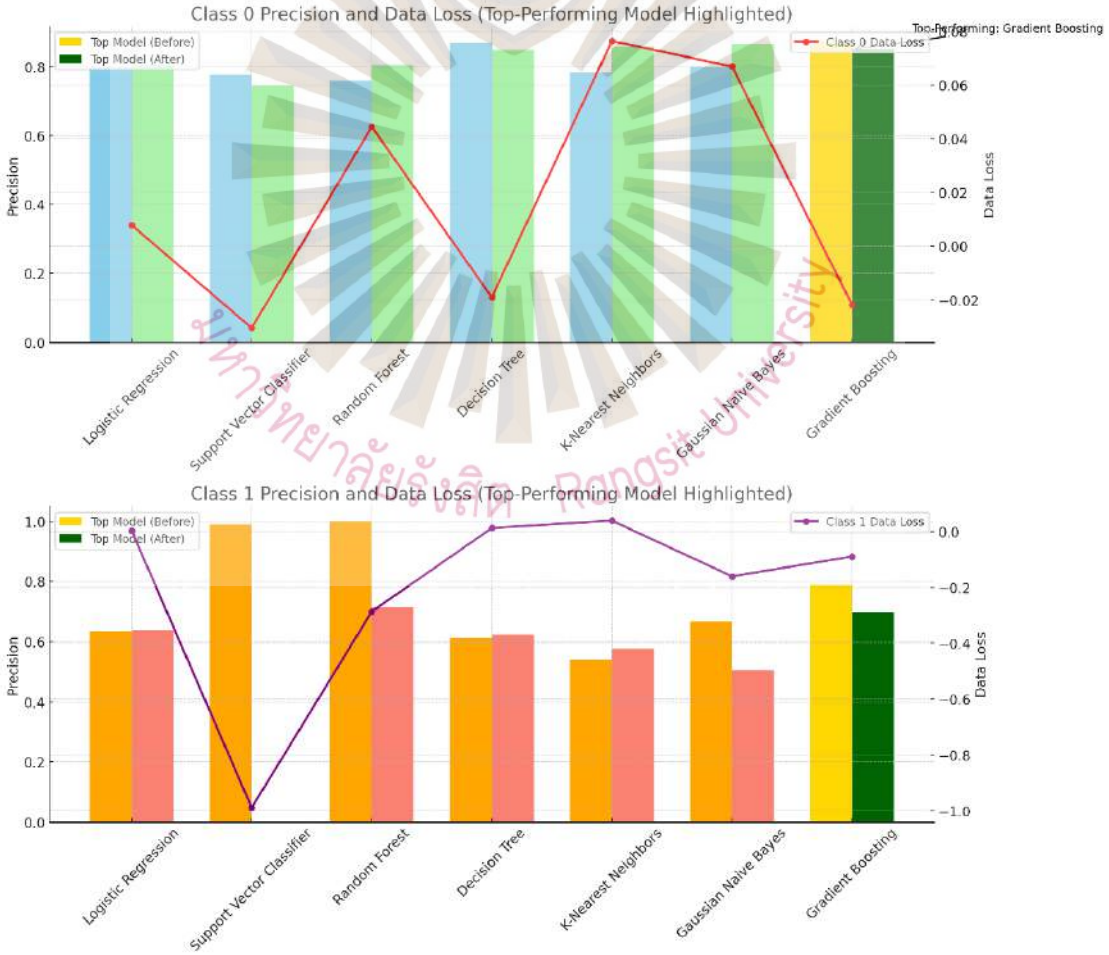
3.2) การใช้หน่วยวัดประสิทธิภาพอื่น ๆ: แม้ว่าความแม่นยำจะเป็นสิ่งสำคัญแต่บ่อยครั้งที่ตัวชี้วัดเหล่านี้ไม่สะท้อนประสิทธิภาพของแบบจำลองที่แท้จริงได้ โดยเฉพาะในชุดข้อมูลที่ไม่สมดุล หน่วยวัดเพิ่มเติม เช่น ความถูกต้อง การเรียกคืน และคะแนนเอฟวัน จะทำให้มองเห็นประสิทธิภาพได้ละเอียดยิ่งขึ้น โดยเฉพาะอย่างยิ่งสำหรับชุดข้อมูลที่ไม่สมดุลหรือคลาสเฉพาะ

(1) ความถูกต้อง (Precision): ความถูกต้องจะวัดสัดส่วนของผลลัพธ์เชิงบวกที่คาดการณ์ไว้ถูกต้องจากผลลัพธ์เชิงบวกที่คาดการณ์ไว้ทั้งหมด โดยจะเน้นที่การลดผลลัพธ์เชิงบวกปลอมให้เหลือน้อยที่สุด ดังรายละเอียดข้อมูลในตารางที่ 3.7

ตารางที่ 3.7 การเปรียบเทียบความถูกต้องของแบบจำลองก่อนและหลังใช้ k-Anonymity

Model	Class 0			Class 1		
	Before	After	Data Loss	Before	After	Data Loss
Logistic Regression	0.797871	0.805722	0.007851	0.634571	0.637397	0.002826
Support Vector Classifier	0.776274	0.745772	-0.030502	0.989474	0.000000	-0.989474
Random Forest	0.759465	0.803937	0.044472	1.000000	0.713043	-0.286957
Decision Tree	0.868268	0.849195	-0.019073	0.611720	0.623642	0.011922
K-Nearest Neighbors	0.783296	0.859735	0.076439	0.539016	0.577480	0.038464
Gaussian Naïve Bayes	0.800063	0.866998	0.066935	0.666267	0.505584	-0.160683
Gradient Boosting	0.872580	0.850751	-0.021829	0.789205	0.699122	-0.090083

จากรูปที่ 3.38 แสดงการวิเคราะห์ความถูกต้องก่อนและหลังการใช้ k-Anonymity ในแบบจำลองการเรียนรู้ของเครื่องทั้งเจ็ดแบบเผยให้เห็นความแตกต่างอย่างมีนัยสำคัญในประสิทธิภาพ โดยเฉพาะอย่างยิ่งระหว่างคลาส 0 และคลาส 1 แม้ว่าแบบจำลอง เช่น Random Forest, K-Nearest Neighbors และ Gaussian Naïve Bayes จะแสดงการทำให้ดีขึ้นในความถูกต้องของคลาส 0 แต่แบบจำลองเหล่านี้กลับต้องพยายามกับความคลาดเคลื่อนอย่างมากในความถูกต้องของคลาส 1 แต่ Support Vector Classifier ประสบความล้มเหลวอย่างมากโดยความถูกต้องของคลาส 1ลดลงเหลือ 0 หลังจากทำให้เป็นนิรนาม ในทางกลับกัน Gradient Boosting และ Decision Tree ยังคงรักษาประสิทธิภาพที่ค่อนข้างเสถียรในทั้งสองคลาส โดย Gradient Boosting โดดเด่นในฐานะแบบจำลองที่สมดุลและยืดหยุ่นที่สุดโดยรวม การวิเคราะห์นี้เน้นย้ำถึงผลกระทบที่ไม่สมส่วนของการทำให้เป็นนิรนามต่อการคาดการณ์ของคลาส 1 และเน้นย้ำว่า Gradient Boosting เป็นแบบจำลองที่มีประสิทธิภาพสูงสุดในการรักษาความถูกต้องภายใต้การเปลี่ยนแปลงที่รักษาความเป็นส่วนตัว



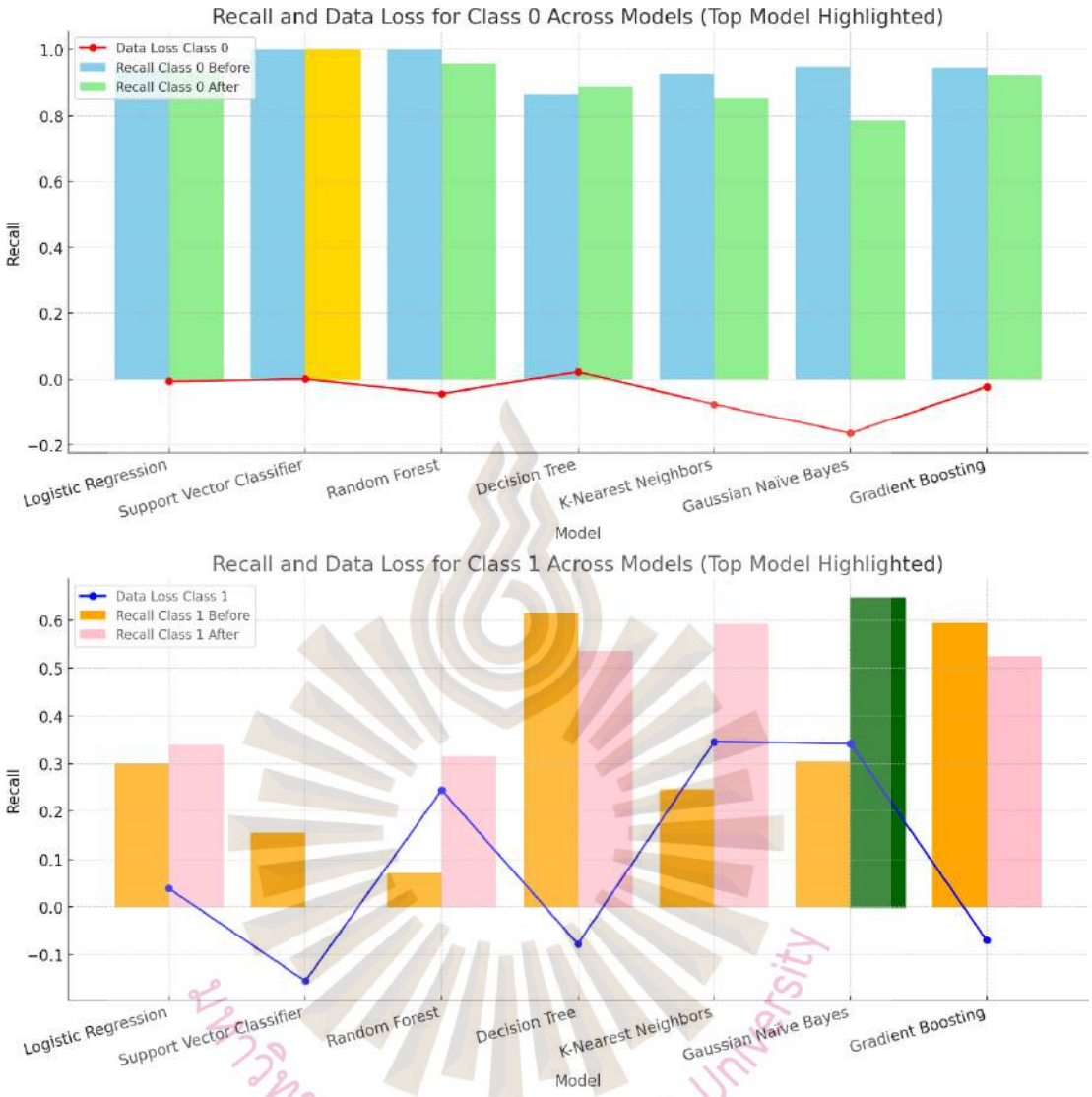
รูปที่ 3.38 การเปรียบเทียบความถูกต้องของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้ k-Anonymity

(2) การเรียกคืน (Recall): การเรียกคืนจะวัดสัดส่วนของผลลัพธ์เชิงบวกที่คาดการณ์ได้อย่างถูกต้องจากผลลัพธ์เชิงบวกที่เกิดจริงทั้งหมด โดยมุ่งเน้นที่การลดผลลัพธ์เชิงลบปลอมให้เหลือน้อยที่สุด ดังรายละเอียดข้อมูลในตารางที่ 3.8

ตารางที่ 3.8 การเปรียบเทียบการเรียกคืนของแบบจำลองก่อนและหลังใช้ k-Anonymity

Model	Class 0			Class 1		
	Before	After	Data Loss	Before	After	Data Loss
Logistic Regression	0.940967	0.934220	-0.006747	0.300715	0.339197	0.038482
Support Vector Classifier	0.999438	1.000000	0.000562	0.155030	0.000000	-0.155030
Random Forest	1.000000	0.956709	-0.043291	0.070918	0.315558	0.244640
Decision Tree	0.867129	0.889618	0.022489	0.614074	0.536559	-0.077515
K-Nearest Neighbors	0.928036	0.852324	-0.075712	0.246839	0.592084	0.345245
Gaussian Naïve Bayes	0.947901	0.784295	-0.163606	0.305113	0.647059	0.341946
Gradient Boosting	0.945840	0.922976	-0.022864	0.594832	0.525014	-0.069818

จากรูปที่ 3.39 แสดงการวิเคราะห์การเรียกคืนก่อนและหลังการใช้ k-Anonymity เผยให้เห็นความแตกต่างอย่างมีนัยสำคัญระหว่างคลาส 0 และคลาส 1 ในแบบจำลองต่าง ๆ Support Vector Classifier โดดเด่นในการเรียกคืนของคลาส 0 โดยรักษาประสิทธิภาพที่เกือบสมบูรณ์แบบแต่ล้มเหลวโดยสิ้นเชิงในการเรียกคืนของคลาส 1 หลังจากทำให้เป็นนิรนาม ในทางตรงกันข้าม Gaussian Naïve Bayes แสดงให้เห็นถึงการปรับปรุงที่สำคัญในการเรียกคืนของคลาส 1 ทำให้เป็นแบบแบบจำลองที่ปรับตัวได้มากที่สุดสำหรับการทำนายคลาสของชนกลุ่มน้อย ส่วน Random Forest และ K-Nearest Neighbors ประสบกับการลดลงอย่างเห็นได้ชัดในทั้งสองคลาส ในขณะที่ Gradient Boosting และ Decision Tree แสดงให้เห็นการลดลงปานกลางแต่ยังคงประสิทธิภาพที่สมดุล โดยรวมแล้วการเรียกคืนของคลาส 1 ได้รับผลกระทบอย่างไม่สมส่วนในแบบจำลองส่วนใหญ่ ซึ่งเน้นย้ำถึงความท้าทายในการรักษาประสิทธิภาพของคลาสของชนกลุ่มน้อยหลังจากการทำให้เป็นนิรนาม ในขณะที่การเรียกคืนของคลาส 0 ยังคงค่อนข้างเสถียรในหลายแบบจำลอง



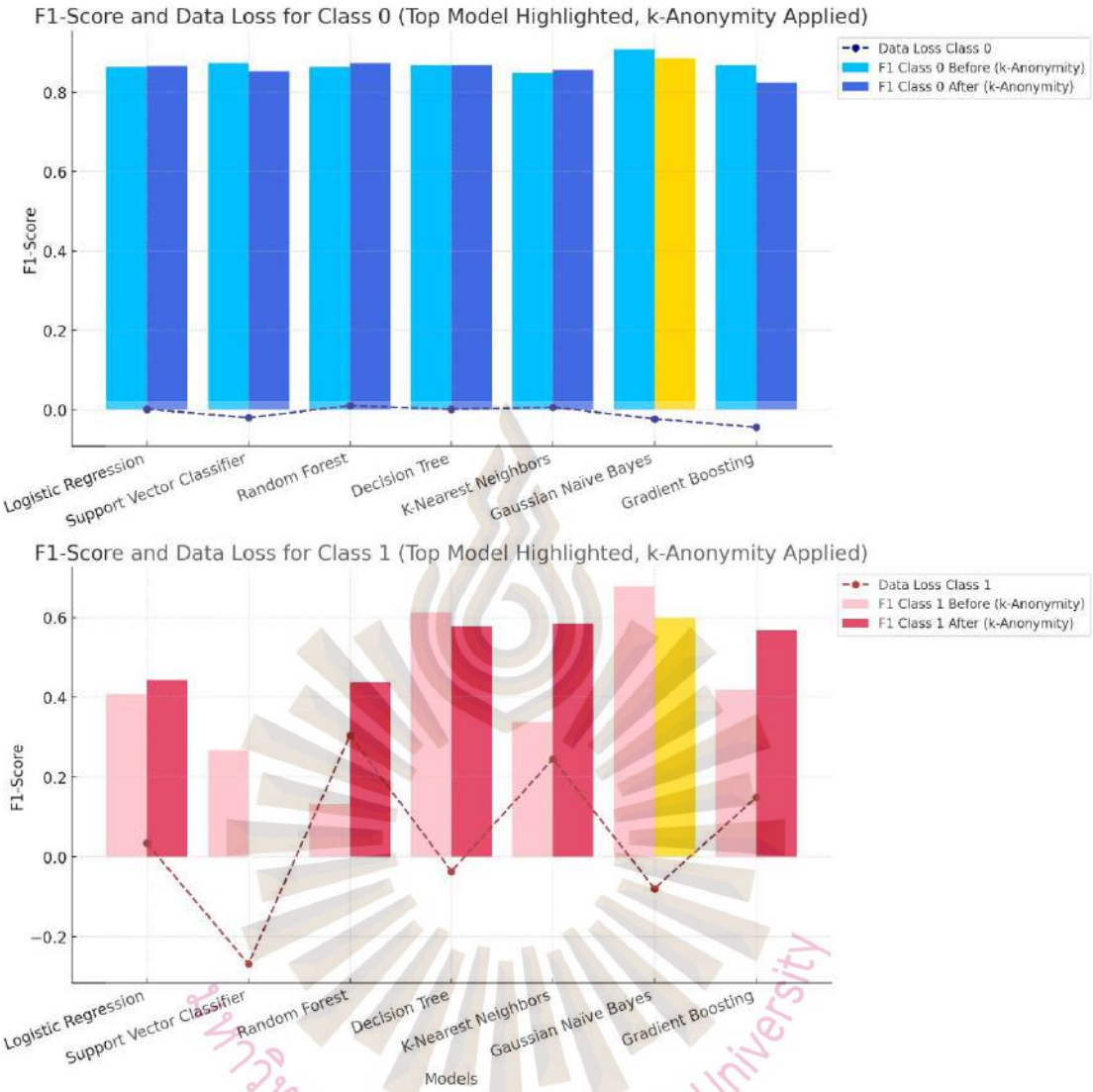
รูปที่ 3.39 การเปรียบเทียบการเรียกคืนของแบบจำลองการเรียนรู้ของเครื่อง
ก่อนและหลังใช้เทคนิค k-Anonymity

(3) คะแนนเอฟวัน (F1-Score): คะแนนเอฟวันเป็นตัวชี้วัดที่สำคัญในการประเมินประสิทธิภาพของแบบจำลองการเรียนของเครื่องเชิงลึก คะแนนเอฟวันสะท้อนถึงความสมดุลระหว่างค่าความถูกต้องซึ่งวัดความแม่นยำของการทำนายผลลัพธ์ที่ถูกต้องและค่าการเรียกคืนซึ่งวัดความสามารถของแบบจำลองในการดึงข้อมูลที่สำคัญออกมาได้ครบถ้วน คะแนนเอฟวันจะคำนวณจากค่าเฉลี่ยความสอดคล้องของทั้งสองตัวชี้วัด ซึ่งช่วยลดผลกระทบของค่าที่แตกต่างกันมากเกินไป เพื่อให้ได้ค่าที่เป็นกลางและสอดคล้องกัน รายละเอียดเพิ่มเติมสามารถดูได้ในตารางที่ 3.9

ตารางที่ 3.9 การเปรียบเทียบคะแนนเอฟวันของแบบจำลองก่อนและหลังใช้ k-Anonymity

Model	Class 0			Class 1		
	Before	After	Data Loss	Before	After	Data Loss
Logistic Regression	0.863531	0.865226	0.001695	0.408057	0.442770	0.034713
Support Vector Classifier	0.873833	0.854375	-0.019458	0.268061	0.000000	-0.268061
Random Forest	0.863291	0.873695	0.010404	0.132444	0.437500	0.305056
Decision Tree	0.867698	0.868936	0.001238	0.612894	0.576832	-0.036062
K-Nearest Neighbors	0.849545	0.856014	0.006469	0.338612	0.584691	0.246079
Gaussian Naïve Bayes	0.907734	0.885393	-0.022341	0.678370	0.599686	-0.078684
Gradient Boosting	0.867730	0.823576	-0.044154	0.418552	0.567639	0.149087

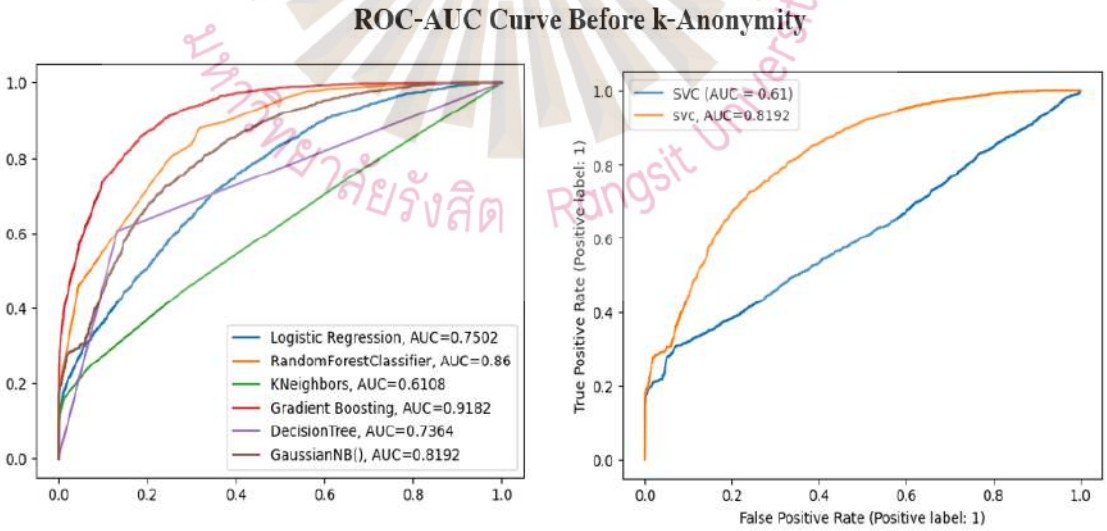
จากรูปที่ 3.40 แสดงการวิเคราะห์คะแนนเอฟวันก่อนและหลังใช้ k-Anonymity พบว่าหลังจากใช้เทคนิค k-Anonymity แล้ว Gaussian Naïve Bayes เป็นแบบจำลองที่มีประสิทธิภาพสูงสุดสำหรับทั้งคลาส 0 และคลาส 1 โดยแสดงผลลัพธ์ที่สม่ำเสมอแม้ว่าประสิทธิภาพจะลดลงเล็กน้อยจาก 0.907734 เป็น 0.885393 โดยที่สูญเสียข้อมูล 0.022341 ในทำนองเดียวกันในคลาส 1 คะแนนเอฟวันลดลงจาก 0.678370 เป็น 0.599686 ซึ่งสะท้อนถึงการสูญเสียข้อมูล 0.078684 แบบจำลองส่วนใหญ่ในคลาส 0 ประสบกับการสูญเสียข้อมูลเพียงเล็กน้อยเท่านั้น ในขณะที่คลาส 1 แสดงความแปรปรวนที่เด่นชัดมากกว่า เช่น Support Vector Classifier เผชิญกับการลดลงอย่างมากในคลาส 1 (คะแนนเอฟวันลดลงเหลือ 0 โดยสูญเสียข้อมูล 0.268061) ในขณะที่ Random Forest สามารถปรับปรุงอย่างมีนัยสำคัญในคลาส 1 ด้วยเพิ่มขึ้น 0.305056 การวิเคราะห์นี้เน้นย้ำว่า Gaussian Naïve Bayes เป็นแบบจำลองที่ยืดหยุ่นและเชื่อถือได้มากที่สุดภายใต้ผลกระทบของ k-Anonymity โดยคงประสิทธิภาพที่ค่อนข้างสูงในทั้งสองคลาส แม้ว่าคะแนนเอฟวันจะลดลงเล็กน้อยก็ตาม



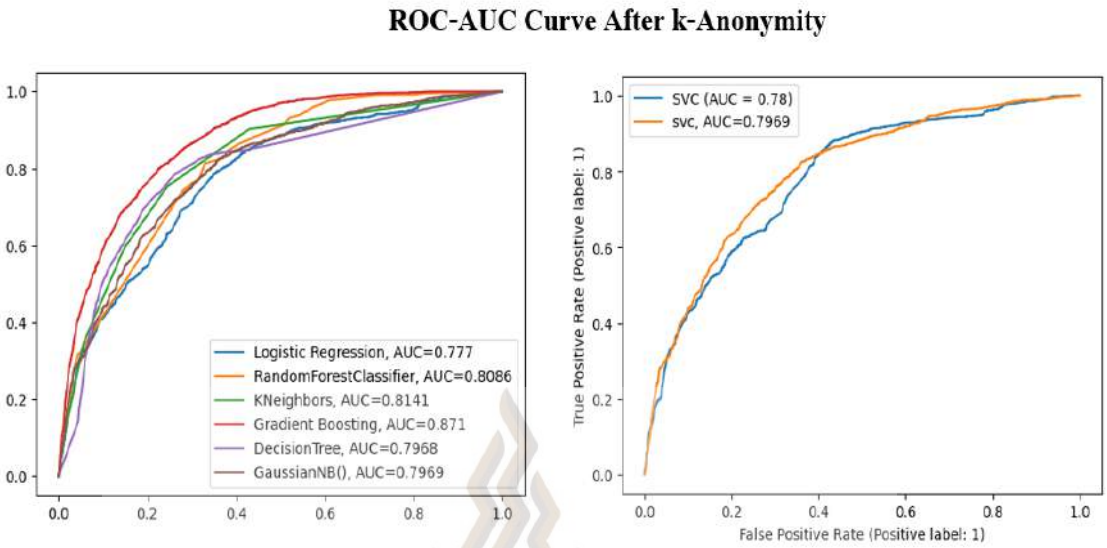
รูปที่ 3.40 การเปรียบเทียบคะแนนเอฟวันของแบบจำลองการเรียนรู้ของเครื่อง ก่อนและหลังใช้เทคนิค k-Anonymity

3.3) การวัดค่าตัวชี้วัดเพิ่มเติม (AUC และ ROC Curve): AUC (พื้นที่ใต้เส้นโค้ง) วัดความสามารถของแบบจำลองในการแยกแยะระหว่างคลาสเชิงบวกและเชิงลบตั้งแต่ 0 ถึง 1 โดยที่ค่าที่สูงกว่าบ่งบอกถึงประสิทธิภาพที่ดีขึ้น ROC (ลักษณะการทำงานของตัวรับ) แสดงให้เห็นภาพการแลกเปลี่ยนระหว่างอัตราผลบวกที่แท้จริง (การเรียกคืน) และอัตราผลบวกลวง ข้ามเกณฑ์ที่แตกต่างกัน แบบจำลองที่มีค่า AUC สูงกว่าจะมีเส้นโค้งใกล้กับมุมซ้ายบนมากขึ้น ซึ่งบ่งบอกถึงประสิทธิภาพที่ดีขึ้น AUC และ ROC ร่วมกันนำเสนอข้อมูลเชิงลึกเกี่ยวกับความสามารถในการจำแนกประเภทของแบบจำลองข้ามขอบเขตการตัดสินใจที่แตกต่างกัน

จากรูปที่ 3.41 และ 3.42 เป็นการวิเคราะห์ ROC-AUC ก่อนและหลังการใช้ k-Anonymity พบว่าหลังจากใช้ k-Anonymity ประสิทธิภาพโดยรวมของตัวจำแนกประเภทการเรียนรู้ของเครื่องแสดงให้เห็นการเปลี่ยนแปลงที่เห็นได้ชัดเจนไปสู่ความสอดคล้องมากขึ้น โดยมีความแปรปรวนของค่า AUC ในแต่ละแบบจำลองลดลง ก่อนการใช้ k-Anonymity นั้น Gradient Boosting เป็นตัวจำแนกประเภทที่มีประสิทธิภาพสูงสุด โดยมีค่า AUC อยู่ที่ 0.9182 ตามมาด้วย Random Forest มีค่า AUC ที่ 0.86 อย่างไรก็ตาม ตัวจำแนกประเภทเช่น K-Nearest Neighbors และ Support Vector Classifier เริ่มต้นประสบปัญหาโดยมีค่า AUC ที่ 0.6108 และ 0.61 ตามลำดับ หลังเป็นนิรนามค่า AUC สูงสุดลดลงเล็กน้อย โดยที่ Gradient Boosting มีค่า AUC ถึง 0.871 ในขณะที่ K-Nearest Neighbors ปรับปรุงอย่างมีนัยสำคัญเป็น 0.8141 ตัวจำแนกประเภทอื่น ๆ เช่น Random Forest, Gaussian Naïve Bayes และ Decision Tree รวมตัวกันอยู่ใกล้กันมากขึ้นด้วยค่า AUC ประมาณ 0.7969 ความแปรปรวนที่สังเกตได้ในผลลัพธ์ก่อนเป็นนิรนามลดลงอย่างมีนัยสำคัญ ซึ่งบ่งชี้ถึงประสิทธิภาพการทำนายที่สมดุลมากขึ้นในทุกแบบจำลอง แม้ว่าตัวจำแนกประเภทบางตัวจะมีการแลกเปลี่ยนประสิทธิภาพสูงสุดเล็กน้อย แต่กระบวนการทำให้เป็นนิรนามได้ปรับปรุงความทนทานของแบบจำลองอย่างมีประสิทธิภาพ และรับประกันผลลัพธ์ที่เสถียรยิ่งขึ้นในแบบจำลองต่าง ๆ ซึ่งแสดงให้เห็นถึงความสมดุลระหว่างการรักษาความเป็นส่วนตัวและความแม่นยำในการคาดการณ์ สามารถสรุปข้อมูลสำคัญในการวิเคราะห์เชิงเปรียบเทียบของ ROC-AUC Curve ได้ดังตารางที่ 3.10



รูปที่ 3.41 การวิเคราะห์ ROC-AUC Curve ก่อนใช้ k-Anonymity



รูปที่ 3.42 การวิเคราะห์ ROC-AUC Curve หลังใช้ k-Anonymity

ตารางที่ 3.10 เปรียบเทียบ ROC-AUC Curve ก่อนและหลังใช้ k-Anonymity

ตัวชี้วัด	ก่อนใช้ k-Anonymity	หลังใช้ k-Anonymity
ค่า AUC ที่ดีที่สุด	Gradient Boosting (0.9182)	Gradient Boosting (0.871)
ค่า AUC ที่น้อยที่สุด	K-Nearest Neighbors (0.6108)	Logistic Regression (0.777)
ค่า AUC ที่ดีที่สุดสำหรับ Support Vector Classifier	0.8192	0.7969
ความแปรปรวนของประสิทธิภาพ	สูง	ลดลง

4) การประเมินความเสี่ยงของการระบุตัวตนซ้ำอีกครั้ง: เป็นกระบวนการที่ใช้วิเคราะห์และประเมินว่าข้อมูลนิรนาม (Anonymized Data) สามารถถูกเชื่อมโยงกลับไปยังตัวตนจริงของบุคคลได้มากน้อยเพียงใด โดยเฉพาะในกรณีที่ข้อมูลมีการแบ่งปันหรือเผยแพร่สู่สาธารณะ การระบุความเสี่ยงนี้แบ่งออกเป็น 2 ขั้นตอนหลักดังนี้

4.1) การประเมินความเสี่ยงก่อนการประยุกต์ใช้ k-Anonymity: ชี้ให้เห็นถึงความสามารถของแบบจำลองในการจำแนกและจับคู่ข้อมูลได้อย่างแม่นยำ ซึ่งแม้ว่าจะเป็นผลดีต่อประสิทธิภาพของแบบจำลอง แต่ก็เป็นช่องโหว่ในมุมของความเป็นส่วนตัว เพราะแบบจำลองอาจเรียนรู้จากข้อมูลที่มีความเฉพาะเจาะจงสูง ทำให้เกิดความเสี่ยงที่ข้อมูลนี้อาจถูกใช้เพื่อระบุตัวตนซ้ำได้หากตกอยู่ในมือผู้ไม่หวังดี

4.2) การประเมินความเสี่ยงหลังการประยุกต์ใช้ k-Anonymity: ข้อมูลจะถูกปรับเปลี่ยนให้อยู่ในรูปแบบที่ยากต่อการระบุตัวตนโดยตรง เช่น การรวมกลุ่มข้อมูล หรือการปิดบังรายละเอียดบางส่วน ส่งผลให้แบบจำลองไม่สามารถเรียนรู้จากข้อมูลที่มีความเฉพาะเจาะจงเกินไปได้ ส่งผลให้ค่าความแม่นยำและคะแนนเอฟวันของแบบจำลองบางตัวลดลง แต่ในขณะเดียวกันก็ช่วยลดโอกาสในการระบุตัวตนซ้ำได้อย่างมีประสิทธิภาพ

4.3) ปัจจัยที่ส่งผลต่อความเสี่ยงในการระบุตัวตนซ้ำอีกครั้ง

(1) คุณลักษณะตัวระบุเสมือน (Quasi-Identifiers): เช่น อายุ เพศ วันเกิด และรหัสไปรษณีย์ ซึ่งสามารถใช้ร่วมกับแหล่งข้อมูลอื่น ๆ เพื่อติดตามตัวบุคคลได้

(2) ความหลากหลายของข้อมูล (Data Diversity): หากข้อมูลมีความหลากหลายต่ำ ความเสี่ยงในการระบุตัวตนจะสูงขึ้น

(3) การรวมข้อมูลจากหลายแหล่ง (Data Linkage): การรวมข้อมูลจากหลายแหล่งสามารถเพิ่มโอกาสในการระบุตัวตนซ้ำได้

4.4) บทบาทของ k-Anonymity ในการลดความเสี่ยง

(1) k-Anonymity เป็นเทคนิคที่รับรองว่าบุคคลในข้อมูลจะไม่สามารถแยกแยะได้จากบุคคลอื่นอย่างน้อย k คนขึ้นไปที่มีลักษณะเหมือนกันในกลุ่มเดียวกัน

(2) ช่วยลดความเสี่ยงจากการวิเคราะห์ย้อนหลังและการระบุตัวตนซ้ำ

(3) การใช้ k-Anonymity อาจส่งผลกระทบต่อความแม่นยำของแต่ละแบบ จำลองการเรียนรู้ของเครื่อง แต่ในขณะเดียวกันก็เพิ่มความปลอดภัยและความเป็นส่วนตัวของข้อมูล

ตารางที่ 3.11 ผลการประเมินความเสี่ยงของการระบุตัวตนซ้ำอีกครั้ง

Model	Before k-Anonymity		After k-Anonymity		Risk Level
	Accuracy	Macro F1-Score	Accuracy	Macro F1-Score	
Logistic Regression	0.778197	0.635794	0.782949	0.653998	Low
Support Vector Classifier	0.784766	0.570947	0.745772	0.427188	High
Random Forest	0.763802	0.497867	0.793711	0.655598	Low
Decision Tree	0.802795	0.740296	0.79986	0.722884	Low
K-Nearest Neighbors	0.754857	0.594079	0.786164	0.720352	Low
Gaussian Naïve Bayes	0.784486	0.643141	0.749406	0.695607	Low
Gradient Boosting	0.856604	0.793052	0.821803	0.74254	High

ตารางที่ 3.11 แสดงผลการวิเคราะห์การประเมินความเสี่ยงในการระบุตัวตนซ้ำจะประเมินประสิทธิภาพของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้ k-Anonymity โดยมุ่งเน้นไปที่ตัวชี้วัดหลักสองประการคือ Accuracy (ความถูกต้องในการทำนายโดยรวม) และ Macro F1-Score (ความสมดุลระหว่างความถูกต้องและการเรียกคืนข้ามคลาส) ระดับความเสี่ยงถูกกำหนดโดยประสิทธิภาพที่ลดลง โดยลดลงเกิน 0.05 จัดอยู่ในประเภทความเสี่ยงสูง และการลดลงเล็กน้อยเป็นความเสี่ยงต่ำ แบบจำลองที่มีความเสี่ยงต่ำได้แก่ Logistic Regression, Random Forest, Decision Tree, K-Nearest Neighbors และ Gaussian Naïve Bayes แสดงให้เห็นการเปลี่ยนแปลงเล็กน้อยในด้าน ประสิทธิภาพ ซึ่งบ่งชี้ว่าแบบจำลองเหล่านี้สร้างความสมดุลระหว่างการปกป้องความเป็นส่วนตัวและอรรถประโยชน์แบบจำลองอย่างมีประสิทธิภาพ ความสามารถในการปรับตัวแสดงให้เห็นว่ามีการพึ่งพารูปแบบเฉพาะที่สามารถระบุตัวตนได้น้อยลง ในทางกลับกัน แบบจำลองที่มีความเสี่ยงสูง เช่น Support Vector Classifier และ Gradient Boosting ประสบปัญหาการลดลงอย่างมาก โดยเฉพาะอย่างยิ่งใน Macro F1-Score โดยเน้นย้ำถึงการพึ่งพารายละเอียดข้อมูลที่ละเอียด โดยเฉพาะอย่างยิ่ง Support Vector Classifier ลดลงอย่างมากจาก 0.5709 เป็น 0.4271 ซึ่งสะท้อนถึงการสูญเสียความ สามารถในการทำข้อมูลให้เป็นลักษณะทั่วไปอย่างมาก ในทางตรงกันข้าม Gradient Boosting แม้ว่าจะยังมีประสิทธิภาพแต่ก็แสดงให้เห็นถึงความเสื่อมโทรมมากพอที่จะถือว่ามีความเสี่ยงสูง การค้นพบนี้เน้นย้ำว่าแบบจำลองที่แตกต่างกันตอบสนองต่อการไม่เปิดเผยตัวตน โดยแบบจำลองที่มีความเสี่ยงสูงจะมีความเสี่ยงสูงที่จะถูกระบุตัวตนซ้ำเนื่องจากการพึ่งพาลักษณะชุดข้อมูลที่แม่นยำ การประเมินเน้นย้ำถึงความสำคัญของการเลือกเทคนิคทำให้เป็นนิรนามอย่างเหมาะสมเพื่อสร้างสมดุลระหว่างความเป็นส่วนตัวของข้อมูลและประสิทธิภาพการคาดการณ์อย่างมีประสิทธิภาพ

3.4 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยฉบับนี้ มีรายละเอียดดังนี้

3.4.1 เทคโนโลยีบล็อกเชน (Blockchain Technology)

บล็อกเชนเป็นเทคโนโลยีแบบกระจายศูนย์ มีความน่าเชื่อถือ หลายธุรกิจจึงหันมาพัฒนาบล็อกเชนกันมากขึ้น โดยเฉพาะธุรกิจด้านการเงิน ปัจจุบันมหาวิทยาลัยในประเทศไทยเริ่มตื่นตัวกับการนำเทคโนโลยีบล็อกเชนเข้ามาใช้กับภาคการศึกษามากขึ้น ผนวกกับต้องรองรับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ต้องเป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(พีดีพีเอ) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ปีพ.ศ. 2559 (จีดีพีอาร์) ส่วนหนึ่งเพื่อสร้างมาตรฐานของความน่าเชื่อถือเพราะการออกเอกสารผ่านบล็อกเชนนั้นจะไม่สามารถแก้ไขหรือปลอมแปลงได้ อีกส่วนหนึ่งเพื่อสร้างการเรียนรู้ใหม่ ๆ ผ่านโลกเมตาเวิร์ส (Metaverse) ซึ่งต้องใช้บล็อกเชนเป็นโครงสร้างพื้นฐานของการทำธุรกรรมต่าง ๆ เช่นเดียวกัน

แพลตฟอร์มบล็อกเชน (Blockchain Platforms) คือ โซลูชันซอฟต์แวร์ที่ช่วยให้ธุรกิจสร้างแอปพลิเคชันที่ใช้เทคโนโลยีบล็อกเชน ซึ่งอำนวยความสะดวกในบันทึกธุรกรรมและติดตามทรัพย์สินในเครือข่ายธุรกิจ ในปัจจุบันมีแพลตฟอร์มเกิดขึ้นมากมาย แต่ในการวิจัยฉบับนี้ผู้วิจัยได้เลือกแพลตฟอร์ม เพื่อใช้ในการทดลองเชิงเปรียบเทียบ จะเลือกใช้แพลตฟอร์มที่แตกต่างกัน เช่น ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain)

3.4.2 สัญญาอัจฉริยะ (Smart Contract)

สัญญาอัจฉริยะเป็นโปรแกรมที่บังคับตนเองและดำเนินการด้วยตัวเอง ซึ่งเป็นข้อกำหนดและเงื่อนไขเฉพาะข้อตกลงโดยใช้รหัสซอฟต์แวร์และโครงสร้างพื้นฐานการคำนวณ สัญญาอัจฉริยะเป็นโปรแกรมกระจายศูนย์ที่ขยายการใช้งานเครือข่ายบล็อกเชนพื้นฐาน โปรแกรมนี้เปลี่ยนรูปไม่ได้และได้รับการตรวจสอบด้วยการเข้ารหัสเพื่อความน่าเชื่อถือ คุณสมบัติบางอย่างของสัญญาอัจฉริยะได้สืบทอดมาจากพื้นฐานของเทคโนโลยีบล็อกเชน คุณลักษณะเหล่านี้ช่วยให้มีการจ้างงานเกี่ยวกับสัญญาอัจฉริยะได้หลากหลายมากขึ้น โดยทั่วไปแล้ว สัญญาอัจฉริยะจะดำเนินการในโหมดการให้บริการระหว่างบุคคลหรือบริษัทโดยตรง (เพียร์ทูเพียร์, peer-to-peer) โดยไม่มีการแทรกแซงจากคนกลาง พวกเขาให้ความพร้อมในการให้บริการ โดยไม่พึ่งพาการรวมศูนย์แต่อย่างใด และอนุญาตให้ดำเนินการธุรกรรมอัตโนมัติเมื่อถึงเงื่อนไขที่กำหนดไว้ล่วงหน้า

3.4.3 ภาษาซอลิดิตี (Solidity Language)

ซอลิดิตี เป็นภาษาเชิงวัตถุ (Object Oriented Programming – OOP) ระดับสูงที่พัฒนาขึ้นโดยเฉพาะสำหรับการสร้างและใช้งานสัญญาอัจฉริยะบนแพลตฟอร์มการพัฒนาบล็อกเชนต่าง ๆ โดยเฉพาะอีเธอเรียมซอลิดิตี (Ethereum Solidity) การเขียนด้วยภาษาซอลิดิตีทำให้สามารถสร้างสัญญาสำหรับการใช้งานต่าง ๆ ได้เช่น การลงคะแนน การระดมทุน การประมูลของคนพิการทางสายตา การซื้อระยะไกลที่ปลอดภัย และกระเป๋าเงินแบบหลายลายเซ็น สัญญาอัจฉริยะซอลิดิตี

(Solidity Smart Contracts) ช่วยให้ทำธุรกรรมดิจิทัลที่มีความปลอดภัยสูงซึ่งจะไม่เกี่ยวข้องกับคนกลาง สัญญาอัจฉริยะถูกรวมเข้ากับเทคโนโลยีบล็อกเชน ทำให้สามารถตรวจสอบย้อนกลับได้ โปร่งใส่ ย้อนกลับไม่ได้และในทันที

3.4.4 ภาษาไพทอนและไลบรารี่ Scikit-learn (Python and Scikit-learn)

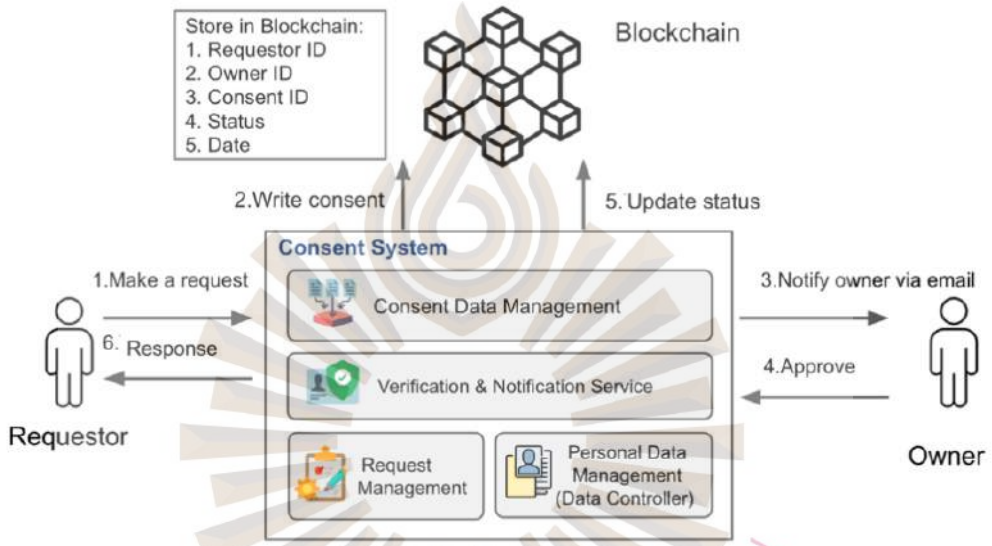
ภาษาไพทอน คือ ภาษาโปรแกรมคอมพิวเตอร์ระดับสูง โดยถูกออกแบบมาให้เป็นภาษาสคริปต์ที่อ่านง่าย โดยตัดความซับซ้อนของโครงสร้างและไวยากรณ์ของภาษาออกไป ในส่วนของการแปลงชุดคำสั่งที่เราเขียนให้เป็นภาษาเครื่อง ไพทอนมีการทำงานแบบ Interpreter คือเป็นการแปลงชุดคำสั่งทีละบรรทัด เพื่อป้อนเข้าสู่หน่วยประมวลผลให้คอมพิวเตอร์ทำงานตามที่เราต้องการ นอกจากนั้นภาษาไพทอนยังสามารถนำไปใช้ในการเขียนโปรแกรมได้หลาก หลายประเภท โดยไม่ได้จำกัดอยู่ที่งานเฉพาะทางใดทางหนึ่ง (General-purpose Language) จึงทำให้มีการนำไปใช้กันอย่างแพร่หลายในหลายองค์กรใหญ่ระดับโลกเช่น Google YouTube Instagram Dropbox NASA Netflix Spotify Amazon Python เป็นต้น

Scikit-Learn หรือที่รู้จักในชื่อ Sklearn เป็นมอดูลหนึ่งของภาษาไพทอน เป็นแพ็กเกจที่รวบรวมไลบรารี่ด้านการเรียนรู้ของเครื่องเอาไว้ และถูกออกแบบมาให้ทำงานร่วมกับไลบรารี่ของภาษาไพทอน อย่าง Numpy และ Scipy ได้ดี นอกจากนี้ Sklearn ยังเป็นโอเพนซอร์สที่เปิดให้ผู้ที่สนใจสามารถเข้าไปพัฒนาต่อยอดได้ และที่ทำให้ทุกคนต่างยอมรับก็คือ เป็นแหล่งรวมไลบรารี่และอัลกอริทึมที่เน้นไปในด้านของการเรียนรู้ของเครื่อง ซึ่ง Sklearn จะเน้นในส่วนของการสร้างแบบจำลองเพื่อทำนายหรือพยากรณ์ต่าง ๆ มีเครื่องมือที่ได้รับความนิยมเช่น การถดถอย (Regressing) การจำแนกประเภท (Classification) การจัดกลุ่ม (Clustering) การเลือกรุ่น (Model Selection) การลดมิติ (Dimensionality Reduction) และการประมวลผลล่วงหน้า (Pre-processing)

3.4.5 ระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต หรือ RSU-CMS (RSU-Consent Management System)

ระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต จะใช้แพลตฟอร์มบล็อกเชนที่ชื่อว่าเอ็กซ์เชน (xCHAIN) จากรูปที่ 3.43 แสดงแผนผังการจัดการความยินยอมของมหาวิทยาลัยรังสิตซึ่งเป็นรูปแบบแนวคิดในการจัดการข้อมูลส่วนบุคคลที่บูรณาการร่วมกับสัญญาอัจฉริยะภาย

ในโครงสร้างพื้นฐานบล็อกเชนส่วนตัว ระบบนี้ได้รับการออกแบบมาเพื่อจัดการความยินยอมอย่างปลอดภัยและเพื่อตรวจสอบตัวตนของเจ้าของข้อมูลภายในสภาพแวดล้อมบล็อกเชนส่วนตัว ทั้งนี้เพื่อเพิ่มความเป็นส่วนตัวและความปลอดภัยของข้อมูล เพื่อให้มั่นใจว่าสอดคล้องและปฏิบัติตามกฎหมายคุ้มครองข้อมูล เช่น พีดีพีเอ ระบบ RSU-CMS ประกอบด้วย 4 มอดูล ได้แก่ มอดูลการจัดการข้อมูลความยินยอม มอดูลบริการการยืนยันและการแจ้งเตือน มอดูลการจัดการคำขอ และมอดูลการจัดการส่วนบุคคล



รูปที่ 3.43 สถาปัตยกรรมของระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต

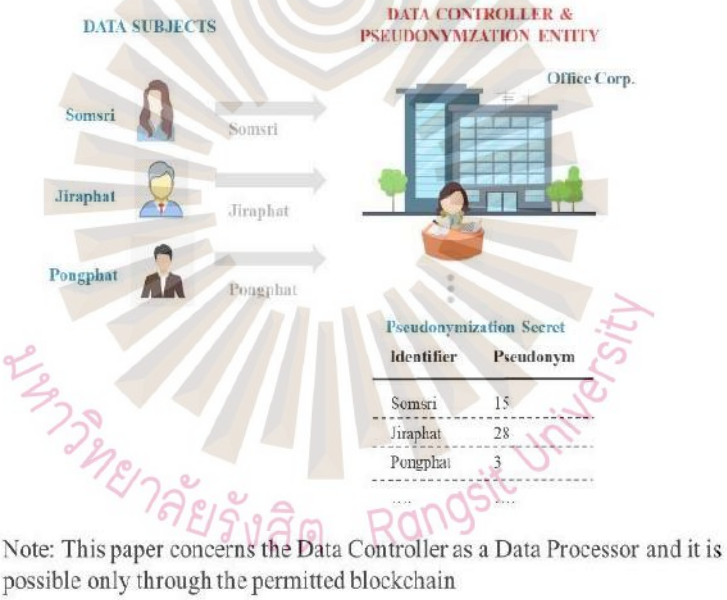
3.4.6 เทคนิคการแฝงข้อมูล (Pseudonymization Technique)

ตามข้อกำหนดของจีดีพีอาร์ การแฝงข้อมูลคือการประมวลผลข้อมูลส่วนบุคคลเพื่อไม่ให้เชื่อมโยงกับข้อมูลเฉพาะอีกต่อไปโดยไม่ต้องใช้ข้อมูลเพิ่มเติมอีก (European Network and Information Security Agency, 2019) หากต้องการใช้ชุดข้อมูลแฝง “ข้อมูลเพิ่มเติม” จะต้องถูก “เก็บแยกจากกันและอยู่ภายใต้มาตรการทางเทคนิคและองค์กร เพื่อให้แน่ใจว่าไม่มีการระบุแหล่งที่มาของบุคคลที่ระบุได้หรือสามารถระบุตัวตนได้”

ตัวระบุเสมือน (Quasi-identifier) ถูกกำหนดโดย The Organisation for Economic Co-operation and Development (OECD) ให้เป็นแอตทริบิวต์ทางอ้อมอื่น ๆ ทั้งหมดที่สามารถระบุข้อมูลส่วนบุคคลอื่น ๆ ซ้ำได้ (The Organisation for Economic Co-operation and Development, 2005)

ตามข้อกำหนดของจีดีพีอาร์ คำจำกัดความของการแฝงข้อมูล “ข้อมูลเพิ่มเติม” รวมถึงตัวระบุเฉพาะและตัวระบุเสมือนจะถูกแบ่งออกจากตารางต้นฉบับและจัดเก็บแยกต่างหากในบล็อกเชน ข้อมูลอื่น ๆ ทั้งหมดยกเว้นตัวระบุทั้งสองที่ได้กล่าวมาแล้วจะถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์แม่ข่าย รูปแบบนี้มีไว้เพื่อรักษาข้อมูลส่วนบุคคลต้นฉบับไว้ ข้อมูลที่ระบุตัวตนได้โดยตรงจะถูกจัดเก็บแยกต่างหากและปลอดภัยจากข้อมูลที่ประมวลผล

จากรูปที่ 3.44 แสดงถึงแนวปฏิบัติจาก European Union Agency for Cybersecurity (ENISA) ดังตัวอย่างโดยใช้วิธีการแฝงข้อมูล ตัวอย่างนี้มีข้อเสียสองประการด้วยกัน คือ 1) แม้ว่าตารางการแมปในรูปนี้จะเก็บเป็นความลับภายในบริษัท แต่ก็ถูกจัดเก็บไว้ในที่เก็บข้อมูลเดียวกัน 2) กุญแจการแมปสามารถทำซ้ำได้ ดังนั้นจึงไม่มีกุญแจหลัก



รูปที่ 3.44 แสดงตัวอย่างของเทคนิคการแฝงข้อมูล

3.4.7 กระบวนการทำให้เป็นนิรนาม (Anonymization Process) โดยใช้อัลกอริทึม k-Anonymity แบบวิธีการทำให้เป็นลักษณะทั่วไป (Generalization)

กระบวนการทำให้เป็นนิรนาม (Anonymization process) โดยทั่วไปจะเกี่ยวข้องกับการลบข้อมูลหรือการปิดบังข้อมูลของข้อมูลส่วนบุคคลที่ระบุตัวบุคคลนั้นได้ (Personally Identifiable Information - PII) เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ รายละเอียดหนังสือเดินทาง หรือหมายเลขประกัน

สังคม เป็นต้น ด้วยเหตุนี้ ค่าต่าง ๆ จะถูกแทนที่หรือลบออกโดยใช้เทคนิคการเข้ารหัส หรือการเพิ่มสัญญารบกวนแบบสุ่ม หรือ k-Anonymity เพื่อปกป้องข้อมูล

k-Anonymity: การเปิดเผยข้อมูลได้รับการกล่าวขานว่าเป็นไปตาม k-Anonymity หากมีอยู่อย่างน้อย k รายการสำหรับทุกค่าผสมที่เป็นไปได้ของตัวระบุเสมือน การใช้งาน k-Anonymity นั้นใช้เทคนิคที่พิเศษบางอย่างที่เรียกว่าเทคนิคการเปลี่ยนแปลง (Transformation Techniques) เช่น การทำให้เป็นลักษณะทั่วไป (Generalization) การปราบปราม (Suppression) และการบันทึกรหัสสากล (Global Recording) เป็นต้น

งานวิจัยฉบับนี้ ผู้วิจัยเลือกใช้เทคนิค k-Anonymity ด้วยวิธีการทำให้เป็นลักษณะทั่วไป (Generalization Techniques) ซึ่งเป็นการแทนที่ค่าเฉพาะด้วยค่าทั่วไป ตัวอย่างเช่น รหัสไปรษณีย์ในชุดข้อมูลสามารถทำให้เป็นเขตหรือแขวงได้ (เช่น เปลี่ยนจาก 10500 เป็น 105xx) อายุอาจถูกแทนจัดอยู่ในกลุ่มอายุ (เช่น การจัดกลุ่มอายุ 22 ปี ให้อยู่ในกลุ่มอายุ [20 – 29])

3.5 การเก็บรวบรวมข้อมูล

งานวิจัยฉบับนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้วิธีการทดลองจริง (True Experiment) ซึ่งการเก็บรวบรวมข้อมูลจะต้องเก็บจากแหล่งข้อมูล 2 ประเภท ดังนี้

3.5.1 ข้อมูลปฐมภูมิ (Primary Data) ผู้วิจัยเก็บรวบรวมข้อมูลปฐมภูมิด้วยวิธีการทดลองจริง โดยใช้ทรัพยากรหลักของมหาวิทยาลัยรังสิต เช่น ระบบเครือข่ายอินเทอร์เน็ต ระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิตที่บูรณาการร่วมกับสัญญาอัจฉริยะบนบล็อกเชนโดยทดลองบนแพลตฟอร์มที่แตกต่างกัน เช่น ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain) ซึ่งการทดลองทำให้มีการทำธุรกรรมจริง และมีค่าธรรมเนียม (Gas fee and Transaction fee) ที่เกิดขึ้นจริง ผนวกกับใช้ชุดข้อมูลรายได้สำหรับผู้ใหญ่ (US Adult Income dataset) หรือเรียกอีกชื่อหนึ่งว่า “adult.csv” เป็นชุดข้อมูลการสำรวจประชากรของประเทศสหรัฐอเมริกาในปีพ.ศ. 2537 ที่ได้มาจาก UCI Machine Learning Repository เป็นชุดข้อมูลตัวอย่างที่ได้รับความนิยมเป็นอย่างมากเพื่อใช้เป็นเกณฑ์มาตรฐานในการปกปิดข้อมูล

3.5.2 ข้อมูลทุติยภูมิ (Secondary Data) ผู้วิจัยเก็บรวบรวมข้อมูลสถิติ ตัวเลขต่าง ๆ ตลอดจนแนวคิดและทฤษฎีที่เกี่ยวข้อง จากการค้นคว้าเอกสาร หนังสือ ผลงานวิจัยที่เกี่ยวข้องทั้งในและ

ต่างประเทศ รวมถึงข้อมูลจากสื่ออิเล็กทรอนิกส์และฐานข้อมูลทางอินเทอร์เน็ตของหน่วยงานที่เกี่ยวข้อง

3.6 การวิเคราะห์ข้อมูล

เมื่อได้ข้อมูลตามต้องการ จึงนำมาวิเคราะห์สรุปด้วยการวิเคราะห์ข้อมูลเชิงเปรียบเทียบ (Comparative Analysis) แล้วนำเสนอในลักษณะของการบรรยายเชิงพรรณา โดยใช้แนวคิดและทฤษฎีที่เกียวกับเทคโนโลยีบล็อกเชนที่มาเป็นระบบช่วยเหลือในด้านการจัดการข้อมูลส่วนบุคคลผ่านกระบวนการจัดการความยินยอมและใช้เทคนิคการแฝงข้อมูลเพื่อให้สอดคล้องและปฏิบัติตามข้อกำหนดกฎหมายการคุ้มครองข้อมูลส่วนบุคคล มาเป็นกรอบในการวิเคราะห์เพื่อให้ได้คำตอบตามวัตถุประสงค์ของการศึกษาวิจัย

3.6.1 การเปรียบเทียบประสิทธิภาพการทำงานของแพลตฟอร์มบล็อกเชน

ผู้วิจัยได้ทำการวิเคราะห์เชิงเปรียบเทียบประสิทธิภาพการทำงานของแต่แพลตฟอร์มบล็อกเชนด้วยการเขียนโปรแกรมด้วยภาษาซอลิดิตี เพื่อการประมวลผลสัญญาอัจฉริยะบนบล็อกเชน โดยประมวลผลโปรแกรมบนแพลตฟอร์มบล็อกเชนที่แตกต่าง 4 แพลตฟอร์ม ได้แก่ ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain) โดยผู้วิจัยสนใจเฉพาะในส่วนของประสิทธิภาพ (แบนด์วิดท์, เวลาการทำธุรกรรม) ค่าธรรมเนียมการทำธุรกรรม (ธุรกรรม, ก๊าซ) และมาตรฐานการรักษาความปลอดภัย

3.6.2 การเปรียบเทียบประสิทธิภาพของการใช้เทคนิคการแฝงข้อมูลบนบล็อกเชน

งานวิจัยนี้จะใช้มาตรวัดในการวัดประสิทธิภาพของการใช้เทคนิคการแฝงข้อมูลบนบล็อกเชนด้วยข้อมูลที่ถูกปกปิดคือ ความแม่นยำของอัลกอริทึมการเรียนรู้ของเครื่อง จำนวนการสูญเสียข้อมูล และอัตราความเสี่ยงที่จะถูกโจมตีเพื่อระบุตัวตนซ้ำอีกครั้ง โดยที่งานวิจัยนี้ต้องการที่จะศึกษาว่าบล็อกเชนมีส่วนช่วยเหลือในการป้องกันและรักษาความเป็นต้นฉบับของข้อมูลโดยการใช้เทคนิคการแฝงข้อมูลน้อยลงหรือไม่เมื่อเทียบกับการทำการปกปิดข้อมูลเพียงอย่างเดียว และทำการประเมินประสิทธิภาพของแต่ละอัลกอริทึมการเรียนรู้ของเครื่อง มีการประเมินเชิงลึกเกี่ยวกับประสิทธิภาพของอัลกอริทึมของการเรียนรู้ด้วยเครื่องแตกต่างกัน 7 แบบ ได้แก่ เกรเดียนต์บูทติ้ง

(Gradian Booting - GB) เกาส์เซียนนาอีฟเบย์ (Gaussian Naïve Bayes – GNB) การถดถอยลอจีสติก (Logistic Regression – LR) ต้นไม้ป่าสุ่ม (Random Forest – RF) ซัพพอร์ตเวกเตอร์คลาสสิฟายเออร์ (Support Vector Classifier – SCV) ต้นไม้การตัดสินใจ (Decision Tree – DT) เพื่อนบ้านที่อยู่ใกล้ฉันมากที่สุด (K-Nearest Neighbor – KNN) การเปรียบเทียบจะดำเนินการโดยการประเมินประสิทธิภาพทั้งก่อนและหลังการใช้เทคนิคบางอย่างเช่น k-Anonymity และการใช้การแฝงข้อมูล

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 4

ผลการวิจัย

งานวิจัยเรื่องระบบช่วยเหลือด้วยเทคโนโลยีบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมและระบบการแฝงข้อมูล ระเบียบวิธีวิจัยเป็นการวิจัยเชิงปริมาณ (Quantitative Research) ผ่านการวิจัยเชิงทดลองที่แท้จริง (True Experiment) เป็นการวิจัยที่มีการเก็บข้อมูลและวิเคราะห์ข้อมูลในเชิงเปรียบเทียบ (Comparative Analysis) งานวิจัยนี้นำเสนอผลการทดลองที่เกิดขึ้นในสองส่วนสำคัญ คือ การทดสอบการใช้สัญญาอัจฉริยะบนบล็อกเชนในระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS) และการประยุกต์ใช้เทคนิคการแฝงข้อมูล (Pseudonymization) ร่วมกับโครงการนำร่อง RSU-Data-Anonymization โดยใช้เทคนิค k-Anonymity เพื่อปกป้องความเป็นส่วนตัวของข้อมูลในบริบทต่าง ๆ และปฏิบัติตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA – พีดีพีเอ)

4.1 ผลทดลองการวิเคราะห์เชิงเปรียบเทียบของแพลตฟอร์มบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมโดยชุดคำสั่งสัญญาอัจฉริยะ

การทดลองนี้เป็นการนำระบบบริหารจัดการความยินยอมโดยใช้ชุดคำสั่งสัญญาอัจฉริยะที่พัฒนาด้วยภาษาซอลิดิตีมาประมวลผลบนแพลตฟอร์มบล็อกเชนต่าง ๆ ในงานวิจัยฉบับนี้จะมุ่งเน้นไปที่แพลตฟอร์มบล็อกเชน 4 ราย ได้แก่ ไบแนนซ์ (Binance Smart Chain) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain) โดยอาศัยคุณลักษณะเด่นที่สำคัญของเทคโนโลยีบล็อกเชน เช่น ข้อมูลธุรกรรมมีความโปร่งใส และข้อมูลย้อนกลับไปแก้ไขไม่ได้ ซึ่งข้อมูลที่เข้าถึงจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน สามารถสรุปรายละเอียดจากการทดลองได้ดังนี้

4.1.1 การประเมินประสิทธิภาพของระบบบริหารจัดการความยินยอม:

4.1.1.1 วัตถุประสงค์: ระบบบริหารจัดการความยินยอม (RSU-CMS) ได้รับการออกแบบด้วยเทคโนโลยีสัญญาอัจฉริยะ (Smart Contracts) บนบล็อกเชน เพื่อเพิ่มความโปร่งใส (Transparency) ความปลอดภัย (Security) และความน่าเชื่อถือ (Reliability) ในกระบวนการจัดการข้อมูลความยินยอม

ของผู้ใช้ ระบบนี้มีจุดหมายเพื่อลดข้อผิดพลาดที่อาจเกิดจากการจัดการด้วยมนุษย์และเพิ่มความเชื่อมั่นให้กับผู้ใช้งานในด้านความปลอดภัยและการเข้าถึงข้อมูล

4.1.1.2 ผลการประเมิน:

1) การจัดการความยินยอมแบบอัตโนมัติ: การใช้สัญญาอัจฉริยะ (Smart Contracts) ช่วยเปลี่ยนกระบวนการจัดการความยินยอมจากรูปแบบเดิมที่อาจเกิดข้อผิดพลาด (เช่น การลืมบันทึก ข้อมูลหรือบันทึกข้อมูลผิดพลาด) ให้กลายเป็นกระบวนการอัตโนมัติที่สามารถตรวจสอบย้อนหลังได้ง่าย

1.1) กระบวนการอัตโนมัติ: ทุกการบันทึกและการปรับปรุงข้อมูลดำเนินการตามเงื่อนไขที่กำหนดในสัญญาอัจฉริยะโดยไม่ต้องมีการแทรกแซงจากมนุษย์

1.2) การตรวจสอบย้อนหลัง: ระบบอนุญาตให้ผู้ใช้งานและผู้เกี่ยวข้องตรวจสอบประวัติการบันทึกความยินยอมได้แบบเรียลไทม์ผ่านระบบบล็อกเชน ซึ่งสร้างความน่าเชื่อถือในข้อมูลที่จัดเก็บ

2) การเก็บข้อมูลในรูปแบบที่ไม่สามารถเปลี่ยนแปลงได้: การบันทึกข้อมูลความยินยอมลงในบล็อกเชนช่วยให้ข้อมูลผยู่ในรูปแบบที่ไม่สามารถเปลี่ยนแปลงได้ ซึ่งเพิ่มระดับความปลอดภัยในหลายด้าน ได้แก่

2.1) ความมั่นคงของข้อมูล: การเก็บข้อมูลในรูปแบบที่ไม่สามารถเปลี่ยนแปลงได้ ป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

2.2) การป้องกันการโจมตี: เนื่องจากข้อมูลไม่สามารถเปลี่ยนแปลงได้ การโจมตีเพื่อปลอมแปลงหรือดัดแปลงข้อมูลจึงถูกลดความเสี่ยงไปอย่างมาก

2.3) ความโปร่งใส: ผู้ใช้งานสามารถมั่นใจได้ว่าข้อมูลที่ถูกบันทึกเป็นของแท้และไม่ได้ถูกแก้ไข

3) รองรับผู้ใช้ในระดับมหาวิทยาลัย: RSU-CMS ได้รับการออกแบบให้สามารถรองรับปริมาณผู้ใช้งานจำนวนมากในระดับมหาวิทยาลัย เช่น อาจารย์ นักศึกษา และบุคลากร ซึ่งมีการบันทึกธุรกรรมเกี่ยวกับความยินยอมอย่างต่อเนื่อง

3.1) ความสามารถในการปรับขยาย: ระบบสามารถรองรับธุรกรรมจำนวนมากในเวลาเดียวกันโดยไม่ส่งผลกระทบต่อประสิทธิภาพ

3.2) ความเสถียร: แม้มีปริมาณธุรกรรมที่เพิ่มขึ้น ระบบยังคงทำงานได้อย่างราบรื่น ด้วยโครงสร้างแบบกระจายศูนย์ของบล็อกเชน

4.1.1.3 ผลการทดสอบในเชิงปฏิบัติ:

1) การลดข้อผิดพลาดจากมนุษย์: หลังจากนำสัญญาอัจฉริยะมาใช้ ระบบสามารถลดข้อผิดพลาดในการบันทึกข้อมูลได้ เมื่อเทียบกับการจัดการด้วยมนุษย์

2) ความโปร่งใสในการใช้งาน: ผู้ใช้งานในระบบสามารถตรวจสอบประวัติการบันทึกความยินยอมของตนเองได้ผ่านบล็อกเชน ซึ่งเพิ่มความมั่นใจและความโปร่งใสในกระบวนการ

4.1.1.4 สรุปผลการทดลอง: การใช้สัญญาอัจฉริยะบนบล็อกเชนช่วยเพิ่มประสิทธิภาพและความน่าเชื่อในระบบ RSU-CMS โดยทำให้กระบวนการจัดการความยินยอมเป็นอัตโนมัติ ปลอดภัย และโปร่งใส ทั้งนี้ ระบบยังคงสามารถรองรับการใช้งานในระดับมหาวิทยาลัยได้อย่างมีประสิทธิภาพ แม้ในกรณีที่มีปริมาณธุรกรรมจำนวนมาก

4.1.2 การประเมินประสิทธิภาพของระบบบริหารจัดการข้อมูล:

4.1.2.1 รายละเอียดการทดลอง: การทดลองนี้เน้นการเปรียบเทียบประสิทธิภาพในเชิงเทคนิคของ 4 แพลตฟอร์มบล็อกเชน ได้แก่ ไบแนนซ์ (Binance) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และเรอิเชน (REI Chain) เพื่อพิจารณาความเหมาะสมในการนำมาใช้ในระบบ RSU-CMS โดยเปรียบ เทียบใน 3 มิติสำคัญ ๆ ได้แก่

1) เวลาประมวลผล (Transaction Time): ความเร็วในการดำเนินธุรกรรม

2) ค่าใช้จ่าย (Transaction Fee): ค่าธรรมเนียมที่เกิดขึ้นจากการดำเนินธุรกรรม

3) ระดับความปลอดภัย (Resistance to Attack): ระดับความทนทานต่อการโจมตีไซเบอร์

4.1.2.2 ผลการทดลอง:

1) เวลาประมวลผล (Transaction Time):

1.1) เรอิเชน: ใช้เวลาประมวลผลเร็วที่สุดเพียง 1 วินาที เหมาะสำหรับงานที่ต้องการการยืนยันทันที เช่น ระบบแจ้งเตือนหรือการชำระเงินขนาดเร็วที่ไม่ซับซ้อน

1.2) ไบแนนซ์: ใช้เวลาประมวลผลเฉลี่ย 3 วินาที เหมาะสำหรับแอปพลิเคชันที่ต้องการการประมวลผลอย่างรวดเร็ว เช่น การชำระเงินออนไลน์แบบเรียลไทม์

1.3) เอ็กซ์เชน: ใช้เวลาประมวลผลเฉลี่ย 4.4 วินาที เป็นแพลตฟอร์มที่สมดุลในด้านความเร็วและประสิทธิภาพ เหมาะสำหรับแอปพลิเคชันที่ต้องการทั้งความเร็วและการรองรับธุรกรรมขนาดใหญ่

1.4) อีเธอเรียม: ใช้เวลาประมวลผลช้าที่สุดที่ 15 วินาที เนื่องจากกลไกฉันทามติแบบ Proof of Stake (PoS) ที่มีลำดับการยืนยันที่ซับซ้อน เหมาะสำหรับงานที่ต้องการความปลอดภัย สูง เช่น การจัดเก็บข้อมูลส่วนบุคคล

2) ค่าใช้จ่าย (Transaction Fee):

2.1) เรอิเชน: มีค่าธรรมเนียมต่ำที่สุดที่ $0.0013 ต่อธุรกรรม ใช้พลังงานน้อยและเป็นมิตรกับสิ่งแวดล้อม เป็นมิตรกับงบประมาณมากที่สุด ต้นทุนการทำธุรกรรมที่ต่ำมากนี้ทำให้เรอิเชนเป็นตัวเลือกที่คุ้มค่าสำหรับการใช้งานกรณีต่าง ๆ เหมาะสำหรับงานที่เน้นลดต้นทุน เช่น การจัดเก็บข้อมูลขนาดใหญ่

2.2) เอ็กซ์เชน: มีค่าธรรมเนียมต่ำที่ $0.13 ทำให้เป็นตัวเลือกที่ดีสำหรับนักวิจัยที่กำลังมองหาธุรกรรมที่คุ้มค่า และเป็นตัวเลือกที่ดีสำหรับแอปพลิเคชันที่ต้องการความสมดุลระหว่างค่าใช้จ่ายและความเร็ว ทำให้เหมาะสำหรับการใช้งานที่หลากหลาย

2.3) ไบแนนซ์: มีค่าธรรมเนียมปานกลางที่ $0.68 เสนอการทำธุรกรรมที่คุ้มค่าโดยมีค่าธรรมเนียมที่ค่อนข้างต่ำ ทำให้เป็นตัวเลือกที่น่าสนใจสำหรับนักวิจัยที่กำลังมองหาสภาพแวดล้อมบล็อกเชนที่คุ้มค่า เหมาะสมสำหรับการใช้งนในระบบที่ต้องการความเร็วและการรองรับธุรกรรมจำนวนมากได้อย่างมีประสิทธิภาพและประหยัด

2.4) อีเธอเรียม: มีค่าธรรมเนียมสูงสุดที่ $1.19 เนื่องจากโครงสร้างการคำนวณค่าก๊าซและการใช้งานก๊าซสำหรับธุรกรรมที่ซับซ้อน แม้จะมีต้นทุนที่สูงขึ้นแต่การนำไปใช้อย่างแพร่หลายและความสามารถของสัญญาอัจฉริยะขั้นสูงมีส่วนช่วยให้มีความน่าดึงดูดใจ

3) ความปลอดภัย (Resistance to Attack): เป็นการประเมินและวิเคราะห์มาตรการรักษาความปลอดภัยและความสามารถของแพลตฟอร์มบล็อกเชนต่าง ๆ เพื่อวัดประสิทธิภาพในความทนทานในการโดนเจาะระบบหรือการโจมดีทางไซเบอร์

3.1) อีเธอเรียม: มีความปลอดภัยสูงสุดที่ระดับ 9/10 มีโหนดจำนวนมาก (มากกว่า 500,000 โหนด) และใช้กลไกฉันทามติแบบ PoS ที่แข็งแกร่งและปลอดภัยยิ่งขึ้น สถาปัตยกรรมและแนวทางปฏิบัติด้านความปลอดภัยของอีเธอเรียมมีส่วนช่วยในการป้องกันภัยคุมคามต่อการถูกโจมตีที่อาจจะเกิดขึ้น

3.2) ไบแนนซ์: มีความปลอดภัยรองลงมาที่ระดับ 7/10 และใช้กลไกฉันทามติแบบ PoSA แต่มีโหนดจำนวนน้อยกว่าอีเธอเรียม ไบแนนซ์ได้ใช้มาตรการรักษาความ

ปลอดภัยทางไซเบอร์ที่แข็งแกร่ง ใช้ประโยชน์จากความเชี่ยวชาญในอุตสาหกรรมของไบแนนซ์ด้านสกุลเงินดิจิทัล โดยใช้เทคนิคการเข้ารหัสขั้นสูง กลไกฉันทามติที่ปลอดภัย และการตรวจสอบความปลอดภัยเป็นประจำเพื่อวิเคราะห์ช่องโหว่และเพิ่มความทนทานต่อภัยคุกคามที่อาจเกิดขึ้น

3.3) เอ็กซ์เชน: มีความปลอดภัยระดับปานกลางที่ 4/10 มีโหนดจำกัด จึงมีความเสี่ยงสูงต่อการถูกโจมตี แต่มีการผสานรวมแนวทางปฏิบัติด้านความปลอดภัยที่ทันสมัยเพื่อเพิ่มความทนทานต่อการพยายามเจาะระบบ ความคล่องตัวของแพลตฟอร์มช่วยให้ปรับตัวเข้ากับแนวโน้มการเจาะระบบที่เกิดขึ้นใหม่ได้อย่างรวดเร็วและมีประสิทธิภาพ

3.4) เรอิเชน: มีความปลอดภัยต่ำสุดที่ระดับ 2/10 เนื่องจากโครงสร้างที่มีโหนดจำนวนน้อยและการกระจายศูนย์ต่ำ ทำให้เสี่ยงต่อการถูกโจมตี

4.1.2.3 สรุปผลการทดลอง:

1) ไบแนนซ์: เหมาะสำหรับงานที่เน้นความเร็ว ในการดำเนินธุรกรรมและความปลอดภัยปานกลาง เช่น ระบบการชำระเงินออนไลน์ที่มีผู้ใช้จำนวนมาก

2) เรอิเชน: เหมาะสำหรับงานที่ต้องการลดต้นทุนและประมวลผลธุรกรรมที่มีขนาดเล็กและไม่ซับซ้อน เช่น ระบบที่เกี่ยวข้องกับ IoT

3) อีเธอเรียม: เหมาะสำหรับงานที่ต้องการความปลอดภัยสูง เช่น การจัดเก็บข้อมูลสำคัญที่ต้องการการรับรองความปลอดภัยและความเชื่อถือ

4) เอ็กซ์เชน: เหมาะสำหรับงานที่ต้องการสมดุลระหว่างความเร็วและความปลอดภัย เช่น แอปพลิเคชันในองค์กรที่ต้องการประมวลผลที่มั่นคง และนักวิจัยเห็นว่าเอ็กซ์เชนเหมาะสมกับการนำมาใช้ร่วมกับระบบ RSU-CMS เพื่อให้ได้ผลลัพธ์ที่เหมาะสมและมีประสิทธิภาพ

4.1.3 การเปรียบเทียบประสิทธิภาพระหว่างแพลตฟอร์มบล็อกเชน: จะช่วยให้เข้าใจถึงจุดเด่นและข้อจำกัดของแต่ละแพลตฟอร์มสำหรับการใช้งานในระบบ RSU-CMS ที่เน้นการจัดการความยินยอมของผู้ใช้งาน

4.1.3.1 จุดเด่นและข้อจำกัดของแต่ละแพลตฟอร์ม:

1) ไบแนนซ์:

1.1) จุดเด่น:

(1) ความเร็วสูง: เวลาประมวลผลธุรกรรมเฉลี่ยเพียง 3 วินาที ทำให้เหมาะกับงานที่ต้องการการตอบสนองแบบเรียลไทม์

(2) ต้นทุนปานกลาง: ค่าธรรมเนียมอยู่ที่ $0.68 ต่อธุรกรรม ซึ่งเหมาะสมสำหรับการใช้งานในระบบที่มีปริมาณธุรกรรมสูง

1.2) ข้อจำกัด:

ความปลอดภัยระดับกลาง: ความปลอดภัยอยู่ในระดับ 7/10 ซึ่งยังอาจไม่เพียงพอสำหรับการจัดการข้อมูลสำคัญ

1.3) เหมาะสำหรับ: ระบบที่ต้องการความเร็วสูง เช่น ระบบการจองห้องประชุมออนไลน์หรือระบบธุรกรรมที่ต้องการการประมวลผลรวดเร็ว

2) เรอิเชน

10.1)จุดเด่น:

(1) ต้นทุนต่ำ: ค่าธรรมเนียมเฉลี่ยเพียง $0.0013 ต่อธุรกรรม ซึ่งเหมาะสำหรับการจัดเก็บข้อมูลขนาดใหญ่หรือข้อมูลที่ไม่สำคัญ

(2) ความเร็วสูงมาก: เวลาประมวลผลเพียง 1 วินาที ทำให้เป็นตัวเลือกที่เหมาะ สมสำหรับงานที่ต้องการการยืนยันทันที

10.2)ข้อจำกัด:

ความปลอดภัยต่ำ: มีระดับความปลอดภัยเพียง 2/10 เนื่องจากโหนดจำนวนน้อยและการกระจายศูนย์ต่ำ

10.3)เหมาะสำหรับ: งานที่เน้นต้นทุนต่ำและความเร็วสูง เช่น การจัดเก็บข้อมูลที่ไม่ได้เกี่ยวกับความปลอดภัย เช่น ข้อมูลที่ใช้ในการวิเคราะห์เชิงสถิติ

3) อีเธอเรียม:

3.1) จุดเด่น:

(1) ความปลอดภัยสูงที่สุด: ระดับความปลอดภัยอยู่ที่ 9/10 เนื่องจากโครงสร้างแบบกระจายศูนย์และจำนวนโหนดที่มากกว่า 500,000 โหนด

(2) ความน่าเชื่อถือ: ใช้กลไกฉันทามติแบบ PoS ที่ช่วยเพิ่มความปลอดภัยในการจัดการธุรกรรม

3.2) ข้อจำกัด:

(1) ต้นทุนสูง: ค่าธรรมเนียมเฉลี่ยอยู่ที่ $1.19 ต่อธุรกรรม ซึ่งเป็นผลมาจากการคำนวณค่าก๊าซและการใช้งานก๊าซ

(2) เวลาประมวลผลช้า: เวลาประมาณผลเฉลี่ย 15 วินาที ซึ่งอาจไม่เหมาะกับแอปพลิเคชันที่ต้องการความเร็ว

4) เอ็กซ์เชน:

4.1) จุดเด่น:

(1) ความสมดุลระหว่างความเร็วและความปลอดภัย: เวลาประมวลผลเฉลี่ย_4.4 วินาที และระดับความปลอดภัยอยู่ที่ 4/10

(2) ต้นทุนต่ำ: ค่าธรรมเนียมเฉลี่ยเพียง $0.13 ต่อธุรกรรม

4.2) ข้อจำกัด:

ความปลอดภัยปานกลาง: โหนดที่จำกัดทำให้ยังมีความเสี่ยงต่อการถูกโจมตีไซเบอร์

4.3) เหมาะสำหรับ: งานที่ต้องการสมดุลระหว่างความเร็วและความปลอดภัย เช่น การบริหารจัดการข้อมูลในองค์กรที่มีการแบ่งปันข้อมูลระหว่างหน่วยงาน

4.1.4 สรุปผลการทดลองการวิเคราะห์เชิงเปรียบเทียบแพลตฟอร์มบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมโดยใช้ชุดคำสั่งสัญญาอัจฉริยะ

การวิเคราะห์ประสิทธิภาพแพลตฟอร์มบล็อกเชนดังรูปที่ 4.1 แพลตฟอร์มบล็อกเชนแต่ละแพลตฟอร์มนำเสนอจุดแข็งและการแลกเปลี่ยนที่เป็นเอกลักษณ์ ทำให้เหมาะสำหรับกรณีการใช้งานเฉพาะ “ไบแนนซ์” นำเสนอตัวเลือกที่รอบด้าน โดยมีค่าธรรมเนียมการทำธุรกรรม $0.68 ระยะเวลาดำเนินการที่รวดเร็วเพียง 3 วินาที และมีระดับความปลอดภัยที่มั่นคงที่ 7/10 ทำให้เป็นตัวเลือกที่เหมาะสำหรับการใช้งานที่ต้องการประสิทธิภาพที่มีประสิทธิภาพโดยไม่ต้องเสียค่าใช้จ่ายมากเกินไป เช่น ระบบธุรกรรมระดับปานกลาง

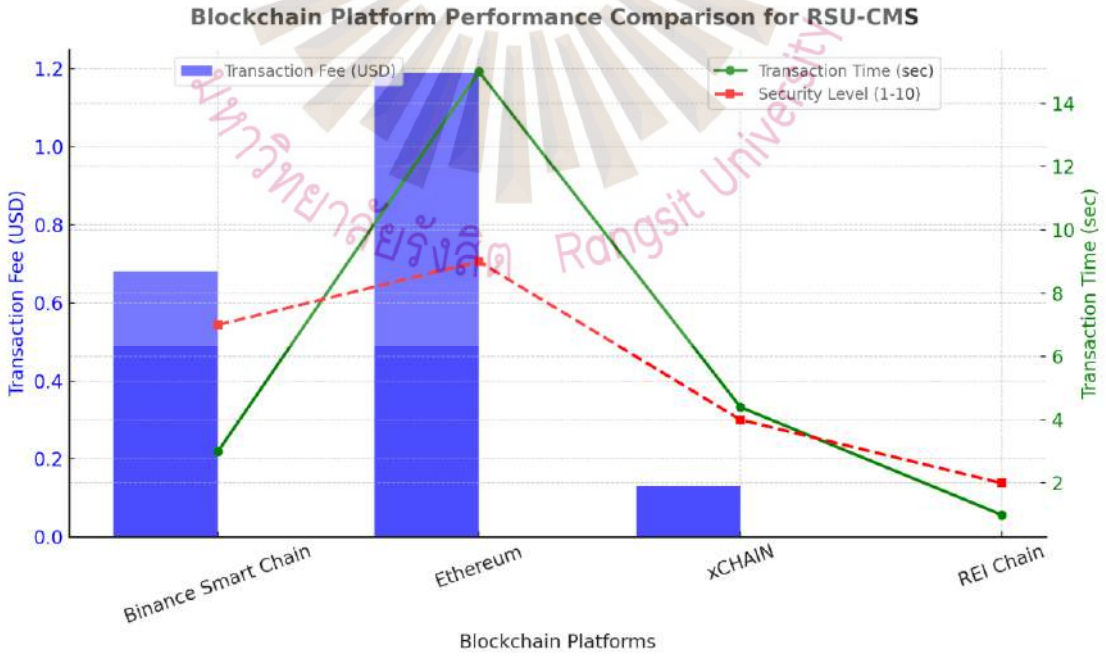
ในทางตรงกันข้าม “อีเธอเรียม” โดดเด่นในฐานะแพลตฟอร์มที่ปลอดภัยที่สุด โดยมีความต้านทานต่อการโจมตีสูงที่ระดับ 9/10 การรักษาความปลอดภัยที่ได้รับการปรับปรุงนี้ทำให้เหมาะอย่างยิ่งสำหรับแอปพลิเคชันที่มีความเสี่ยงสูง เช่น การจัดเก็บข้อมูลที่ละเอียดอ่อนหรือระบบระดับองค์กร อย่างไรก็ตามสิทธิประโยชน์เหล่านี้มาพร้อมกับค่าธรรมเนียมการทำธุรกรรมที่สูงขึ้น $1.19 และความเร็วในการประมวลผลที่ช้าลง 15 วินาที ทำให้อีเธอเรียมไม่เหมาะกับความต้องการด้านต้นทุนหรือความเร็วสูง

สำหรับผู้ที่กำลังมองหาโซลูชันที่คุ้มค่าและสมดุล “เอ็กซ์เชน” เป็นตัวเลือกระดับกลางที่ใช้งานได้ โดยมีค่าธรรมเนียมการทำธุรกรรมการทำธุรกรรมต่ำเพียง $0.13 ระยะเวลาดำเนินการที่เหมาะสมเพียง 4.4 วินาที และประสิทธิภาพโดยรวมอยู่ในระดับปานกลาง การรวมกันนี้ทำให้

เอ็กซ์เชนเป็นตัวเลือกที่เป็นประโยชน์สำหรับองค์กรที่จัดการข้อมูลด้วยงบประมาณ โดยไม่จำเป็นต้องใช้ความเร็วหรือความปลอดภัยระดับสูงสุด

ในอีกด้านหนึ่ง “เรอิเชน” เป็นแพลตฟอร์มที่เร็วและคุ้มค่าที่สุดโดยมีค่าธรรมเนียมการทำธุรกรรมเพียง $0.0013 และเวลาดำเนินการ 1 วินาที อย่างไรก็ตาม ระดับความปลอดภัยต่ำกว่าอย่างมากที่ 2/10 ซึ่งจำกัดความเหมาะสมกับระบบที่ไม่สำคัญ เรอิเชนเหมาะอย่างยิ่งสำหรับกรณีการใช้งานที่ความเร็วและต้นทุนต่ำเป็นสิ่งสำคัญยิ่ง เช่น แอปพลิเคชันไอโอที หรือธุรกรรมทางการเงินขนาดเล็ก แต่ไม่ใช้สำหรับสถานการณ์ที่ความปลอดภัยเป็นสิ่งสำคัญ

จากผลการทดลอง สรุปได้ว่า “เอ็กซ์เชน” สร้างสมดุลระหว่างต้นทุน ความเร็ว และความปลอดภัย ทำให้แพลตฟอร์มนี้เป็นตัวเลือกที่รอบด้านและอเนกประสงค์สำหรับกรณีการใช้งานที่หลากหลาย ในบริบทงานวิจัยนี้ เน้นยำถึงความสามารถในการปรับตัวของ “เอ็กซ์เชน” โดยไม่ต้องเจาะลึกถึงข้อมูลเฉพาะเกี่ยวกับแพลตฟอร์มทางเลือก โดยมุ่งเน้นที่ความเหมาะสมและจุดแข็งเพียงอย่างเดียว การเลือก “เอ็กซ์เชน” ถือเป็นแพลตฟอร์มบล็อกเชนที่เหมาะสมสำหรับระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS)



รูปที่ 4.1 แดชบอร์ดสรุปผลการทดลองที่ 1

4.2 ผลการทดลองการวิเคราะห์เชิงเปรียบเทียบประสิทธิภาพการใช้เทคนิคการแฝงข้อมูลร่วมกับฟังก์ชันแฮชบนบล็อกเชน

การทดลองนี้มีจุดมุ่งหมายสองประการ ประการแรกคือ เพื่อใช้ทั้งเทคนิคการแฝงข้อมูลร่วมกับแฮชฟังก์ชันและใช้เทคนิค k-Anonymity ร่วมกับโครงการนำร่อง “การจัดทำข้อมูลนิรนามของมหาวิทยาลัยรังสิต” (RSU-Data-Anonymization) สิ่งนี้เกี่ยวข้องกับการประยุกต์อัลกอริธึม โพรโทคอล หรือขั้นตอนเฉพาะใน ทางปฏิบัติที่ออกแบบมาเพื่อปกป้องความเป็นส่วนตัวของบุคคลที่ปรากฏในชุดข้อมูล และประการที่สองคือ ดำเนินการวิเคราะห์การเปรียบเทียบที่ครอบคลุมระหว่างเทคนิคเหล่านี้โดยพิจารณาจากปัจจัยต่าง ๆ เช่น การรักษาความเป็นส่วนตัว ประสิทธิภาพการคำนวณ และผลกระทบต่อประโยชน์ข้อมูล โดยมีเป้าหมายสูงสุดคือการสร้างแนวทางสำหรับอุตสาหกรรมข้อมูล โดยให้คำแนะนำว่าเมื่อใดควรใช้การแฝงข้อมูลหรือข้อมูลนิรนามตามกรณีการใช้งานเฉพาะ ข้อกำหนดทางกฎหมาย และข้อพิจารณาด้านความเป็นส่วนตัว แนวทางนี้อาจทำหน้าที่เป็นทรัพยากรอันมีค่าสำหรับองค์กรและบุคคลที่เกี่ยวข้องกับการจัดการข้อมูลที่ละเอียดอ่อน ช่วยให้พวกเขาตัดสินใจได้อย่างชาญฉลาดเพื่อสร้างสมดุลระหว่างความเป็นส่วนตัวและอรรถประโยชน์ข้อมูล

งานวิจัยนี้จะใช้ตัวชี้วัดประสิทธิภาพของการใช้เทคนิคการแฝงข้อมูลร่วมกับฟังก์ชันแฮชบนบล็อกเชนด้วย k-Anonymity คือ ความแม่นยำของอัลกอริทึมการเรียนรู้ของเครื่อง จำนวนการสูญเสียข้อมูล และอัตราความเสี่ยงที่จะถูกโจมตีเพื่อระบุตัวตนซ้ำอีกครั้ง โดยที่งานวิจัยนี้ต้องการที่จะศึกษาว่าบล็อกเชนมีส่วนช่วยเหลือในการป้องกันและรักษาความเป็นต้นฉบับของข้อมูลโดยการใช้เทคนิคการแฝงข้อมูลน้อยลงหรือไม่ เมื่อเทียบกับการทำการปกปิดข้อมูลเพียงอย่างเดียว และทำการประเมินประสิทธิภาพของแต่ละอัลกอริทึมการเรียนรู้ของเครื่อง สามารถสรุปรายละเอียดจากการทดลองได้ดังนี้

4.2.1 การประยุกต์ใช้เทคนิคการแฝงข้อมูล (Pseudonymization) ร่วมกับแฮชฟังก์ชัน (Hash Function) และเทคนิค k-Anonymity

4.2.1.1 การใช้การแฝงข้อมูล (Pseudonymization) ร่วมกับแฮชฟังก์ชัน (Hash Function)

1) วัตถุประสงค์: การแฝงข้อมูล และแฮชฟังก์ชันถูกออกแบบมาเพื่อลดความสามารถในการเชื่อมโยงข้อมูลที่สามารถระบุตัวตนได้โดยตรงกับข้อมูลอื่นๆ ในระบบ

2) ผลการทดลอง:

2.1) การใช้เทคนิคการแฝงข้อมูลร่วมกับแฮชฟังก์ชัน ช่วยเพิ่มความปลอดภัยของข้อมูลอย่างมาก โดยลดโอกาสในการเปิดเผยข้อมูลสำคัญหากข้อมูลถูกเข้าถึงโดยไม่ได้รับอนุญาต

2.2) ข้อมูลที่ผ่านกระบวนการแฮชจะไม่สามารถเชื่อมโยงกลับไปยังบุคคลเดิมได้โดยง่าย ซึ่งช่วยลดโอกาสการถูกละเมิดข้อมูลและลดความเสี่ยงจากการระบุตัวตนซ้ำได้

2.3) การวิเคราะห์ข้อมูลเชิงสถิติยังสามารถทำได้โดยใช้ค่าแฮช เช่น ในการคำนวณสถิติของกลุ่มข้อมูลเฉพาะ

2.4) ลดโอกาสที่ข้อมูลจะถูกใช้ในทางที่ไม่เหมาะสมแม้ข้อมูลจะถูกเปิดเผยบาง ส่วน

4.2.1.2 การใช้เทคนิค k-Anonymity:

1) วัตถุประสงค์: ลดความเสี่ยงของการระบุตัวตนซ้ำโดยการทำให้ข้อมูลที่เฉพาะเจาะจงกลายเป็นข้อมูลกลุ่มด้วยการทำให้เป็นลักษณะทั่วไป (Generalization) และลดความละเอียดของข้อมูลบางส่วน

2) ผลการทดลอง:

2.1) k-Anonymity มีผลกระทบต่อความละเอียดของข้อมูล แต่ยังรักษาความสมดุลระหว่างความปลอดภัยและการวิเคราะห์ข้อมูลได้ดี

2.2) แบบจำลองการเรียนรู้ เช่น Logistic Regression และ Random Forest ยังคงประสิทธิภาพสูงหลังการใช้ k-Anonymity โดยค่าความแม่นยำและคะแนนเอฟวันลดลงเพียงเล็กน้อย แต่แบบจำลองการเรียนรู้ของเครื่องที่ต้องการข้อมูลละเอียด เช่น Support Vector Classifier หรือ Gradient Boosting อาจได้รับผลกระทบบ้างในด้านความแม่นยำ

2.3) ความเสี่ยงของการระบุตัวตนซ้ำลดลง เนื่องจากข้อมูลถูกจัดอยู่ในกลุ่มที่มีสมาชิกอย่างน้อย k คน ทำให้การระบุบุคคลเฉพาะเจาะทำได้ยาก

4.2.1.3 การทำงานร่วมกันของการแฝงข้อมูลและ k-Anonymity:

1) การเสริมความปลอดภัย: การผสมผสานหลาย ๆ เทคนิค เช่น การแฝงข้อมูลและแฮชฟังก์ขันกับเทคนิค k-Anonymity ช่วยเพิ่มความปลอดภัยของข้อมูลอย่างมีนัยสำคัญ:

1.1) การแฝงข้อมูล ถูกใช้เพื่อลดการเชื่อมโยงข้อมูลที่สามารถระบุตัวตนได้โดยตรง

1.2) แฮชฟังก์ชัน ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากตัว

ระบุได้โดยตรง (Direct Identifiers)

1.3) k-Anonymity ปกปิดข้อมูลตัวระบุเสมือน (Quasi-Identifiers) เพื่อป้อง กันการเชื่อมโยงข้อมูลกลับไปยังบุคคลเดิม

2) ประโยชน์เชิงปฏิบัติ:

2.1) ลดความเสี่ยงในการละเมิดข้อมูล: การใช้ทั้งสามเทคนิคพร้อมกันช่วยลดความเสี่ยงในการเชื่อมโยงข้อมูลได้อย่างมีประสิทธิภาพ

2.2) รองรับการวิเคราะห์ข้อมูล: แม้ข้อมูลจะถูกทำให้คลุมเครือ แต่ยังสามารถนำไปใช้ในงานวิจัยเชิงสถิติและการวิเคราะห์เชิงลึกได้

2.3) ความยืดหยุ่นในการปรับใช้: สามารถนำไปใช้ในระบบหลากหลาย เช่น การบริจัดการความยินยอม การเก็บข้อมูลในงานวิจัย หรือการจัดการข้อมูลส่วนบุคคลในองค์กร

4.2.1.4 สรุปผล: การใช้การแฝงข้อมูลและแฮชฟังก์ชันร่วมกับ k-Anonymity ช่วยเสริมความปลอดภัยของข้อมูลส่วนบุคคลในทุกมิติ โดยลดความเสี่ยงของการระบุตัวตนซ้ำ และยังคงรักษาความสามารถในการใช้งานข้อมูลได้ในระดับที่เหมาะสม ซึ่งเหมาะสมอย่างยิ่งสำหรับโครงการนำร่อง “การจัดทำข้อมูลนิรนามของมหาวิทยาลัยรังสิต” (RSU-Data Anonymization) หรือระบบที่ต้องการปกปิดข้อมูลส่วนบุคคลในยุคปัจจุบัน

4.2.2 การเปรียบเทียบแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังใช้เทคนิค k-Anonymity

4.2.2.1 วัตถุประสงค์: การทดลองนี้มีเป้าหมายเพื่อวัดผลกระทบของเทคนิค k-Anonymity ต่อประสิทธิภาพของแบบจำลองการเรียนรู้ของเครื่อง (Machine Learning Models) ที่ใช้ในการวิเคราะห์ข้อมูล โดยประเมินผลกระทบของการลดรายละเอียดข้อมูลด้วยการทำข้อมูลให้เป็นลักษณะทั่วไป (Generalization) ต่อความแม่นยำและความสามารถในการคาดการณ์ของแบบจำลอง

ชุดข้อมูลที่ใช้มีคุณลักษณะสำคัญ เช่น รายได้และคุณลักษณะทางประชากรอื่น ๆ ซึ่งถูกนำไปประยุกต์ใช้กับแบบจำลองการเรียนรู้ของเครื่องต่าง ๆ ทั้ง 7 แบบจำลอง ได้แก่ Gradient Boosting (GB), Gaussian Naïve Bayes (GNB), Logistic Regression (LR), Random Forest (RF), Support Vector Classifier (SVC), Decision Tree (DT) และ K-Nearest Neighbor (KNN) การทดลองนี้วิเคราะห์ประสิทธิภาพในมิติต่าง ๆ เช่น ความแม่นยำ (Accuracy) ประสิทธิภาพในการจำแนกประเภทข้อมูล (ROC-AUC Curve) และการสูญเสียข้อมูล (Data Loss) ที่เกิดขึ้นหลังจากประยุกต์ใช้

k-Anonymity

4.2.2.2 ผลลัพธ์ที่ได้จากการทดลอง:

1) ก่อนการใช้ k-Anonymity

1.1) Gradient Boosting เป็นแบบจำลองที่มีประสิทธิภาพสูงสุด โดยมีค่าความแม่นยำอยู่ที่ 85.66% และค่า ROC-AUC Curve ที่ 0.95 ซึ่งแสดงถึงความสามารถในการจำแนกประเภทข้อมูลได้ดีเยี่ยม

1.2) Gaussian Naïve Bayes แม้ว่าจะมีการประมวลผลที่เร็ว แต่มีค่าความแม่นยำต่ำกว่าแบบจำลองอื่นที่ 78 - 48%

1.3) Support Vector Classifier มีค่าความแม่นยำรองลงมา แต่ ROC-AUC Curve ไม่สามารถเทียบเท่ากับ Gradient Boosting

1.4) Random Forest มีประสิทธิภาพที่ค่อนข้างสมดุล แต่ยังตามหลัง Gradient Boosting

2) หลังใช้ k-Anonymity

2.1) Gradient Boosting ยังคงเป็นแบบจำลองที่มีประสิทธิภาพสูงสุด โดยมีค่าความแม่นยำลดลงเล็กน้อยเหลือ 82.18% แต่ยังคงรักษาความสามารถในการจำแนกข้อมูล (ROC-AUC) ได้ดี

2.2) Gaussian Naïve Bayes ได้รับผลกระทบมากที่สุด ค่าความแม่นยำลดลงเหลือ 78 - 48% และ ROC-AUC ลดลง

2.3) Support Vector Classifier มีประสิทธิภาพลดลงชัดเจน โดยค่าความแม่นยำลดลงมาจาก 74 – 48% เหลือเพียง 74.57%

2.4) Random Forest แม้ว่าความแม่นยำจะลดลงเล็กน้อย แต่ยังคงประสิทธิภาพที่เหมาะสมสำหรับการใช้งาน

3) การเปรียบเทียบแบบจำลอง

3.1) Gradient Boosting ยังคงครองตำแหน่งแบบจำลองที่ดีที่สุด เนื่องจากความ สามารถในการรักษาประสิทธิภาพได้ดีแม้หลังการใช้ k-Anonymity

3.2) Gaussian Naïve Bayes และ Support Vector Classifier ได้รับผลกระทบมากที่สุดในด้านความแม่นยำและ ROC-AUC

3.3) Random Forest ยังคงเหมาะสมสำหรับการใช้งานที่ต้องการสมดุลระหว่างความแม่นยำและความเร็ว

มหาวิทยาลัยรังสิต Rangsit University

4.2.2.3 สรุปผล: การทดลองนี้ช่วยยืนยันว่า Gradient Boosting เป็นตัวเลือกที่เหมาะสมที่สุดสำหรับการใช้งานในระบบที่เน้นการปกป้องข้อมูลส่วนบุคคลด้วยเทคนิค k-Anonymity โดยยังคงรักษาความแม่นยำและประสิทธิภาพได้ดีในระดับสูงสุด

1) Gradient Boosting ยังคงเป็นแบบจำลองที่มีประสิทธิภาพสูงสุดทั้งก่อนและหลังการใช้ k-Anonymity เนื่องจากสามารถรักษาความแม่นยำและคุณภาพของข้อมูล

2) Gaussian Naïve Bayes และ Support Vector Classifier เป็นแบบจำลองที่ได้รับผลกระทบมากที่สุด โดยเฉพาะในแง่ของค่าความแม่นยำหลังจากใช้ k-Anonymity

3) การปรับใช้ k-Anonymity แม้จะลดประสิทธิภาพในบางแบบจำลอง แต่ช่วยเพิ่มความปลอดภัยและความเป็นส่วนตัวของข้อมูล ซึ่งเป็นเป้าหมายสำคัญของการวิจัยนี้

4.2.3 การวัดประสิทธิภาพการสูญเสียข้อมูล:

การวิเคราะห์ผลกระทบจากการประยุกต์ใช้ k-Anonymity ต่อคุณภาพข้อมูลในแง่มุมต่าง ๆ เป็นสิ่งสำคัญเพื่อทำความเข้าใจถึงความสมดุลระหว่างการปกป้องข้อมูลส่วนบุคคล (Privacy Preservation) และความแม่นยำในการประมวลผลข้อมูล (Data Utility) ในการวิจัยนี้ได้มีการวัดค่าการสูญเสียข้อมูลและประสิทธิภาพการจำแนกข้อมูลผ่าน ROC-AUC Curve ดังนี้

4.2.3.1 การวิเคราะห์การสูญเสียข้อมูล (Data Loss):

การสูญเสียข้อมูล หมายถึง การสูญเสียคุณภาพข้อมูลหรือการลดความละเอียดของข้อมูลที่เกิดขึ้นจากกระบวนทำให้ข้อมูลไม่สามารถระบุตัวตนได้ ซึ่งมีผลกระทบต่อความ สามารถของแบบจำลองในการเรียนรู้และการจำแนกข้อมูล โดยผลการวิเคราะห์พบว่า

1) Gradient Boosting

1.1) ค่าการสูญเสียข้อมูลต่ำสุด: มีค่าการสูญเสียข้อมูลที่ 0.01 ซึ่งต่ำที่สุดในบรรดาแบบจำลองทั้งหมด แสดงถึงความสามารถในการปรับตัวต่อข้อมูลที่ถูกปรับเปลี่ยน

1.2) สาเหตุของประสิทธิภาพที่ดี: ใช้กระบวนการเรียนรู้แบบวนซ้ำ (iterative) โดยการเรียนรู้จากข้อผิดพลาดในรอบก่อนหน้า ซึ่งช่วยให้แบบจำลองสามารถรักษาคุณภาพการจำแนกข้อมูลได้แม้ข้อมูลจะถูกทำให้ไม่สมบูรณ์

2) Gaussian Naïve Bayes และ Support Vector Classifier

2.1) ค่าการสูญเสียข้อมูลสูงสุด: ทั้งสองแบบจำลองมีค่าการสูญเสียข้อมูลที่ 0.08 ซึ่งเป็นผลกระทบที่มากที่สุดในบรรดาแบบจำลองทั้งหมด

2.2) ข้อจำกัด: Gaussian Naïve Bayes อาศัยสมมติฐานว่าแต่ละคุณลักษณะเป็นอิสระจากกัน (Independence Assumption) ซึ่งไม่สามารถจัดการกับข้อมูลที่ถูกลดความซับซ้อนได้ดี

2.3) Support Vector Classifier มีความไวต่อข้อมูลที่ถูกเปลี่ยนแปลงโครงสร้าง ทำให้การจำแนกข้อมูลมีความผิดพลาดเพิ่มขึ้น

3) Logistic Regression และ Random Forest

3.1) มีค่าการสูญเสียข้อมูลในระดับปานกลาง โดย Logistic Regression สามารถคงประสิทธิภาพได้ดีในงานที่มีข้อมูลลดความละเอียด

3.2) Random Forest มีความทนทานต่อข้อมูลที่ถูกปรับเปลี่ยน เนื่องจากการรวมผลจากหลายต้นไม้การตัดสินใจช่วยลดความผิดพลาดจากข้อมูลที่สูญเสียคุณภาพ

4.2.3.2 การวิเคราะห์ ROC-AUC Curve:

ROC-AUC Curve เป็นตัวชี้วัดที่แสดงความสามารถของแบบจำลองในการแยกประเภทข้อมูล โดยพิจารณาความสมดุลระหว่าง True Positive และ Fales Positive ซึ่งผลการวิเคราะห์พบว่า

1) Gradient Boosting

1.1) ค่าประสิทธิภาพสูงสุด: มีค่า ROC-AUC สูงสุดที่ 0.95 แสดงถึงความสามารถในการจำแนกข้อมูลได้อย่างแม่นยำ แม้ข้อมูลจะผ่านการปรับเปลี่ยน

1.2) การปรับตัวที่ดีต่อข้อมูล: ใช้การปรับน้ำหนักข้อมูในแต่ละรอบการเรียนรู้ ซึ่งช่วยเพิ่มประสิทธิภาพในการจำแนกแม้ข้อมูลจะมีการเปลี่ยนแปลง

2) Logistic Regression และ Random Forest

มีค่า ROC-AUC ใกล้เคียงกันและอยู่ระดับสูง โดย Logistic Regression เหมาะกับข้อมูลที่มีการลดรายละเอียดน้อย และ Random Forest เหมาะสำหรับข้อมูลที่มีโครงสร้างที่หลากหลาย

3) Gaussian Naïve Bayes และ Support Vector Classifier

ค่าประสิทธิภาพลดลง: ROC-AUC ของ Gaussian Naïve Bayes และ Support Vector Classifier ลดลงชัดเจนหลังการปรับเปลี่ยนข้อมูล แสดงถึงความไวต่อการสูญเสียรายละเอียดของข้อมูล

4.2.3.3 สรุปผลการวิเคราะห์:

1) Gradient Boosting เป็นแบบจำลองที่มีประสิทธิภาพสูงสุดทั้งในแง่ของการสูญเสียข้อมูลต่ำและค่า ROC-AUC Curve สูง แสดงถึงความสามารถในการรักษาคุณภาพข้อมูลและประสิทธิภาพการจำแนกข้อมูล จึงยืนยันได้ว่าเป็นแบบจำลองที่เหมาะสมที่สุดสำหรับการใช้งานในระบบที่ต้องการความปลอดภัยของข้อมูลผ่านการใช้ k-Anonymity โดยยังคงรักษาความสามารถในการประมวลผลและจำแนกข้อมูลได้อย่างแม่นยำ

2) Gaussian Naïve Bayes และ Support Vector Classifier ได้รับผลกระทบมากที่สุดจากการประยุกต์ใช้ k-Anonymity โดยมีค่าการสูญเสียข้อมูลสูงและประสิทธิภาพลดลงใน ROC-AUC Curve

3) Logistic Regression และ Random Forest แสดงความสามารถที่สมดุลในทุกสถานการณ์ โดยมีประสิทธิภาพในระดับสูงทั้งก่อนและหลังใช้ k-Anonymity

4.2.4 การประเมินความเสี่ยงของการระบุตัวตนซ้ำ (Re-identification Risk)

การทดลองประเมินความเสี่ยงจากการระบุตัวตนซ้ำในระบบ RSU-Data-Anonymity โดยใช้เทคนิค k-Anonymity แสดงให้เห็นถึงประสิทธิภาพในการลดโอกาสการเชื่อมโยงข้อมูลกลับไปยังบุคคลได้อย่างชัดเจน แบบจำลองการเรียนรู้ของเครื่องส่วนใหญ่ เช่น Logistic Regression, Random Forest, Decision Tree และ Gaussian Naïve Bayes ยังคงรักษาความแม่นยำได้ดีหลังการลดรายละเอียดของข้อมูล โดยมีค่าความแม่นยำและ Macro F1-Score ลดลงเพียงเล็กน้อย (น้อยกว่า 5%) ทำให้เหมาะสมกับการใช้งานในระบบที่ต้องการความปลอดภัยสูงโดยไม่สูญเสียประสิทธิภาพ

ในทางกลับกัน แบบจำลองที่ซับซ้อนกว่า เช่น Support Vector Classifier และ Gradient Boosting มีความไวต่อข้อมูลที่ลดความละเอียด ส่งผลให้ Macro F1-Score ลดลงมากกว่า 10% ซึ่งบ่งชี้ว่าความแม่นยำของแบบจำลองเหล่านี้ต้องพึ่งพาข้อมูลที่มีความละเอียดสูง อย่างไรก็ตาม การประยุกต์ใช้ k-Anonymity สามารถลดความเสี่ยงในการระบุตัวตนซ้ำได้ถึง 30% ช่วยเพิ่มความปลอดภัยให้กับข้อมูลส่วนบุคคลอย่างมีนัยสำคัญ

สรุปได้ว่า k-Anonymity เป็นเทคนิคที่มีประสิทธิภาพในการรักษาสมดุลระหว่างความปลอดภัยของข้อมูลและความสามารถในการวิเคราะห์ ทำให้เหมาะสมสำหรับการใช้งานในระบบที่ต้องการลดความเสี่ยงจากการระบุตัวตนซ้ำ

มหาวิทยาลัยรังสิต Rangsit University

4.2.5 สรุปผลโดยรวม

จากรูปที่ 4.2 แสดงแผนภูมิเปรียบเทียบประสิทธิภาพของแบบจำลองการเรียนรู้ของเครื่องก่อนและหลังการใช้ k-Anonymity ในแง่ของความแม่นยำและการสูญเสียข้อมูลสำหรับแบบจำลองต่าง ๆ รวมถึง Logistic Regression, Support Vector Classifier, Random Forest, Decision Tree, K-Nearest Neighbor, Gaussian Naïve Bayes และ Gradient Boosting สามารถแสดงการวิเคราะห์โดยละเอียดดังนี้

4.2.5.1 ข้อสังเกตสำคัญ:

1) ผลกระทบของ k-Anonymity ต่อประสิทธิภาพของแบบจำลอง

1.1) แบบจำลองทั้งหมดมีความแม่นยำลดลงเล็กน้อยหลังจากใช้ k-Anonymity

1.2) Gradient Boosting มีความยืดหยุ่นสูงและสามารถทำงานได้ดี แม้ข้อมูลจะถูกลดรายละเอียดหลังจากใช้ k-Anonymity

1.3) แบบจำลองที่เรียบง่าย เช่น Logistic Regression, Random Forest และ Decision Tree มีความสามารถในการรองรับข้อมูลที่ลดรายละเอียดได้ดี โดยมีการสูญเสียข้อมูลต่ำกว่า 5%

1.4) แบบจำลองที่ซับซ้อน เช่น Support Vector Classifier มีประสิทธิภาพลดลงอย่างชัดเจนเมื่อข้อมูลถูกปรับเปลี่ยนด้วย k-Anonymity

2) การสูญเสียข้อมูล

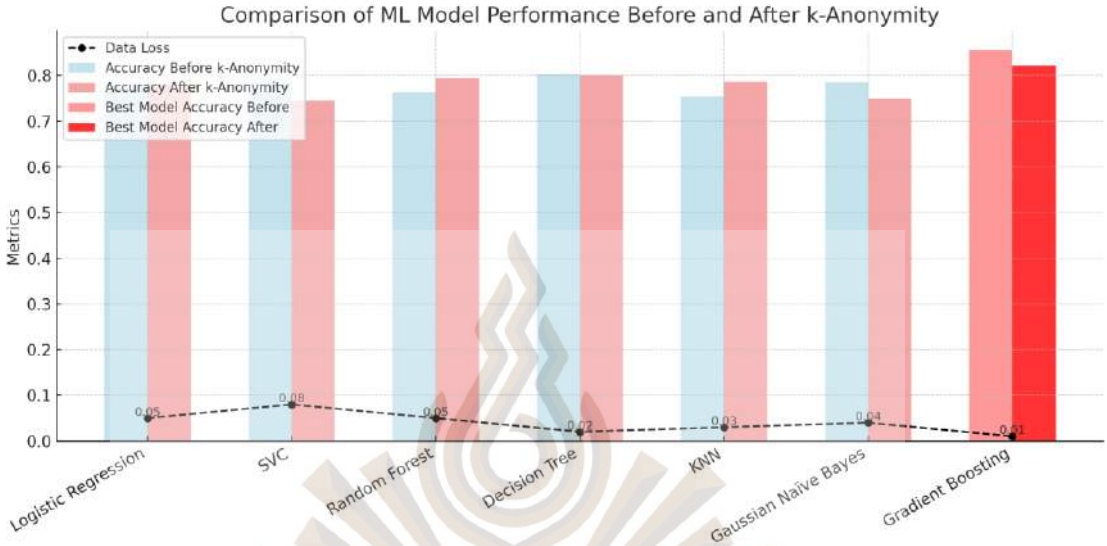
2.1) แบบจำลองที่มีการสูญเสียต่ำที่สุด (เช่น Gradient Boosting) แสดงการสูญเสียน้อยที่สุด (0.01) แสดงถึงความสามารถที่ดีที่สุดในการรักษาความแม่นยำ แม้ข้อมูลจะถูกลดทอนรายละเอียด

2.2) โดยรวมแล้ว การสูญเสียข้อมูลยังคงมีเพียงเล็กน้อยในแบบจำลองต่าง ๆ ซึ่งบ่งชี้ว่ามีการใช้ k-Anonymity อย่างมีประสิทธิภาพโดยไม่กระทบต่อโครงสร้างข้อมูลอย่างมีนัยสำคัญ

3) ความแม่นยำของแบบจำลองที่ดีที่สุด

3.1) Gradient Boosting เป็นแบบจำลองที่ดีที่สุด ทำงานได้ดีที่สุดอย่างสม่ำเสมอทั้งก่อนและหลังการใช้ k-Anonymity

3.2) แบบจำลองอื่น ๆ แสดงความแม่นยำที่ลดลงอย่างเห็นได้ชัด ซึ่งบ่งชี้ว่าแบบ จำลองเหล่านี้มีความอ่อนไหวต่อการแปลง k-Anonymityมากกว่า



รูปที่ 4.2 แดชบอร์ดสรุปผลการทดลองที่ 2

4.2.5.2 บทสรุป: การวิเคราะห์เน้นย้ำว่าในขณะที่ k-Anonymity ทำให้เกิดการแลกเปลี่ยนระหว่างความแม่นยำและความเป็นส่วนตัว แต่ผลกระทบนั้นน้อยมากสำหรับแบบจำลองที่แข็งแกร่ง เช่น Gradient Boosting แบบจำลองนี้แสดงให้เห็นถึงประสิทธิภาพที่เหนือกว่าในแง่ของการรักษาความแม่นยำและลดการสูญเสียข้อมูล ทำให้เป็นตัวเลือกที่ต้องการสำหรับแอปพลิเคชันที่ต้องการทั้งประสิทธิภาพความเป็นส่วนตัวและการคาดการณ์ แบบจำลองอื่น ๆ เช่น Random Forest และ Support Vector Classifier อาจต้องมีการปรับแต่งเพิ่มเพิ่มจัดการกับการเปลี่ยนแปลงที่เกิดจาก k-Anonymity ได้อย่างมีประสิทธิภาพ

บทที่ 5

สรุปผลการวิจัย การอภิปราย และข้อเสนอแนะ

งานศึกษาฉบับนี้ใช้ระเบียบวิจัยเชิงปริมาณ (Quantitative Research) ผ่านการวิจัยเชิงทดลองที่แท้จริง (True Experiment) เป็นการวิจัยที่มีการเก็บข้อมูลและมีการวิเคราะห์ข้อมูลโดยเชิงเปรียบเทียบ (Comparative Analysis) งานวิจัยจะกล่าวถึงประเด็นสำคัญสองประการ ได้แก่ การใช้เทคโนโลยีบล็อกเชนในการจัดการความยินยอมที่บูรณาการร่วมกับสัญญาอัจฉริยะ และการใช้เทคนิคการแฝงข้อมูลเพื่อรักษาความเป็นต้นฉบับของข้อมูล เทคโนโลยีบล็อกเชนสามารถเป็นเครื่องมือที่มีประสิทธิภาพในการปรับปรุงการปกป้องข้อมูลและความเป็นส่วนตัวได้อย่างไร ด้วยการใช้ประโยชน์จากคุณสมบัติเด่นของบล็อกเชนเพื่อการจัดการความยินยอมและการใช้การแฝงข้อมูล ทำให้สามารถปรับปรุงความปลอดภัยและการควบคุมข้อมูลส่วนบุคคลได้อย่างมีนัยสำคัญ ทำให้เป็นโซลูชันที่มีแนวโน้มที่เป็นไปได้สำหรับความท้าทายที่ต้องเผชิญในการจัดการความยินยอมและการปกป้องความเป็นส่วนตัวของข้อมูล

5.1 สรุปผลการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนาระบบบริหารจัดการความยินยอมและการปกป้องข้อมูลส่วนบุคคลผ่านการประยุกต์ใช้เทคโนโลยีบล็อกเชนและเทคนิค k-Anonymity โดยมุ่งเน้นการเพิ่มความโปร่งใส ความปลอดภัย และลดความเสี่ยงของข้อมูลส่วนบุคคล ทั้งนี้ยังมุ่งเน้นการออกแบบให้สอดคล้องกับข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (จีดีพีอาร์) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พีดีพีเอ) ของประเทศไทย ผลการวิจัยชี้ให้เห็นถึงความสำเร็จใน 2 ส่วนสำคัญดังนี้

5.1.1 การใช้สัญญาอัจฉริยะ (Smart Contracts) บนบล็อกเชนสำหรับระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS)

ระบบบริหารจัดการความยินยอมของมหาวิทยาลัยรังสิต (RSU-CMS) ได้รับการออกแบบโดยใช้สัญญาอัจฉริยะ (Smart Contracts) บนบล็อกเชน เพื่อบริหารจัดการความยินยอมของผู้ใช้

ในลักษณะที่โปร่งใสและตรวจสอบได้ โดยผลการทดลองแสดงถึงประโยชน์ที่ชัดเจนในหลายด้าน ได้แก่

5.1.1.1 เพิ่มความโปร่งใสและความปลอดภัย:

1) การใช้บล็อกเชนในระบบ RSU-CMS ทำให้การจัดเก็บข้อมูลบันทึกความยินยอมของผู้ใช้มีความโปร่งใสและไม่สามารถเปลี่ยนแปลงหรือแก้ไขได้ (Immutable)

2) สัญญาอัจฉริยะช่วยให้งานบริหารจัดการความยินยอมดำเนินการได้อย่างอัตโนมัติและตรวจสอบได้ ซึ่งช่วยลดโอกาสการละเมิดข้อมูลส่วนบุคคลและเพิ่มความมั่นใจให้แก่ผู้ใช้งาน

5.1.1.2 ลดข้อผิดพลาดของมนุษย์: กระบวนการจัดการความยินยอมที่ดำเนินการโดยสัญญาอัจฉริยะ ช่วยลดขั้นตอนที่ต้องพึ่งพาการปฏิบัติงานด้วยมนุษย์ เช่น การบันทึกข้อมูลผิดพลาดหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กระบวนการอัตโนมัติช่วยให้การจัดการเป็นไปอย่างราบรื่น

5.1.1.3 การเปรียบเทียบประสิทธิภาพแพลตฟอร์มบล็อกเชน: การทดลองในแพลตฟอร์มบล็อกเชน เช่น ไบแนนซ์ (Binance Smart Chain) อีเธอเรียม (Ethereum) เอ็กซ์เชน (xCHAIN) และ เรอิเชน (REI Chain) แสดงให้เห็นว่าแต่ละแพลตฟอร์มมีจุดเด่นเฉพาะตัว เช่น

1) ไบแนนซ์ เหมาะกับงานที่เน้นความเร็วในการประมวลผลธุรกรรม

2) อีเธอเรียม มีความปลอดภัยสูงสุด เหมาะกับงานที่ต้องการความน่าเชื่อถือสูง

3) เรอิเชน มีต้นทุนการใช้งานต่ำ เหมาะกับงานที่มีข้อจำกัดด้านทรัพยากรและไม่ต้องการความซับซ้อน

4) เอ็กซ์เชน ให้สมดุลระหว่างความเร็วและความปลอดภัย

ดังนั้นการเลือกแพลตฟอร์มที่เหมาะสม จะช่วยเพิ่มประสิทธิภาพของระบบตามความต้องการของงานที่แตกต่างกัน

5.1.2 การวิเคราะห์ผลกระทบของการใช้ k-Anonymity ในโครงการนำร่องที่ชื่อว่า RSU-Data-Anonymization

การประยุกต์ใช้เทคนิค k-Anonymity เพื่อปกป้องข้อมูลส่วนบุคคลในระบบ RSU-Data-Anonymization แสดงให้เห็นถึงศักยภาพในการลดความเสี่ยงของการระบุตัวตนซ้ำ (Re-identification Attack) โดย

5.1.2.1 ลดความเสี่ยงจากการระบุตัวตนซ้ำ: เทคนิค k-Anonymity ช่วยลดความเสี่ยงในการเชื่อมโยงข้อมูลกลับไปยังบุคคลเฉพาะเจาะจงได้อย่างมีนัยสำคัญ โดยจัดกลุ่มข้อมูลให้มีผู้ใช้ที่คล้ายคลึงกันอย่างน้อย k คน ผลการทดลองแสดงว่า k-Anonymity ลดความเสี่ยงของการระบุตัวตนซ้ำได้มากกว่า 30% ซึ่งเหมาะสำหรับการนำไปใช้ในระบบที่ต้องการรักษาความปลอดภัยของข้อมูลในระดับสูง

5.1.2.2 ผลกระทบต่อประสิทธิภาพแบบจำลองการเรียนรู้ของเครื่อง:

1) แบบจำลองที่มีโครงสร้างเรียบง่าย เช่น Logistic Regression และ Random Forest ได้รับผลกระทบจากการใช้ k-Anonymity ในระดับต่ำ โดยมีความแม่นยำลดลงไม่เกิน 5% ซึ่งยังคงใช้งานได้อย่างมีประสิทธิภาพ

2) Gradient Boosting เป็นแบบจำลองที่มีประสิทธิภาพสูงสุดทั้งก่อนและหลังใช้ k-Anonymity โดยมีความแม่นยำและค่าความไว้วางใจสูงที่สุด

3) แบบจำลองที่ซับซ้อน เช่น Support Vector Classifier และ Gaussian Naïve Bayes ได้รับผลกระทบมากกว่า โดยมีคะแนนเอฟวันลดลงมากกว่า 10% เนื่องจากแบบจำลองเหล่านี้ต้องการข้อมูลที่มีความละเอียดสูงเพื่อสร้างผลลัพธ์ที่แม่นยำ

5.1.3 ข้อสรุปโดยรวม: งานวิจัยนี้แสดงให้เห็นว่า

การผสานเทคโนโลยีบล็อกเชนและเทคนิค k-Anonymity ในงานวิจัยนี้ไม่ได้แสดงเพียงแค่ความสามารถในการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยและโปร่งใส แต่ยังเป็นก้าวสำคัญในการสร้างมาตรฐานใหม่ด้านความเป็นส่วนตัวและการรักษาความปลอดภัยของข้อมูล ระบบ RSU-CMS และระบบ RSU-Data Anonymization ที่พัฒนาขึ้นเป็นตัวอย่างที่ชัดเจนในการแสดงให้เห็นว่าการใช้เทคโนโลยีทั้งสองสามารถช่วยเพิ่มความมั่นใจให้กับผู้ใช้งาน และเสริมความน่าเชื่อถือของระบบได้อย่างมีประสิทธิภาพ

นอกจากนี้ ระบบยังช่วยให้การปฏิบัติตามข้อกำหนดทางกฎหมาย เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (จีดีพีอาร์) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พีดีพีเอ) เป็นไปอย่างครบถ้วนและราบรื่น การนำไปประยุกต์ในบริบทอื่น ๆ เช่น การจัดการข้อมูลทางการแพทย์ สามารถช่วยปกป้องความลับของผู้ป่วย ขณะเดียวกันยังช่วยสนับสนุนการวิจัยที่ต้องพึ่งพาข้อมูลในระดับกว้าง หรือการจัดการข้อมูลทางการศึกษา ซึ่งอาจช่วยพัฒนานโยบาย

หรือกระบวนการเรียนการสอนอย่างมีประสิทธิภาพโดยไม่ละเมิดความเป็นส่วนตัวของนักเรียนหรือบุคลากร

ความสำคัญของงานวิจัยนี้จึงอยู่ที่การพิสูจน์ว่าเทคโนโลยีบล็อกเชนและ k-Anonymity ไม่เพียงตอบสนองความต้องการด้านความปลอดภัย แต่ยังเปิดโอกาสให้มีการพัฒนาระบบที่โปร่งใส เชื่อถือได้ และพร้อมต่อการขยายไปยังอุตสาหกรรมต่าง ๆ ที่ต้องการจัดการข้อมูลอย่างรอบคอบและปลอดภัยในยุคดิจิทัล

5.2 การอภิปรายและข้อจำกัดในการวิจัย

การวิจัยนี้แสดงให้เห็นถึงศักยภาพของการใช้เทคโนโลยีบล็อกเชนและเทคนิค k-Anonymity ในการเพิ่มความปลอดภัยและความโปร่งใสของระบบบริหารจัดการความยินยอมและการปกป้องข้อมูลส่วนบุคคล อย่างไรก็ตาม ยังมีข้อจำกัดที่สำคัญ เช่น ความสอดคล้องกับจีดีพีอาร์และพีดีพีเอ ซึ่งการจัดการสิทธิการลบข้อมูลและการแก้ไขข้อมูลในระบบที่ใช้บล็อกเชนยังคงเผชิญความท้าทาย เนื่องจากลักษณะที่ไม่สามารถเปลี่ยนแปลงได้ของบล็อกเชน นอกจากนี้ข้อจำกัดด้านการปรับขยายทำให้ระบบอาจรองรับธุรกรรมจำนวนมากได้ยากในช่วงที่มีการใช้งานสูง และความยืดหยุ่นในการปรับเปลี่ยนสูง เช่น การปรับค่า k ใน k-Anonymity เพื่อรองรับข้อมูลหลากหลายรูปแบบ ยังคงเป็นประเด็นที่ต้องพัฒนาเพิ่มเติม การพึ่งพาการควบคุมแบบรวมศูนย์ในบางส่วนยังลดทอนความเป็นการกระจายศูนย์ของระบบ ซึ่งการแก้ไขข้อจำกัดเหล่านี้จะเป็นแนวทางสำคัญสำหรับการพัฒนาระบบในอนาคตให้มีประสิทธิภาพและตอบสนองต่อความต้องการได้ดียิ่งขึ้น มีรายละเอียดได้ดังนี้

5.2.1 ข้อจำกัดและการตอบสนองต่อจีดีพีอาร์และพีดีพีเอ

การพัฒนาระบบ RSU-CMS และระบบ RSU-Data-Anonymization โดยการประยุกต์ใช้เทคโนโลยีบล็อกเชนและเทคนิค k-Anonymity มีวัตถุประสงค์เพื่อเพิ่มความปลอดภัยข้องข้อมูลส่วนบุคคลและสอดข้องกับข้อกำหนดของ จีดีพีอาร์และพีดีพีเอ อย่างไรก็ตาม ลักษณะเฉพาะของบล็อกเชน เช่น ความเป็นการไม่เปลี่ยนรูป (ไม่สามารถแก้ไข เปลี่ยนแปลง หรือลบข้อมูลได้) และการกระจายศูนย์ ส่งผลให้ยังคงมีข้อจำกัดในบางกรณี ซึ่งอธิบายได้ดังนี้

5.2.1.1 Article 17 (จีดีพีอาร์): Right to Erasure (or Right to be Forgotten)

1) ข้อท้าทาย: บล็อกเชนที่มีลักษณะไม่เปลี่ยนรูป ทำให้ข้อมูลที่ถูกบันทึกไม่สามารถลบ แก้ไข หรือเปลี่ยนแปลงได้โดยตรง ซึ่งอาจขัดแย้งกับสิทธิการลบข้อมูลตามจีดีพีอาร์ที่อนุญาตให้เจ้าของข้อมูลร้องขอลบข้อมูลส่วนบุคคลของคนในกรณีที่ไม่จำเป็นอีกต่อไป หรือไม่ได้รับการยินยอม

2) แนวทางการแก้ไข: การใช้เทคนิคค่าแฮช (Hash Value) เพื่อเก็บข้อมูลในรูปแบบรหัสที่สามารถอ้างอิงได้ในบล็อกเชน และจัดเก็บข้อมูลต้นฉบับในพื้นที่เก็บข้อมูลนอกเครือข่าย (Off-chain Storage) ซึ่งสามารถลบหรือแก้ไขได้ จะช่วยลดความขัดแย้งนี้ โดยยังคงรักษาความโปร่งใสและความน่าเชื่อถือของระบบบล็อกเชน

5.2.1.2 Article 16 (จีดีพีอาร์): Right to Rectification

1) ข้อท้าทาย: การแก้ไขข้อมูลที่ถูกบันทึกบนบล็อกเชนไม่สามารถดำเนินการโดยตรงกับข้อมูลเดิมได้ แต่จำเป็นต้องเพิ่มบล็อกใหม่ที่มีข้อมูลที่ถูกต้องแทนที่ ซึ่งอาจเพิ่มความซับซ้อนของต้นทุนในกระบวนการจัดการข้อมูล

2) แนวทางแก้ไข: การพัฒนาระบบกำหนดเวอร์ชัน (Versioning System) หรือเมทาดาตา (Metadata) ที่แสดงประวัติการแก้ไขข้อมูล สามารถช่วยให้การจัดการข้อมูลโปร่งใสและตรวจสอบได้ง่ายขึ้น โดยไม่กระทบความน่าเชื่อถือของบล็อกเชน

5.2.1.3 Section 37 (พีดีพีเอ): การป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การปฏิบัติตามข้อกำหนด: ระบบ RSU-CMS ใช้สัญญาอัจฉริยะเพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลตามบทบาทหรือความยินยอมของผู้ใช้งาน ข้อมูลที่ถูกจัดเก็บในบล็อกเชนได้รับการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ช่วยลดความเสี่ยงในการละเมิดข้อมูล (Data Breach) และทำให้ระบบสามารถตรวจสอบย้อนหลังได้อย่างชัดเจน

โดยสรุป ระบบ RSU-CMS และ RSU-Data-Anonymization แสดงให้เห็นถึงศักยภาพของการใช้เทคโนโลยีบล็อกเชนและสัญญาอัจฉริยะในการเพิ่มความปลอดภัยและความโปร่งใสของข้อมูลส่วนบุคคล โดยสามารถตอบสนองข้อกำหนดส่วนใหญ่ของจีดีพีอาร์และพีดีพีเอได้ อย่างไรก็ตาม ข้อจำกัดด้านความสามารถในการลบและแก้ไขข้อมูลตามสิทธิของผู้ใช้งาน ยังคงเป็นความท้าทายที่ต้องการแนวทางเพิ่มเติม เช่น การใช้พื้นที่เก็บข้อมูลนอกเครือข่ายและการบันทึกเมทาดาตาเพื่อเสริมสร้างความยืดหยุ่นในการจัดการข้อมูล ขณะเดียวกันยังคงรักษาความโปร่งใสและความน่าเชื่อถือของระบบบล็อกเชนไว้อย่างครบถ้วน

5.2.2 ความสามารถในการปรับขนาดและความยืดหยุ่น

ระบบ RSU-CMS และ RSU-Data-Anonymization ที่ใช้เทคโนโลยีบล็อกเชนและเทคนิค k-Anonymity ยังคงเผชิญกับความท้าทายสำคัญ 2 ด้าน ได้แก่ ความสามารถในการรองรับธุรกรรมจำนวนมากและความยืดหยุ่นในการปรับเปลี่ยนข้อมูล ซึ่งส่งผลต่อประสิทธิภาพ ความรวดเร็ว และต้นทุนในการดำเนินงาน มีรายละเอียดดังนี้

5.2.2.1 ความสามารถในการรองรับธุรกรรมจำนวนมาก (Scalability)

1) ข้อจำกัดในปัจจุบัน: เพิ่มจำนวนธุรกรรมในระบบ RSU-CMS และ RSU-Data-Anonymization อาจทำให้เกิดปัญหา เช่น ความล่าช้าและต้นทุนที่เพิ่มขึ้น โดยเฉพาะบนแพลตฟอร์มบล็อกเชนที่มีข้อจำกัด เช่น

1.1) อีเธอเรียม: แม้จะมีความปลอดภัยสูง แต่ระบบยังคงประสบปัญหาในการรองรับธุรกรรมในช่วงที่มีความหนาแน่นของเครือข่ายสูง ส่งผลให้ค่าธรรมเนียมเพิ่มขึ้นและประสิทธิภาพลดลง

1.2) ไบแนนซ์: รองรับธุรกรรมได้เร็วกว่าอีเธอเรียม แต่ยังมีความเสี่ยงด้านความหนาแน่นของเครือข่ายในกรณีที่มีผู้ใช้งานจำนวนมากพร้อมกัน

2) ผลกระทบ: ความล่าช้าและต้นทุนที่เพิ่มขึ้นส่งผลกระทบต่อการดำเนินงาน เช่น การจัดการความยินยอมของผู้ใช้งานแบบเรียลไทม์ หรือการประมวลผลข้อมูลจำนวนมากด้วย k-Anonymity

3) แนวทางการแก้ไข:

3.1) Layer-2 Solutions: การใช้เทคโนโลยี Slidechains, State Channels หรือ Rollups เพื่อลดภาระการประมวลผลบนบล็อกเชนเลเยอร์หนึ่ง

3.2) Sharding: การแบ่งเครือข่ายบล็อกเชนออกเป็นส่วนย่อยเพื่อกระจายการประมวลผลธุรกรรม

3.3) Hybrid Systems: ใช้กระบวนการประมวลผลนอกเครือข่ายร่วมกับการยืนยันในเครือข่าย

5.2.2.2 ความยืดหยุ่นในการจัดการข้อมูล (Flexibility)

1) ความท้าทายในการปรับเปลี่ยนข้อมูล: การรองรับความต้องการใหม่ เช่น การปรับเปลี่ยนโครงสร้างข้อมูลหรือการปรับค่าพารามิเตอร์ใน k-Anonymity เพื่อให้เหมาะสม

กับข้อมูลประเภทต่าง ๆ ยังคงเป็นเรื่องท้าทาย

2) ข้อจำกัดในด้านเทคนิค k-Anonymity: การนำ k-Anonymity มาใช้กับข้อมูลที่มีลักษณะหลากหลาย เช่น ข้อมูลที่ไม่สมดุลหรือข้อมูลที่มีมิติสูง อาจก่อให้เกิดการสูญเสียรายละเอียดข้อมูลสำคัญ

3) แนวทางการแก้ไข:

3.1) ใช้แบบจำลองที่สามารถปรับค่าพารามิเตอร์ k ให้เหมาะสมกับข้อมูลแต่ละประเภทโดยอัตโนมัติ (Dynamic k-Anonymity)

3.2) ใช้เทคนิคการบูรณาการการเรียนรู้ของเครื่องช่วยวิเคราะห์และปรับโครงสร้างข้อมูลให้เหมาะสม (Machine Learning Integration)

5.2.2.3 ผลกระทบโดยรวม:

1) Scalability: หากไม่สามารถรองรับธุรกรรมจำนวนมาก ๆ ได้ ระบบจะไม่สามารถตอบสนองต่อความต้องการในอนาคตได้อย่างรวดเร็ว

2) Flexibility: ความล่าช้าหรือข้อจำกัดในการปรับเปลี่ยนข้อมูล อาจลดทอนความเหมาะสมและความน่าเชื่อถือของระบบ

5.2.3 ความท้าทายในการยืนยันตัวตน

การยืนยันตัวตนในระบบ RSU-CMS และ RSU-Data-Anonymization ที่ใช้เทคนิคการแฝงข้อมูล (Pseudonymization) และ k-Anonymity มีเป้าหมายเพื่อลดความเสี่ยงจากการระบุตัวตนซ้ำ (Re-identification) และเพิ่มความปลอดภัยของข้อมูลส่วนบุคคล แม้จะช่วยลดโอกาสในการเข้าถึงข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต แต่กระบวนการดังกล่าวยังคงเผชิญกับความท้าทายที่ต้องได้รับการแก้ไขเพื่อเพิ่มความแม่นยำและประสิทธิภาพในการดำเนินงานดังนี้

5.2.3.1 การจับคู่ข้อมูลระหว่างค่าแฮชและข้อมูลต้นฉบับ

1) ความซับซ้อนของค่าแฮช: การใช้เทคนิคการแฝงข้อมูลเปลี่ยนข้อมูลที่สามารถระบุตัวตนได้ให้เป็นค่าแฮชเพื่อลดความเสี่ยง แต่การจับคู่ข้อมูลกลับไปยังต้นฉบับนั้นจำเป็นต้องใช้อัลกอริธึมหรือคีย์เฉพาะ ซึ่งอาจยุ่งยากในกรณีที่ข้อมูลถูกลดรายละเอียดเพิ่มเติม เช่น การจัดกลุ่มข้อมูลใน k-Anonymity

2) ผลกระทบจากการลดรายละเอียด: การลดทอนความแม่นยำของข้อมูล

เช่น การรวมช่วงอายุหรือการลดระดับความละเอียดของข้อมูลเชิงพื้นที่ อาจทำให้การจับคู่ข้อมูลเกิดข้อผิดพลาดส่งผลต่อความน่าเชื่อถือในการยืนยันตัวตน

5.2.3.2 ผลกระทบของการลดรายละเอียดใน k-Anonymity

1) ความแม่นยำที่ลดลง: การจัดกลุ่มข้อมูลให้คล้ายคลึงกันใน k-Anonymity แม้จะเพิ่มความปลอดภัย แต่ในกรณีที่ต้องการข้อมูลที่มีความละเอียดสูง อาจลดประสิทธิภาพและความถูกต้องในการยืนยันตัวตน

2) ความสมดุลระหว่างความปลอดภัยและความแม่นยำ: การตั้งค่า k ที่สูงเกินไปอาจลดความเสี่ยงจากการระบุตัวตน แต่จะลดทอนความละเอียดของข้อมูล ขณะที่ค่า k ที่ต่ำเกินไปอาจเพิ่มโอกาสในการระบุตัวตนซ้ำ

5.2.3.3 ความซับซ้อนของอัลกอริธึมในการยืนยันตัวตน

1) ความซับซ้อนที่จำเป็น: การออกแบบอัลกอริธึมที่สามารถจับคู่ข้อมูลอย่างปลอดภัยโดยไม่กระทบต่อความเป็นส่วนตัว เช่น การใช้ Homomorphic Encryption หรือ Secure Multi-Party Computation (SMPC) แม้จะช่วยเพิ่มความปลอดภัย แต่ยังต้องการทรัพยากรการประมวลผลที่สูง

2) ผลกระทบด้านประสิทธิภาพ: การเพิ่มความซับซ้อนในกระบวนการยืนยันตัวตนอาจทำให้ระบบทำงานช้าลงโดยเฉพาะเมื่อมีข้อมูลปริมาณมาก

5.2.3.4 การปรับตัวในบริบทที่เปลี่ยนแปลง

1) การจัดการข้อมูลแบบไดนามิก: ในระบบที่ข้อมูลเปลี่ยนแปลงแบบเรียลไทม์ เช่น การปรับปรุงข้อมูลทางการแพทย์ การจับคู่ข้อมูลต้องมีความยืดหยุ่นสูง

2) การผสานข้อมูลจากหลายแหล่ง: เมื่อข้อมูลต้องผสานจากแหล่งต่าง ๆ เช่น ฐานข้อมูลขององค์กรและแพลตฟอร์มภายนอก ความแตกต่างในโครงสร้างข้อมูลและการเข้ารหัสอาจเพิ่มความยุ่งยาก

5.2.3.5 แนวทางการปรับปรุง

1) การใช้เทคโนโลยีแบบใหม่: การนำการพิสูจน์ความรู้เป็นศูนย์ (Zero-Knowledge Proofs - ZKP) หรือการระบุตัวตนแบบกระจายศูนย์ (Decentralized Identity - DOD) มาใช้จะช่วยยืนยันตัวตนได้โดยไม่ต้องเปิดเผยข้อมูลต้นฉบับ

2) การพัฒนาระบบปรับเปลี่ยนได้: การสร้างระบบที่สามารถปรับแต่งค่า k หรือวิธีการจับคู่ข้อมูลให้เหมาะสมกับลักษณะข้อมูลและการใช้งาน

3) การจัดการข้อมูลแบบยืดหยุ่น: การใช้พื้นที่เก็บข้อมูลนอกเครือข่ายสำหรับจัดเก็บข้อมูลที่ละเอียดและการควบคุมสิทธิ์การเข้าถึงผ่านบล็อกเชน

โดยสรุป แม้การใช้เทคนิคการแฝงข้อมูลและ k-Anonymity จะเพิ่มความปลอดภัยให้กับข้อมูล แต่การยืนยันตัวตนในบริบทที่ข้อมูลถูกลดรายละเอียดหรือเปลี่ยนแปลงยังเป็นความท้าทายสำคัญ การพัฒนาเทคโนโลยีที่ทันสมัยและการออกแบบระบบที่ยืดหยุ่นจะช่วยเสริมความแม่นยำและประสิทธิภาพให้กับการยืนยันตัวตนในระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในอนาคต

5.2.4 การพึ่งพาการควบคุมแบบรวมศูนย์

แม้ว่าเทคโนโลยีบล็อกเชนจะมีคุณลักษณะเด่นในด้านการกระจายศูนย์ ซึ่งช่วยเพิ่มความโปร่งใส ความปลอดภัย และความน่าเชื่อถือในระบบ แต่ในบริบทของระบบ RSU-CMS และ RSU-Data-Anonymization การดำเนินงานบางส่วนยังต้องพึ่งพาการควบคุมแบบรวมศูนย์ ซึ่งอาจส่งผลต่อความเป็นอิสระของระบบในเชิงโครงสร้าง

5.2.4.1 ประเด็นที่เกี่ยวข้องกับการพึ่งพาการควบคุมแบบรวมศูนย์

1) การตั้งค่าระบบและการจัดการพารามิเตอร์

1.1) ในระบบ RSU-CMS การกำหนดพารามิเตอร์ เช่น จำนวนโหนด (Nodes) หรือระดับความปลอดภัย (Security Level) ของสัญญาอัจฉริยะยังต้องพึ่งพาการควบคุมจากผู้ดูแลระบบโดยตรง

1.2) ในระบบ RSU-Data-Anonymization การจัดการ k-Anonymity เช่น การกำหนดค่า k ซึ่งแสดงจำนวนกลุ่มข้อมูล ยังต้องพึ่งการตัดสินใจจากเจ้าหน้าที่ที่มีความเชี่ยวชาญ

2) การอนุมัติการเข้าถึงข้อมูล

แม้ว่าการใช้สัญญาอัจฉริยะจะช่วยจัดการสิทธิ์การเข้าถึงข้อมูลได้อย่างโปร่งใสและอัตโนมัติ แต่การกำหนดเงื่อนไขเบื้องต้นและการอนุมัติสิทธิ์ยังคงต้องพึ่งพาบุคคลหรือองค์กรที่เป็นศูนย์กลาง เช่น ผู้ดูแลระบบหรือผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นไปตามข้อกำหนดของกฎหมาย

3) การจัดการสัญญาอัจฉริยะ

การออกแบบและปรับปรุงสัญญาอัจฉริยะยังคงต้องเป็นหน้าที่ของนักพัฒนาที่ได้รับสิทธิ์เฉพาะ ซึ่งอาจก่อให้เกิดความเสี่ยงหากมีข้อผิดพลาดหรือการละเมิดสิทธิ์

5.2.4.2 ผลกระทบของการควบคุมแบบรวมศูนย์

1) ลดความเป็นอิสระของระบบ: การพึ่งพาบุคคลหรือองค์กรในการจัดการบางส่วนของระบบ อาจลดทอนความเป็นกระจายศูนย์ของบล็อกเชน ซึ่งเป็นคุณสมบัติของบล็อกเชน

2) ความเสี่ยงจากการละเมิดสิทธิ์: การควบคุมจากรวมศูนย์ หากขาดความโปร่งใส อาจเปิดช่องทางให้เกิดการละเมิดสิทธิ์ เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3) เพิ่มภาระในด้านความปลอดภัย: บทบาทที่สำคัญของผู้ดูแลระบบอาจทำให้เกิดความเสี่ยงในกรณีที่การโจมตีเฉพาะเจาะจงหรือเกิดความผิดพลาดจากการจัดการ

5.2.4.3 แนวทางการปรับปรุงเพื่อลดการพึ่งพาการควบคุมแบบรวมศูนย์

1) การนำการระบุตัวตนแบบกระจายศูนย์ (Decentralized Identity – DID) มาใช้ช่วยให้ผู้ใช้ควบคุมข้อมูลของตนเองได้โดยตรง ลดความจำเป็นในการอนุมัติจากผู้ดูแลระบบ

2) การใช้องค์กรอิสระแบบกระจายศูนย์ (Decentralized Autonomous Organization-DAO) ช่วยให้การตัดสินใจ เช่น การตั้งค่าพารามิเตอร์หรือการปรับปรุงสัญญาอัจฉริยะเป็นกระบวนการที่โปร่งใสผ่านการลงมติจากสมาชิกในระบบ

3) การพัฒนาระบบอัตโนมัติที่โปร่งใส การบันทึกการเปลี่ยนแปลงระบบที่สามารถตรวจสอบได้โดยผู้เกี่ยวข้องจะช่วยเพิ่มความน่าเชื่อถือ

โดยสรุป การลดการพึ่งพาการควบคุมแบบรวมศูนย์ในระบบ RSU-CMS และ RSU-Data-Anonymization เป็นสิ่งสำคัญที่จะช่วยเพิ่มความกระจายศูนย์ ลดความเสี่ยง และเสริมสร้างความมั่นใจในระบบให้แก่ผู้ใช้งาน ทั้งยังเป็นการตอบโจทย์ด้านความโปร่งใสและความน่าเชื่อถือที่เป็นเป้าหมายหลักของการใช้บล็อกเชน

5.3 ข้อเสนอแนะและงานวิจัยในอนาคต

จากข้อจำกัดและปัญหาที่ระบุไว้ การวิจัยในอนาคตสามารถดำเนินการเพื่อพัฒนาระบบและแก้ไขข้อท้าทายได้ในหลายด้าน การวิจัยในอนาคตควรมุ่งเน้นการพัฒนาระบบบริหารจัดการความยินยอม (RSU-CMS) และการจัดการข้อมูลนิรนาม (RSU-Data-Anonymization) ของมหาวิทยาลัย

รังสิตให้มีประสิทธิภาพ ความยืดหยุ่น และความปลอดภัยสูงขึ้น เพื่อรองรับความต้องการที่เปลี่ยนแปลงและหลากหลายในบริบทต่าง ๆ ไม่ว่าจะเป็นภาคธุรกิจหรือหน่วยงานรัฐ ระบบควรได้รับการออกแบบให้สอดคล้องกับข้อกำหนดทางกฎหมาย เช่น จีดีพีอาร์และพีดีพีเอ เพื่อให้สามารถจัดการข้อมูลส่วนบุคคลได้อย่างถูกต้องและปลอดภัย นอกจากนี้ การวิจัยควรให้ความสำคัญไปที่การเพิ่มความสามารถในการผสานเทคโนโลยีใหม่ ๆ เช่น บล็อกเชนแบบกระจายศูนย์และการเรียนรู้ของเครื่องเพื่อตอบสนองต่อความท้าทายด้านการจัดการข้อมูลในอนาคตอย่างมีประสิทธิภาพ โดยมีรายละเอียดดังนี้

5.3.1 การพัฒนาระบบให้สอดคล้องกับข้อกำหนดทางกฎหมายตามจีดีพีอาร์และพีดีพีเอ

5.3.1.1 การจัดการข้อมูลส่วนบุคคล: ระบบควรจะออกแบบให้สามารถลบหรือแก้ไขข้อมูลตามคำขอของเจ้าของข้อมูลได้ โดยยังความปลอดภัยและโปร่งใส เช่น การใช้การพิสูจน์ความรู้เป็นศูนย์ (Zero-Knowledge Proofs – ZKP) เพื่อยืนยันการลบข้อมูลโดยไม่เปิดเผยรายละเอียด หรือการจัดเก็บข้อมูลในพื้นที่เก็บข้อมูลนอกเครือข่าย (Off-Chain Storage) ซึ่งสามารถปรับเปลี่ยนข้อมูลได้โดยไม่กระทบต่อข้อมูลที่บันทึกในบล็อกเชน

5.3.1.2 การปรับปรุงการจัดการสิทธิ์: ใช้เทคนิคการลบแบบเลือกสรร (Selective Deletion Algorithms) เพื่อให้สามารถลบเฉพาะข้อมูลที่เกี่ยวข้องตามคำขอได้อย่างแม่นยำ โดยลดผลกระทบต่อข้อมูลอื่น ๆ ในระบบ การจัดการสิทธิ์นี้ยังรวมถึงการใช้สัญญาอัจฉริยะเพื่อกำหนดและควบคุมการเข้าถึงข้อมูลส่วนบุคคลในลักษณะที่โปร่งใสและตรวจสอบได้

5.3.2 การพัฒนาการปรับขนาดและการยืดหยุ่น

5.3.2.1 การเพิ่มการปรับขนาด: การใช้เทคโนโลยี Layer-2 เช่น Slidechains, Sharding หรือ Rollups สามารถเพิ่มขีดความสามารถในการรองรับธุรกรรมจำนวนมาก ลดความล่าช้าและลดต้นทุนการดำเนินงาน Layer-2 ช่วยกระจายภาระการประมวลผลจาก Layer-1 ทำให้ระบบสามารถทำงานได้เร็วขึ้นแม้ในช่วงที่ธุรกรรมหนาแน่น

5.3.2.2 ปรับปรุงการยืดหยุ่น: ออกแบบโครงสร้าง k-Anonymity ให้มีความยืดหยุ่นสามารถรองรับข้อมูลหลากหลายรูปแบบ เช่น ข้อมูลเชิงพื้นที่หรือข้อมูลเชิงเวลา โดยยังคงรักษาความปลอดภัยและความแม่นยำ ด้วยการปรับค่า Dynamic k-Anonymity เพื่อให้เหมาะสมกับข้อมูลที่แตกต่างกัน จะช่วยลดผลกระทบต่อความถูกต้องของข้อมูลและเพิ่มประสิทธิภาพในการใช้งานระบบ

5.3.3 การพัฒนาการกระจายศูนย์

5.3.3.1 ลดการพึ่งพาการควบคุมแบบรวมศูนย์: การพัฒนาโครงสร้างที่เน้นการกระจายศูนย์ สามารถลดบทบาทของหน่วยงานที่ควบคุมแบบรวมศูนย์ได้ เช่น การใช้องค์กรอิสระแบบกระจายศูนย์ (Decentralized Autonomous Organizations – DAOs) เพื่อจัดการการตัดสินใจในระบบอาศัยการลงมติจากสมาชิกในเครือข่าย ช่วยเพิ่มความโปร่งใสและลดความเสี่ยงที่เกิดจากการควบคุมโดยหน่วยงานเดียว

5.3.3.2 ส่งเสริมการระบุตัวตนแบบกระจายศูนย์: การวิจัยและพัฒนาเทคโนโลยีการระบุตัวตนแบบกระจายศูนย์ (Decentralized Identity – DID) และข้อมูลรับรองที่ตรวจสอบได้ (Verifiable Credentials -VCs) ช่วยเพิ่มความแม่นยำและความปลอดภัยในการยืนยันตัวตน โดยผู้ใช้สามารถควบคุมข้อมูลส่วนบุคคลของตนเองได้โดยตรง และลดความซับซ้อนในกระบวนการจัดการข้อมูลส่วนบุคคลในระบบ

5.3.4 การสร้างสมดุลระหว่างความปลอดภัยและประสิทธิภาพ

5.3.4.1 ปรับปรุง k-Anonymity: วิจัยการผสมผสานระหว่าง k-Anonymity และความเป็นส่วนตัวที่แตกต่าง (Differential Privacy) เพื่อเสริมความปลอดภัยของข้อมูลในระดับที่สูงขึ้น โดยลดโอกาสในการเชื่อมโยงข้อมูลกลับไปยังบุคคลเฉพาะเจาะจง ทั้งนี้ต้องคำนึงถึงการรักษาประสิทธิภาพของแบบจำลองการเรียนรู้ของเครื่องให้ไม่ลดลงอย่างมีนัยสำคัญ เพื่อให้สมารถนำข้อมูลไปประมวลและวิเคราะห์ต่อได้อย่างมีประสิทธิภาพ

5.3.4.2 พัฒนาแบบจำลองที่ยืดหยุ่น: โดยสร้างแบบจำลองการลดรายละเอียดข้อมูล (Data Reduction Models) ที่สามารถรักษาความแม่นยำและความสมบูรณ์ของข้อมูลได้ แม้จะมีการลดระดับความละเอียดในข้อมูล โดยออกแบบให้รองรับการประมวลผลในอนาคต และสามารถปรับตัวเข้ากับข้อมูลหลากหลายประเภท เช่น ข้อมูลเชิงเวลา หรือข้อมูลที่มีมิติสูง

5.3.5 การขยายการใช้งานในบริบทใหม่

5.3.5.1 การประยุกต์ใช้ในการแพทย์: ระบบ RSU-CMS และ RSU-Data-Anonymization สามารถพัฒนาเพื่อตรวจสอบและจัดการข้อมูลทางการแพทย์ที่ต้องการความปลอดภัยสูง เช่น ข้อมูลประวัติการรักษาและผลตรวจทางการแพทย์ โดยบล็อกเชนช่วยเพิ่มความโปร่งใสและความ

น่าเชื่อถือ ในขณะที่ k-Anonymity ลดความเสี่ยงจากการระบุตัวตนซ้ำ

5.3.5.2 การศึกษาข้อมูลในระบบการศึกษา: เทคโนโลยีบล็อกเชนและ k-Anonymity สามารถนำมาใช้ในการวิเคราะห์ข้อมูลนักเรียน เช่น ผลการเรียน ความต้องการพิเศษ และการบริหารจัดการสถานศึกษา ช่วยเพิ่มความแม่นยำในการวิเคราะห์ข้อมูลขนาดใหญ่และรักษาความปลอดภัยของข้อมูลนักเรียน

5.3.5.3 การจัดการข้อมูลโลจิสติกส์: ระบบสามารถนำไปใช้ในอุตสาหกรรมโลจิสติกส์เพื่อเพิ่มความโปร่งใสในการติดตามและจัดการข้อมูล เช่น การติดตามสถานะสินค้าหรือการจัดการเส้นทางขนส่ง ทั้งนี้ยังช่วยรักษาความปลอดภัยของข้อมูลสำคัญ เช่น สัญญาหรือข้อมูลซัพพลายเชน ลดความเสี่ยงจากการปลอมแปลงข้อมูลได้

5.3.6 การใช้เทคโนโลยีใหม่เพื่อเพิ่มประสิทธิภาพระบบ

5.3.6.1 การเรียนรู้แบบสหพันธ์ (Federate Learning) และบล็อกเชน: ศึกษาการผสานการเรียนรู้แบบสหพันธ์กับเทคโนโลยีบล็อกเชนเพื่อเพิ่มประสิทธิภาพในการประมวลผลแบบกระจาย โดยการเรียนรู้แบบสหพันธ์ช่วยให้ระบบสามารถวิเคราะห์ข้อมูลได้โดยไม่ต้องถ่ายโอนข้อมูลดิบออกจากอุปกรณ์หรือเครื่องแม่ข่ายของผู้ใช้งาน ขณะที่บล็อกเชนช่วยจัดการสิทธิ์และบันทึกธุรกรรมอย่างโปร่งใสและปลอดภัย

5.3.6.2 เทคโนโลยีการเข้ารหัสใหม่: วิจัยการนำเทคโนโลยีการเข้ารหัสแบบโฮโมมอร์ฟิก (Homomorphic Encryption) หรือ การประมวลผลแบบหลายฝ่ายที่ปลอดภัย (Secure Multi-Party Computation) มาใช้เพื่อเพิ่มความปลอดภัยในการจัดการข้อมูล โดยการเข้ารหัสแบบโฮโมมอร์ฟิกช่วยให้สามารถคำนวณข้อมูลที่เข้ารหัสได้โดยตรงโดยไม่ต้องถอดรหัส และการประมวลผลแบบหลายฝ่ายที่ปลอดภัยช่วยป้องกันการเข้าถึงข้อมูลที่ได้รับอนุญาตในระหว่างกระบวนการประมวลผลข้อมูลร่วมกันในระบบแบบกระจาย

บรรณานุกรม

กมลา บัวยั่งยืน. (2562). ปัญหากฎหมายเกี่ยวกับสัญญาอัจฉริยะ. *วารสารรามคำแหง ฉบับนิติศาสตร์, ปีที่ 8* (ฉบับที่ 27, 100-131. สืบค้นจาก https://so05.tci-thaijo.org/index.php/lawjournal/ article/view/231858

ขจรศักดิ์ ศิริศิลาศักดิ์, และมัชฌิกา อ่องแตง. (2565). การปกป้องข้อมูลส่วนบุคคลด้วยเทคนิคข้อมูลแฝงและข้อมูลนิรนามผ่านบริการพร็อกซี่บนระบบเครือข่าย. *วารสารบัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์*, 3, 39-58. สืบค้นจาก https://grad.dpu.ac.th/journal10-3-64.html

ชวิน อุ่นภัทร, และปิยบุตร บุญอร่ามเรือง. (2564). *Thailand data protection guidelines 3.2: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลสำหรับการวิจัยและสถิติ*. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย

ดวงดาว จินดาวัฒนะ. (2560). ปัญหากฎหมายของไทยเกี่ยวกับสัญญาอัจฉริยะ (Smart Contract). *วารสารวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย*, *9* (1), 18-29. สืบค้นจาก http://utcc2.utcc.ac.th/lawjournal/91/18_29.pdf

ธนาคารแห่งประเทศไทย (2564). *แนวปฏิบัติการใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการให้บริการทางการเงิน*. สืบค้นจาก https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2564/ThaiPDF/25640101.pdf

นคร เสรีรักษ์, ฉรงค์ ใจหาญ, ประสิทธิ์ ปิวาวัฒนพานิช, ศุภเกียรติ ศุภศักดิ์ศึกษากร, และนิชานันท์ นันทศิริศรณ์. (2562). *General Data Protection Regulation ฉบับภาษาไทย*. กรุงเทพมหานคร: บริษัท พี.เพรส จำกัด. กรุงเทพมหานคร

ปิยะบุตร บุญอร่ามเรือง, พัฒนาพร โกวพัฒนกิจ, พีรพัฒ โชคสุวัฒนสกุล, เสกสิริ นิวัติศัยวงศ์, ปิติ เยี่ยมจำรูญลาภ, ชวิน อุ่นภัทร, … , โมกข์พิศุทธิ์ รตารุณใ (2563). *Thailand data protection guidelines 3.0: แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล*. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

พีรดล สามะศิริ, และอันนต์วัฒน์ ทิพย์ภาวัต. (2564). *การจัดทำข้อมูลนิรนาม (Data Anonymization)*. สืบค้นข้อมูลจาก https://bdi.or.th/big-data-101/data-anonymization/

ราชกิจจานุเบกษา. (2562). *พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (2562)*. เล่ม 136 ตอนที่ 69 ก., 52-95 ประกาศใช้ 27 พฤษภาคม 2562.

บรรณานุกรม (ต่อ)

วันพิชิต ชินตระกูลชัย. (2564). *ข้อมูลส่วนบุคคล ใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล มีกี่ประเภท อะไรบ้าง?* สืบค้นจาก https://openpdpa.org/personal-data-type/

ศูนย์บริการข้อมูลภาครัฐเพื่อประชาชน. (2565*). เจ้าของข้อมูลส่วนบุคคล (Data Subject)*. สืบค้นจาก https://www.gcc.go.th/2022/06/21/เจ้าของข้อมูลส่วนบุคคล/

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ฝ่ายบริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี. (2566). *สิทธิของเจ้าของข้อมูลส่วนบุคคล*. สืบค้นจาก https://www.thailibrary.in.th/2023/09/25/datasubjectrights/

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2564). *Blockchain for government services: การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐ เวอร์ชัน 2.0.* สืบค้นจาก https://www.dga.or.th/document-sharing/dga-e-book/annual-blockchain/47115/

อธิพร สิทธิธีรรัตน์. (2558). *ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์*. สืบค้นจาก http://ethesisarchive.library.tu.ac.th/thesis/2015/TU_2015_5701033531_3922_2696.pdf

อริยะ ตั้งสวานิช. (2564). *ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562*. สืบค้นจาก https://www.law.chula.ac.th/ public-services/chula-lawlab-for-pdpa/ep-4/

Alhajri, M., Rudolph, C., & Shahraki, A. S. (2022). A blockchain-based consent mechanism for access to fitness data in the healthcare context. *IEEE Access,*10, 22960-22979. doi: 10.1109/ACCESS.2022.3154106

Baskaran, H., & Yussof, S., (2020). Blockchain and the Personal Data Protection Act 2010 (PDPA) in Malaysia. In *2020 8th International Conference on Information Technology and Multimedia (ICMU)* (pp. 189-193). IEEE. doi: 10.1109/ICIMU49871.2020.9243493

Bauer, D. P. (2022). Solidity Chapter. In *Getting Started with Ethereum* (pp. 29-52). Apress. doi: 10.1007/978-1-4842-8045-4_2

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908-164940. doi: 10.1109/ACCESS.2019.2950872

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy* (pp. 104-121). IEEE. doi: 10.1109/SP.2015.14

Burton, C., & Hoffman, S. (2015, September). *Personal data, anonymization, and pseudonymization in the EU*. WSGR Data Advisor. Retrieved from https://www.wsgrdataadvisor.com/2015/09/personal-data-anonymization-and-pseudonymization-in-the-eu/

Data Privacy Manager. (2021). *Pseudonymization according to the GDPR [Definitions and examples]*. Retrieved from https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/

Data Privacy Manager. (2024). *20 biggest GDPR fines so far [2025]*. Retrieved from https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020

Diaz, C., Seys, S., Classens, J., & Praneel, B. (2002). Towards measuring anonymity. In R. Dingledine & P. Syverson (Eds.), *Privacy enhancing technologies* (Vol. 248, pp. 54-68). Springer. doi: 10.1007/3-540-36467-6_5.

Dwork, C., Smith, A., Steinke, T., & Ullman, J. (2017). Exposed! A survey of attacks on private data. *Annual Review of Statistics and Its Application*, 4, 61-84. doi: 10.1146/annurev-statistics-060116-054123.

European Network and Information Security Agency (2018). *Recommendations on shaping technology according to GDPR provisions. – An overview on data pseudonymization*. doi:10.2824/74954

European Network and Information Security Agency (2019). *Pseudonymization techniques and best practices: Recommendations on shaping technology according to data protection and privacy provisions.* doi: 10.2824/247711

European Network and Information Security Agency (2021). *Data pseudonymization – Advanced techniques and use cases: technical analysis of cybersecurity measures in data protection and privacy.* doi: 10.2824/860099

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

European Parliament. (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Federal Bureau of Investigations. (2015). *Rose Ulbrich, the creator and owner of the Silk Road website, found guilty in Manhattan federal court on all counts* [Press release]. Retrieved from https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts.

Formichella, J. P., Jamallsawat, N., & Brikshasri, A. (2020). *Comparing privacy laws: GDPR v. Thai Personal Data Protection Act.* OneTrust DataGuidance. Retrieved from https://www.dataguidance.com/sites/default/files/gdpr_v_thailand_updated.pdf

GeeksforGeeks. (2024). *Types of blockchain.* Retrieved from https://www.geeksforgeeks.org/types-of-blockchain/

GeeksforGeeks. (2024). *Top 10 Python applications in real world.* Retrieved from https://www.geeksforgeeks.org/python-applications-in-real-world/

Gowrishankar, S., & Veena, A. (2019). *Introduction to Python programming*. CRC Press, Taylor & Francis Group, Retrieved from https://www.iimchyderabad.com/Material/introduction-to-python-programming.pdf

Haque, A. B., Islam, A. K. M. N., Hyrynsalmi, S., Naqyi, B., & Smolander, K. (2021). GDPR compliant blockchain: A systematic literature review. *IEEE Access*, 9, 50593-50606. doi: 10.1109/ACCESS.2021.3069877

Hamidovic, H., Kabil, J., & Šehić, E. (2019, April). EU General Data Protection Regulation (GDPR): Anonymisation and pseudonimisation in function of data protection. In *Book of Proceedings of International Scientific Conference on Digital Economy (DIEC 2019*) (pp. 219-230). Tuzla, Bosnia and Herzegovina.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Henriksen-Bulmer, J., & Jeary, S. (2016). Re-identification attacks: A systematic literature review. *International Journal of Information Management, 36*(6), 1184-1192. doi: 10.1016/j.ijinfomgt.2016.08.002

Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S., and Ylianttila, M. (2021). Survey on blockchain-based smart contracts: Technical aspects and future research. *IEEE Access*, 9, 87643-87662. doi: 10.1109/ACCESS.2021.3068178

Hristov P., & Dimitrov W. (2018). The blockchain as a backbone of GDPR compliant frameworks. In *Proceedings of 8th International Multidisciplinary Symposium – Challenges and Opportunities for Sustainable Development Through Quality and Innovation in Engineering and Research Management* (Vol. 20, No. 1, pp. 305-310).

Information Commissioner's Office. (2022). *Chapter 5: Privacy-enhancing technologies (PETs)*. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based distributed data sharing platforms. *arXiv Preprint arXiv:2007.04847,* 1-18. doi: 10.48550/arXiv.2007.04847

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). Design and development of a blockchain-based consent management. *Electronics, 10(24)*, 3131, 1-22. doi: 10.3390/electronics10243131

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). A systematic review of blockchain for consent management. *Healthcare*, *9*(2), 137, 1-21. doi: 10.3390/healthcare9020137

Kaul, S. (2024). *Learn: Machine learning in Python with code examples*. Retrieved from https://medium.com/@sumit.kaul.87/a-comprehensive-guide-to-scikit-learn-machine-learning-in-python-with-code-examples-8e4670877d03

Kondova, G., & Erbguth, J. (2020). Self-sovereign identity on public blockchains and the GDPR. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing* (pp. 342-345). Brno, Czech Republic. doi: 10.1145/3341105.3374066

Kumari, S. (2024). *Advantages and disadvantages of Python*. Retrieved from https://www.naukri.com/code360/library/advantages-and-disadvantages-of-python

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

LaFever, G. (2021). *10 Truths about GDPR pseudonymization*. Retrieved from https://www.linkedin.com/pulse/10-truths-gdpr-pseudonymisation-gary-lafever

Lapwattanaworakul, J., Srisa-An, C., & Aribarg, T. (2023). Blockchain-based auxiliary systems for pseudonymization and consent management. *TEM Journal*, *12*(4), 2470-2480. doi: 10.18421/TEM124-59

Lin, S., Zhang, L., Li, J., Ji, L., & Sun, Y. (2022). A survey of application research based on blockchain smart contract. *Wireless Networks*, 28, 635-690, doi: 10.1007/s11276-021-02874-x

Maker, A. (2019). *What is scikit learn?* Retrieved from https://dev.to/amigosmaker/what-is-scikit-learn-5ddl

Melin, K. (2019). *The GDPR compliance of blockchain: A qualitative study on regulating innovative technology* (Master's thesis, Uppsala University). UPTEC STS 19046. Retrieved from http://uu.diva-portal.org/smash/get/diva2:1370599/FULLTEXT01.pdf

Mitra, S. (2022). OConsent: Open consent protocol for privacy and consent management with blockchain. *arXiv Preprint arXiv:2201.01326*, 1-39. doi: 10.48550/arXiv.2201.01326

Mohanta, B. K., Jene D., Panda, S. S., & Sobhanayak S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, 8, 1-19. doi: 10.1016/j.iot.2019.100107

Molina, F., Betarte, G., & Luna, C. (2021). Design principles for constructing GDPR-compliant blockchain solutions. In *Proceedings of the IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB),* IEEE Xplore. doi: 10.1109/WETSEB2558.2021.00008

Morgan, S. (2023). *2022 Official Cybercrime Report: Cybercrime to cost the world $8 trillion annually in 2023.* Cybersecurity Ventures. Retrieved from https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Mumu, S., Kappos, D., & Sumroy, R. (2021). *The right to be forgotten meets the immutable: A practical guide to GDPR-compliant blockchain solutions.* Retrieved from https://www.cravath.com/files/Uploads/Documents/Publications/3898415_1.pdf

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review*, 21260. Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large database (How to break anonymity to the Netflix Prize database). In *2008 IEEE Symposium on Security and Privacy* (pp. 111-125), Oakland, USA. doi: 10.1109/SP.2008.33.

Parrots, S. (2024*). Blockchain hash: What is it and what is it for.* Retrieved from https://www.scalingparrots.com/en/blockchain-hash-what-is-it/

Privacy Working Group of INATBA. (2020). *Report on data privacy regulations applicable to blockchain technology in various jurisdictions worldwide.* International Association for Trusted Blockchain Applications. Retrieved from https://inatba.org/wp-content/uploads/2021/01/2020-12-Privacy-WG-Report-on-Data-Protection.pdf

Rupasinghe, T., Burstein, F., & Rudolph, C. (2019). Blockchain-based dynamic patient consent: A privacy-preserving data acquisition architecture for clinical data analytics. In *Proceedings of the 40th International Conference on Information Systems (ICIS 2019)* (pp. 1-9). Munich, Germany.

Sabzwari, N. (2024). *Advantages and disadvantages of smart contracts in blockchain technology*. Retrieved from https://blockapex.io/advantages-and-disadvantages-of-smart-contracts/

Sardá, T., Natale, S., Sotirakopoulos N., & Monaghan, M. (2019). Understanding online anonymity. *Media Culture & Society*, *41*(4), 557-564. doi:10.1177/0163443719842074

Service of the Republic of Poland. (2018). *Security standard: Data openness standards.* Retrieved from https://dane.gov.pl/media/ckeditor/2018/11/06/security-standard_ 2018.odt

Shah, P., Forester, D., Berherich, M., & Raspe, C. (2019). *Blockchain technology: Data privacy issues and potential mitigation strategies.* Practical Law, Thomson Reuters, Retrieved from https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Sirur, S., Nurse, J. R. C., & Webb, H. (2019). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security at ACM Conference on Computer and Communications Security (CCS)* (pp. 88-95). doi: 10.1145/3267357.3267368

Slijepcevic, D., Henzl, M., Klausner, L. D., Dam, T., Kieseberg, P., & Zeppelzauer, M. (2021). *k*-Anonymity in Practice: How generalisation and suppression affect machine learning classifiers. *Computers & Security*, 111, 102488, 1-19. doi: 10.1016/j.cose.2021.102488

Suripeddi, M. K.S., & Purandare, P. (2021). Blockchain and GDPR: A study on compatibility issues of the distributed ledger technology with GDPR data processing. *Journal of Physics: Conference Series*, *1964*(2021), 042005, 1-12. doi: 10.1088/1742-6596/1964/4/042005

Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems*, *10*(5), 557-570. doi: 10.1142/s0218488502001648

Szabo, N. (2017). *Winning strategies for smart contracts* (Blockchain Research Institute Big Idea Whitepaper. 1-37). Retrieved from https://grazielabrandao.wordpress.com/wp-content/uploads/2019/06/g86cmijoeemm8wp4g3tktg_1c16c8a028ce11e999f58be72bb04114_szabo-smart-contracts-v6d_1_.pdf

Techsauce Team. (2022). *ชวนรู้จัก Consensus Algorithm ระบบฉันทามติบน Blockchain มีอะไรบ้าง แตกต่างกันอย่างไร*. [Get to know consensus algorithms on blockchain: What are they and how do they differ?]. Retrieved from https://techsauce.co/tech-and-biz/how-are-blockchain-consensus-algorithm-different

Techshill Brew. (2022). *Types of blockchain (Part 4-Blockchain series).* Retrieved from https://medium.com/techskill-brew/types-of-blockchain-part-4-blockchain-basics-c0b2e40c1780

Teodora, C. L., & Lodie, C. A. (2023). *Re-identification attacks and data protection law,* ai-regulation.com. Retrieved from https://ai-regulation.com/re-identification-attacks-and-data-protection-law

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

The Organisation for Economic Co-operation and Development (2005). *Glossary of statistical terms: Quasi-identifier.* Retrieved from https://stats.oecd.org/glossary/detial.asp? ID=6961

Tinabo, R., Mtenzi, F., & Shea, B. O. (2009). Anonymisation vs. pseudonymisation: Which one is most useful for both privacy protection and usefulness of e-healthcare data. In *2009 International Conference for Internet Technology and Secured Transactions* (pp. 1-6). IEEE Xplore. doi: 10.1109/ICITST.2009.5402501

Tith, D. (2020). *Data sharing and consent management of electronic health record based on the blockchain technology* (Master's thesis, Tokyo Institute of Technology). Tokyo Tech Research Repository. Retrieved from https://t2r2.star.titech.ac.jp/rrws/file/CTT100830878/ATD100000413/

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). GDPR-compliant personal data management: A blockchain-based solution. *IEEE Transaction on Information Forensics and Security*, 15, 1746-1767. doi: 10.1109/TIFS.2019.2948287

Vargas, J. C. (2019). Blockchain-based consent manager for GDPR compliance. In *H. RoBnagel, S. Wagner, & D. Hühnlein* (Eds.)*, Proceedings of the Open Identity Summit 2019* (pp. 165-170). Gesellschaft für. Informatik.

Voss, W. G. (2021). Data protection issues for smart contracts. In M. Corrales, M. Fenwick, & S. Wrbka (Eds.), *Smart contracts: Technological, business & legal perspectives* (pp. 79-100). Hart Publishing/Bloomsbury. doi: 10.5040/9781509937059.ch-004

Zarakowski, M., Jongerius, S., Arribas, I., Grant, J., Garrido, E. F., & Vandy, N. (2020). *The impact of data protection regulations on the blockchain ecosystem: Report on survey results.* International Association for Trusted Blockchain Applications. Retrieved from https://inatba.org/wp-content/uploads/2020/11/2020-11-Privacy-WG-Survey-Report.pdf

Zemler, F. (2019). Concepts for GDPR-compliant processing of personal data on blockchain: A literature review. *Anwendungen und Konzepte der Wirtschaftsinformatik*, 10, 96-107. Retrieved from https://www.researchgate.net/publication/338117615_Concepts_for_GDPR-ompliant_Processing_of_Personal_Data_on_Blockchain_A_Literature_Review

บรรณานุกรม (ต่อ)

Zhang, R., Xue, R., & Liu, L. (2020). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), Article 51, 1-34. doi: 10.1145/3316481

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the IEEE International Congress on Big Data* (pp. 557-564). doi: 10.1109/BigDataCongress.2017.85

Zou, W., Lo, D., Kochhar, P. S., Le, X. D., Xia, X., Feng, Y., …, Xu, B. (2021). Smart contract development: Challenges and opportunities. *IEEE Transactions on Software Engineering*, 47(10), 2084-2106. doi: 10.1109/TSE.2019.2942301

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the IEEE Security and Privacy Workshop* (pp. 180-184). doi: 10.1109/SPW.2015.27

มหาวิทยาลัยรังสิต Rangsit University

ประวัติผู้วิจัย

ชื่อ	จิรภัทร ลาภวัฒนวรกุล
วัน เดือน ปีเกิด	5 สิงหาคม 2516
สถานที่เกิด	จังหวัดตรัง ประเทศไทย
ประวัติการศึกษา	มหาวิทยาลัยสงขลานครินทร์ ปริญญาบริหารธุรกิจบัณฑิต สาขาวิชาคอมพิวเตอร์ธุรกิจ, 2538 มหาวิทยาลัยหอการค้าไทย ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศและการสื่อสาร, 2558
ที่อยู่ปัจจุบัน	399/25 โชคชัยร่วมมิตรคอนโด ถนนวิภาวดีรังสิต ซอย 16/5 แขวงจอมพล เขตจตุจักร กรุงเทพฯ
ตำแหน่งปัจจุบัน	นักวิจัยและที่ปรึกษาอิสระด้านเทคโนโลยีสารสนเทศ

มหาวิทยาลัยรังสิต Rangsit University