การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

โดย

สรพรรค ภักดีศรี

มหาวิทยาลัยรังสิต Rangsit University

ดุษฎีนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม

หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี

บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต

ปีการศึกษา 2564

MULTIMODAL BIOMETRIC AUTHENTICATION USING FACE AND VOICE RECOGNITION FOR CLOUD COMPUTING SERVICES

BY

SORAPAK PUKDESREE

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 2021

ดุษฎีนิพนธ์เรื่อง

การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

โดย

สรพรรค ภักดีศรี

ได้รับการพิจารณาให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยรังสิต
ปีการศึกษา 2564

รศ. อานนท์ สุขเสถียรวงศ์ ประธานกรรมการสอบ	รศ. ดร.สิริพร ศุภทราทิพย์ กรรมการ
ผศ. ดร.กวีวัฒน์ อำนาจโชติพันธุ์ กรรมการ	ผศ. ดร.มีนนภา รักษ์หิรัญ กรรมการ
	รศ. ดร.ปณิธิ เนตินันทน์ กรรมการและอาจารย์ที่ปรึกษา

บัณฑิตวิทยาลัยรับรองแล้ว

(ผศ. ร.ต. หญิง ดร.วรรณี ศุขสาตร)
คณบดีบัณฑิตวิทยาลัย
24 พฤษภาคม 2565

มหาวิทยาลัยรังสิต Rangsit University

Dissertation entitled

MULTIMODAL BIOMETRIC AUTHENTICATION USING FACE AND VOICE RECOGNITION FOR CLOUD COMPUTING SERVICES

by

SORAPAK PUKDESREE

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

Rangsit University
Academic Year 2021

----------	----------
Assoc. Prof. Anon Sukstrienwong Examination Committee Chairperson	Assoc. Prof. Siriporn Supratid, D.S. Member
----------	----------
Asst. Prof. Kawiwat Amnatchotiphan, Ph.D. Member	Asst. Prof. Meennapa Rukhiran, Ph.D. Member
	----------
	Assoc. Prof. Paniti Netinant, Ph.D. Member and Advisor

มหาวิทยาลัยรังสิต Rangsit University

Approved by Graduate School

(Asst. Prof. Plt. Off. Vannee Sooksatra, D.Eng.)
Dean of Graduate School
May 24, 2022

กิตติกรรมประกาศ

ดุษฎีนิพนธ์ฉบับนี้สำเร็จได้เป็นอย่างดีเนื่องด้วยความอนุเคราะห์จาก รศ. ดร.ปณิธิ เนตินันทน์ อาจารย์ที่ปรึกษา ที่ให้ความเอาใจใส่ช่วยเหลือ และคอยให้คำปรึกษาแนะนำเป็นอย่างดีมาโดยตลอด นอกจากนี้ข้าพเจ้าขอแสดงความขอบพระคุณเป็นอย่างสูงต่อบุคคลที่ได้มีส่วนร่วมและสนับสนุนให้ข้าพเจ้าสำเร็จการศึกษา รศ. อานนท์ สุขเสถียรวงศ์ ผศ. ดร.มีนนภา รักษ์หิรัญ และคณาจารย์ทุกท่าน ขอขอบคุณกำลังใจและการแบ่งปันซึ่งกันและกันจากเพื่อนๆร่วมหลักสูตรทุกคน สุดท้ายนี้ข้าพเจ้าขอขอบพระคุณครอบครัวศรีวะรมย์ คุณวนิดา ศรีวะรมย์ ครอบครัวภักดีศรี คุณพ่อ คุณแม่ ภรรยาและบุตร ที่เป็นกำลังใจ อดทน และร่วมสนับสนุนให้ข้าพเจ้าสำเร็จการศึกษา

สรพรรค ภักดีศรี
ผู้วิจัย

มหาวิทยาลัยรังสิต Rangsit University

5808350 : สรพรรค ภักดีศรี
ชื่อดุษฎีนิพนธ์ : การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง เพื่อการบริการประมวลผลแบบคลาวด์
หลักสูตร : ปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา : รศ. ดร.ปณิธิ เนตินันทน์

บทคัดย่อ

ปัจจุบันเทคโนโลยีการคำนวณแบบคลาว์ดมีการนำไปประยุกต์ใช้ในด้านต่าง ๆ ปี ค.ศ. 2017 มีการคาดการณ์ว่าเทคโนโลยีการคำนวณแบบคลาว์ดจะมีมูลค่ามากถึง 250 พันล้านเหรียญ ในประเทศไทยเทคโนโลยีการคำนวณแบบคลาว์ดก็มีแนวโน้มที่สอดคล้องกับประเทศอื่น ๆ เช่นกัน จากข้อมูลการสำรวจโดย Forester ปี ค.ศ. 2012 แสดงให้เห็นว่าเทคโนโลยีการคำนวณแบบคลาว์ดมีอัตราการขยายตัวเพิ่มขึ้นอย่างต่อเนื่อง ดังนั้นผู้วิจัยจึงได้นำเสนอกรอบแนวคิดในการประยุกต์ใช้การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

งานวิจัยนี้ยังมุ่งเน้นการประเมินผลกรอบแนวคิดในการประยุกต์การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ ผลการศึกษาเชิงประจักษ์พบว่า 1) ค่า Accuracy Score เท่ากับ 0.712500 2) ค่า Precision Positive เท่ากับ 0.844828 3) ค่า Precision Negative เท่ากับ 0.363636 4) ค่า Recall Positive เท่ากับ 0.777778 5) ค่า Recall Negative เท่ากับ 0.470588 6) ค่า F1 score positive เท่ากับ 0.809917 7) ค่า F1 score negative เท่ากับ 0.410256 ผู้วิจัยใช้สถิติไคสแควร์พบว่าสมมติฐานการวิจัยมีความถูกต้อง นอกจากนี้พบว่า 1) ชีวมิติเสียงมีความเหมาะสมที่ในการพิสูจน์ตัวจริงร่วมกับชีวมิติภาพใบหน้า 2) อัตราการผิดพลาดของการรู้จำลดลง (Fake Detection) 3) ระยะเวลาของเสียงที่บันทึกควรอยู่ระหว่าง 2 ถึง 4 วินาที 4) จำนวนภาพใบหน้า 4 ภาพเหมาะสมต่อการรู้จำ และ 5) ควรกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ไว้ที่ร้อยละ 60 การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ที่นำเสนอมีประโยชน์หลายด้าน เช่น ความปลอดภัย ความพร้อมใช้งาน และความยืดหยุ่น ผู้วิจัยได้ประยุกต์ใช้กรอบแนวคิดนี้กับระบบการยืนยันตัวตนในการเข้าสอบออนไลน์ในช่วงสถานการณ์การแพร่ระบาดของโรคโควิด-19 ในประเทศไทย

(ดุษฎีนิพนธ์มีจำนวนทั้งสิ้น 215 หน้า)

คำสำคัญ: ชีวมิติ, การพิสูจน์ตัวจริง, การประมวลผลแบบคลาวด์

ลายมือชื่อนักศึกษา ..... ลายมือชื่ออาจารย์ที่ปรึกษา .....

5808350 : Sorapak Pukdesree

Dissertation Title : Multimodal Biometric Authentication using Face and Voice Recognition for Cloud Computing Services

Program : Doctor of Philosophy in Information Technology

Dissertation Advisor : Assoc. Prof. Paniti Netinant, Ph.D.

Abstract

Cloud computing technology is now widely used in a wide variety of domains. Cloud computing trends are expected to reach a value of approximately $250 billion in 2017. Thailand's cloud computing situation is similar to that of other countries. According to a 2012 Forester survey, cloud computing utilization has been increasing at a constant rate. As a result, we proposed using face and voice recognition to provide multimodal biometric authentication for cloud computing services. The proposed methodology has several advantages, including its speed, adaptability, and security.

Additionally, the research evaluates the proposed multimodal biometric authentication for cloud computing services using face and voice recognition. The following are the findings of this empirical study: 1) The accuracy score is 0.712500. 2) The precision value is 0.844828. 3) Precision The minus sign indicates a negative value of 0.363636. 4) The positive recall value is 0.777778. 5) The negative value for the recall is 0.470588. 6) The positive value of the F1 score is 0.809917. 7) The negative value of the F1 score is 0.410256. Finally, the researchers analyze the collected data using Chi-square statistics to determine the validity of the research hypothesis. Additionally, this result demonstrates that 1) voice biometrics can be used in conjunction with facial biometrics for biometric authentication, 2) the rate of fake detection can be decreased by utilizing multimodal biometric authentication with face and voice recognition, and 3) the duration of the voice recorded should be between 1 and 4 seconds. 4) There should be four face images, and 5) the minimum acceptable threshold should be 60%. We discovered that the proposed framework is advantageous in terms of security, availability, and adaptability. We are using the system to authenticate online examinations in Thailand during the COVID-19 pandemic.

(Total 215 pages)

Keywords: Biometrics, Authentication, Cloud Computing

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

มหาวิทยาลัยรังสิต Rangsit University

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	4
	1.3 คำถามการวิจัย / สมมติฐานการวิจัย	4
	1.4 กรอบแนวคิดการวิจัย	5
	1.5 นิยามศัพท์	10
บทที่ 2	**ทบทวนวรรณกรรมที่เกี่ยวข้อง / ทฤษฎีที่เกี่ยวข้อง**	**12**
	2.1 การประมวลผลแบบคลาวด์ (Cloud Computing)	12
	2.2 การพิสูจน์ตัวจริง (Authentication)	27
	2.3 คอมพิวเตอร์วิทัศน์ (Computer Vision)	53
	2.4 ทบทวนวรรณกรรม	62
บทที่ 3	**ระเบียบวิธีการวิจัย**	**83**
	3.1 กรอบงานที่นำเสนอ (Proposed Framework)	83
	3.2 การออกแบบและพัฒนาระบบ	91
	3.3 ประชากรและกลุ่มตัวอย่าง	100
	3.4 เครื่องมือที่ใช้ในการวิจัย	101

มหาวิทยาลัยรังสิต Rangsit University

สารบัญ (ต่อ)

		หน้า
	3.5 การเก็บรวบรวมข้อมูล	102
	3.6 การวิเคราะห์ข้อมูล	102
บทที่ 4	**ผลการวิจัย**	**106**
	4.1 ผลการพัฒนาระบบ	106
	4.2 ผลการวิเคราะห์ค่าสถิติไคสแควร์	113
	4.3 ผลการวิจัย	117
บทที่ 5	**สรุปผลและข้อเสนอแนะ**	**123**
	5.1 สรุปผลการวิจัย	123
	5.2 ข้อเสนอแนะ	127
บรรณานุกรม		**130**
ภาคผนวก		**139**
ภาคผนวก ก	บทความที่ตีพิมพ์เผยแพร่ในวารสารวิชาการ Advances in Intelligent Systems and Computing ฐานข้อมูล Scopus Q3	140
ภาคผนวก ข	บทความที่ตีพิมพ์เผยแพร่ในวารสารวิชาการ TEM Journal ฐานข้อมูล Scopus Q3	155
ภาคผนวก ค	บทความที่ตีพิมพ์เผยแพร่ในวารสารวิชาการ International Journal of Information Technology and Web Engineering ฐานข้อมูล Scopus Q3	168
ภาคผนวก ง	บทความที่รอตีพิมพ์เผยแพร่ในวารสารวิชาการ ICIC Express Letters ฐานข้อมูล Scopus Q3	205
ประวัติผู้วิจัย		**215**

มหาวิทยาลัยรังสิต Rangsit University

สารบัญตาราง

หน้า

ตารางที่

2.1	ตารางแสดงชนิดของไฮเปอร์ไวเซอร์	23
2.2	ตารางแสดงคุณสมบัติการเพิ่มประสิทธิภาพใน OpenCV	59
2.3	ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม	63
3.1	ตารางข้อมูลผู้เรียน (Students)	93
3.2	ตารางข้อมูลอาจารย์ (Instructors)	94
3.3	ตารางข้อมูลผู้ดูแลระบบ (Administrators)	95
3.4	ตารางข้อมูลวิชา (Courses)	97
3.5	ตารางข้อมูลวิชาที่ผู้เรียนลงทะเบียน (Courses_Students)	97
3.6	ตารางข้อมูลการสอบ (Examinations)	98
3.7	ตารางข้อมูลการสอบของผู้เรียน (Exam_Students)	98
3.8	ตารางข้อมูลการเข้าสู่ระบบ (Authen_Log)	98
4.1	ตารางคอนฟิวชันเมทริกส์ (Confusion Matrix) สำหรับการทดสอบสถิติไคสแควร์	114
4.2	ตารางคอนฟิวชันเมทริกส์ (Confusion Matrix)	117
4.3	ตารางแสดงค่าสถิติจากการทดลอง	118
4.4	ตารางแสดงค่าสถิติจากการทดลองชีวมิติแบบมัลติโมดัล	120

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป

หน้า

รูปที่

1.1	ภาพรวมกรอบงานที่นำเสนอ	6
1.2	ระยะของการพิสูจน์ตัวตนโดยใช้ชีวมิติ	7
2.1	ภาพแสดงการคำนวณแบบคลาวด์	12
2.2	นิยามการคำนวณแบบคลาวด์ของ NIST	14
2.3	แบบจำลองการให้บริการการคำนวณแบบคลาวด์	17
2.4	รูปแบบการใช้งานการคำนวณแบบคลาวด์	20
2.5	แผนภาพระบบชีวมิติ (Biometric System Diagram)	28
2.6	กระบวนการรู้จำโดยใช้ใบหน้า	32
2.7	กระบวน Haar-like Feature ในการตรวจจับใบหน้า	34
2.8	แสดงตัวอย่างของ Haar-like Feature ในการตรวจหาใบหน้า	35
2.9	แสดงกระบวนการ Haar-cascade	36
2.10	แสดงการผสมผสานคุณสมบัติของ Haar-like Features	36
2.11	แสดงฮิสโตแกรมของการไล่ระดับสี (Histogram of Oriented Gradients)	37
2.12	รูปแสดงคุณลักษณะเด่นของภาพใบหน้า	39
2.13	แสดงขั้นตอนวิธีการรู้จำภาพใบหน้า	40
2.14	แสดงขั้นตอนวิธีการรู้จำภาพใบหน้าแบบ LBP	41
2.15	แสดงกระบวนการรู้จำเสียง	43
2.16	แผนภาพกระบวนการ MFCC	46
2.17	กระบวนการคัดแยกคุณลักษณะเด่นของ MFCC	47
2.18	การรวมชีวมิติ (Biometric Fusion)	51
2.19	การหาค่ารวมชีวมิติแบบ Score Fusion	52
2.20	มุมมองเชิงบริบทสำหรับ OpenCV	55
2.21	การขึ้นต่อกันระหว่างโมดูลของ OpenCV	57
2.22	มุมมองการนำไปใช้งานของ OpenCV	58
2.23	รูปแสดงประสิทธิภาพที่เพิ่มขึ้นจากการใช้ CUDA	61
3.1	ภาพรวมกรอบงานที่นำเสนอ	84

มหาวิทยาลัยรังสิต Rangsit University

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.2	เฟสของการพิสูจน์ตัวตนโดยใช้ชีวมิติ	84
3.3	เฟสการลงทะเบียนข้อมูล (Registration Phase)	85
3.4	เฟสการเรียนรู้ของเครื่อง (Training Phase)	89
3.5	เฟสการพิสูจน์ตัวตน (Authentication Phase)	90
3.6	แผนภาพการใช้งานผู้ใช้ (Use Case Diagram)	91
3.7	แผนภาพแสดงความสัมพันธ์ของเอนทิตี้ (E-R Diagram)	92
3.8	แผนภาพการทำงานของระบบ (Flow Diagram)	99
4.1	สถาปัตยกรรมดอกเกอร์คอนเทนเนอร์ (Docker Container)	107
4.2	หน้าจอ Proxmox Virtual-Environment 6.4-6	108
4.3	หน้าจอโฮมเพจของระบบการพิสูจน์ตัวตนด้วยชีวมิติ	110
4.4	หน้าจอแสดงขั้นตอนการป้อนข้อมูลของกระบวนการลงทะเบียน (Registration Process)	110
4.5	หน้าจอแสดงการถ่ายภาพใบหน้าของผู้เรียนในขั้นตอนการลงทะเบียน (Facial Enrollment)	111
4.6	หน้าจอแสดงปุ่มล็อกอินเมื่อผู้ใช้ลงทะเบียนเรียบร้อยแล้ว	111
4.7	หน้าจอแสดงผลการพิสูจน์ตัวตนเพื่อล็อกอินเข้าสู่ระบบ	111
4.8	หน้าจอแสดงการจัดการวิชา (Course Management)	112
4.9	หน้าจอแสดงการจัดการการสอบออนไลน์ (Examination Management)	113
4.10	กราฟแสดงพื้นที่บริเวณวิกฤต	116
4.11	กราฟแสดงค่าจากตารางคอนฟิวชันเมทริกส์	118
4.12	กราฟแสดงค่าสถิติจากการทดลอง	118
4.13	กราฟแสดงค่าสถิติจากการทดลองชีวมิติแบบมัลติโมดัล	121
4.14	กราฟแสดงค่าสถิติจำนวนภาพใบหน้า ความยาวเสียงและเวลาประมวลผล	122

มหาวิทยาลัยราชภัฏรำไพพรรณี Rajabhat Rajapruk University

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

แนวโน้มการประมวลผลแบบคลาวด์ มีการคาดการณ์ว่าจะมีมูลค่าประมาณ 250 พันล้านเหรียญสหรัฐอเมริกา ในปี ค.ศ. 2017 (Gartner, 2013) ส่วนในปี ค.ศ. 2016 มีการคาดการณ์ว่าหนึ่งในสี่ของซอฟต์แวร์ที่ใช้การกันโดยทั่วไปจะสามารถเข้าใช้ได้โดยใช้บริการประมวลผลแบบคลาวด์ ส่วนมูลค่าทางการตลาดของ Service as a Service (SaaS) ที่มีมูลค่าในปี ค.ศ. 2012 ที่ 18.2 พันล้านเหรียญสหรัฐอเมริกา จะมีมูลค่าเพิ่มขึ้นเป็น 45.6 พันล้านเหรียญสหรัฐอเมริกาในปี ค.ศ. 2017 และมีการคาดการณ์ว่าองค์กรธุรกิจขนาดใหญ่ร้อยละ 58 มีการใช้งบประมาณประจำปีมากกว่าร้อยละ 10 บนบริการประมวลผลแบบคลาวด์ (Everest Group, 2014) จะเห็นได้ว่ามีการคาดการณ์แนวโน้มการใช้การประมวลผลแบบคลาวด์ เพิ่มขึ้นอย่างต่อเนื่องของการประมวลผลแบบคลาวด์ ในต่างประเทศ

สำหรับสภาพการณ์การประมวลผลแบบคลาวด์ ในประเทศไทยนั้นจากรายงานการสำรวจดัชนีคลาวด์ ของวีเอ็มแวร์จัดทำโดย Forrester ประจำปี 2555 (VMWare Cloud Index, 2012) พบว่าอัตราการปรับใช้เทคโนโลยีคลาวด์ ในประเทศไทยมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยร้อยละ 83 ของผู้ตอบแบบสอบถามได้ปรับใช้วิธีแก้ปัญหา (Solution) โดยใช้การประมวลผลแบบคลาวด์แล้ว หรือมีแผนที่จะปรับมาใช้การประมวลผลแบบคลาวด์ ส่วนองค์กรที่ยังไม่ได้ติดตั้งวิธีแก้ปัญหาประมวลผลแบบคลาวด์ เกือบร้อยละ 48 มีแผนที่จะจะปรับมาใช้ในช่วง 18 เดือนข้างหน้า ผู้ตอบแบบสอบถามในประเทศไทยร้อยละ 83 มีความคิดเห็นตรงกันว่าการประมวลผลแบบคลาวด์ จะช่วยให้องค์กรสามารถแข่งขันในตลาดได้อย่างมีประสิทธิภาพมากขึ้น และร้อยละ 68 มีความเห็นว่าหากบริษัทของตนไม่ได้ดำเนินโครงการใช้วิธีแก้ปัญหาการประมวลผลแบบคลาวด์ ก็จะไม่สามารถก้าวตามคู่แข่งได้ทัน

ในส่วนของภาครัฐบาลก็ได้ให้ความสำคัญต่อการประมวลผลแบบคลาวด์ ด้วยเช่นกัน โดยเฉพาะการสนับสนุนนโยบายเศรษฐกิจดิจิทัล โดยมีการก่อตั้งโครงการบริการคลาวด์ ภาครัฐ

มหาวิทยาลัยรังสิต Rangsit University

(Government Cloud Service) ภายใต้สำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ) (องค์การมหาชน) มีภารกิจหลัก 4 ประการคือ 1) เพื่อศึกษาแนวทางในการให้บริการประมวลผลแบบคลาวด์แก่หน่วยงานภาครัฐ และพัฒนาไปสู่การให้บริการ 2) เพื่อเป็นแนวทางในการให้บริการโครงสร้างพื้นฐานหลักสำหรับระบบและข้อมูลสารสนเทศของหน่วยงานภาครัฐ 3) เพื่อศึกษาการลดความซ้ำซ้อนของงบประมาณภาครัฐในด้านเทคโนโลยีสารสนเทศ และเพิ่มประสิทธิภาพในการพัฒนาระบบเพื่อให้บริการประชาชนแก่หน่วยงานภาครัฐ ที่ร่วมโครงการและ 4) เพื่อพัฒนาประเทศไทยให้พร้อมสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ที่ทัดเทียมกับนานาประเทศ โดยให้ข้อมูลสนับสนุนว่าผลการสำรวจตลาดเทคโนโลยีสารสนเทศในประเทศไทย มีอัตราการขยายตัวในปี 2554 ที่ร้อยละ 15.60 โดยคิดเป็นมูลค่าทางการตลาด 293,239 ล้านบาท และหากพิจารณาค่าใช้จ่ายจำแนกตามภาคผู้ใช้งานจะพบว่าภาครัฐมีการใช้จ่ายด้านเทคโนโลยีสารสนเทศคิดเป็นประมาณร้อยละ 20.4 หรือ 59,818 ล้านบาท เมื่อพิจารณาในส่วนของบริการด้านศูนย์ข้อมูลคอมพิวเตอร์และศูนย์การฟื้นฟูจากภัยพิบัติ (Data Center and Disaster Recovery Center) พบว่าภาพรวมมีมูลค่าทางการตลาดในปี 2554 เท่ากับ 6,903 ล้านบาท โดยภาครัฐมีการใช้จ่ายในส่วนนี้ถึง 2,567 ล้านบาท หรือคิดเป็นสัดส่วนร้อยละ 38.5 โดยปัจจุบันคาดการณ์ว่ามูลค่าการใช้บริการประมวลผลแบบคลาวด์ และ SaaS ในประเทศไทยจะคิดเป็นประมาณ 2,089 ล้านบาท และมีแนวโน้มเติบโตเพิ่มขึ้นร้อยละ 22.9 โดยเป็นกลุ่มผู้ใช้งานรัฐและเอกชนถึงร้อยละ 71.3 หรือ 180,821 ล้านบาท (โครงการบริการคลาวด์ภาครัฐ, 2558)

จากรายงานของ International Data Corporation (IDC) พบว่าในไตรมาสที่ 2 ปี ค.ศ. 2015 มีจำนวนการส่งมอบเครื่องสมาร์ตโฟนจำนวน 341.5 ล้านเครื่อง มีอัตราเพิ่มขึ้นร้อยละ 13 เมื่อเทียบกับปีที่โดยใช้มาแม้ว่าจะน้อยกว่าที่คาดการณ์ไว้ โดยมีเครื่องที่ใช้ระบบปฏิบัติการแอนดรอยด์ร้อยละ 82.8 และซัมซุงเป็นบริษัทที่ยังคงครองส่วนแบ่งทางการตลาดลำดับที่ 1 ที่ร้อยละ 21.4 ส่วนแอปเปิลมีส่วนแบ่งทางการตลาดลำดับที่ 2 ที่ร้อยละ 13.9 คิดเป็นประมาณ 47.5 ล้านเครื่อง จะเห็นได้ว่าแนวโน้มการเติบโตของสมาร์ตโฟนยังคงมีอัตราที่เพิ่มมากขึ้นแสดงให้เห็นว่าจำนวนผู้ใช้สมาร์ตโฟนมีแนวโน้มสูงขึ้น IDC คาดการณ์ว่าผลิตภัณฑ์ของแอปเปิลน่าจะมีแนวโน้มการขยายตัวที่ดีในครึ่งปีหลังเนื่องจากมีผลิตภัณฑ์ออกมาใหม่เช่น ไอโฟน 6 และในประเทศจีนซึ่งมีประชากรจำนวนมาก มีการปรับใช้เครือข่าย 4G เพิ่มมากขึ้น ส่วนในปี ค.ศ. 2014 IDC ได้คาดการณ์ว่าบริษัทแอปเปิลจะมีการส่งมอบอุปกรณ์จำนวนกว่า 184.1 ล้านเครื่องมูลค่ากว่า 116,540 ล้านเหรียญสหรัฐอเมริกา และในปี ค.ศ. 2018 คาดการณ์ว่าบริษัทแอปเปิลจะมีการส่งมอบอุปกรณ์จำนวนกว่า 247.4 ล้านเครื่อง

มหาวิทยาลัยรังสิต Rangsit University

โดยทั่วไปการพิสูจน์ตัวจริงที่นิยมในการเข้าใช้งานระบบสารสนเทศคือการใช้ชื่อบัญชีผู้ใช้และรหัสผ่าน (Balfanz et al., 2012) เนื่องจากเป็นวิธีการที่ง่ายไม่ซับซ้อนสำหรับทั้งผู้ใช้บริการและผู้ให้บริการ อย่างไรก็ตามวิธีการนี้มีประเด็นปัญหาหลายด้านทั้งฝั่งผู้ใช้บริการและผู้ให้บริการ กล่าวคือปัจจุบันแอปพลิเคชันหรือระบบสารสนเทศมีจำนวนเพิ่มขึ้นอย่างมากมาย ผู้ใช้บริการจำเป็นต้องมีชื่อบัญชีผู้ใช้และรหัสผ่านโดยใช้สำหรับทุกระบบทำให้ยากต่อการจดจำ การที่ผู้ใช้บริการจะจดไว้ในเอกสารหรือไฟล์ข้อมูลในคอมพิวเตอร์ก็มีความเสี่ยงต่อการถูกโจรกรรมข้อมูลชื่อบัญชีผู้ใช้และรหัสผ่านโดยใช้ได้ ส่วนด้านผู้ให้บริการที่ต้องมีการจัดเก็บข้อมูลรายชื่อบัญชีผู้ใช้และรหัสผ่านโดยใช้ของผู้ใช้ทุกคนในระบบ จึงต้องมีวิธีการในการป้องกันการเข้าโจรกรรมหรือการเข้ารหัสข้อมูลชื่อบัญชีผู้ใช้และรหัสผ่านโดยใช้อย่างแข็งแกร่ง ซึ่งปัจจุบันพบว่ามีการโจรกรรมข้อมูลโดยใช้เครือข่ายอินเทอร์เน็ตบ่อยมากขึ้นและในบางกรณีมีความเสียหายในวงกว้างจำนวนมหาศาล ตัวอย่างเช่น ประเทศเกาหลีใต้มีเหตุการณ์โจรกรรมข้อมูลบัตรเครดิตของบริษัทชั้นนำ 3 แห่งในประเทศ ข้อมูลบัตรเครดิตของชาวเกาหลีกว่า 20 ล้านคนซึ่งเชื่อมโยงกับบัตรเครดิต 80 ล้านใบ อีกทั้งยังทำลายความน่าเชื่อถือของการป้องกันความปลอดภัยของข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในองค์กรขนาดใหญ่เช่น ระบบธนาคารเป็นต้น

แนวทางหนึ่งที่สามารถนำมาประยุกต์ใช้แทนการการพิสูจน์ตัวจริงที่ใช้ชื่อบัญชีผู้ใช้และรหัสผ่านโดยใช้คือการพิสูจน์ตัวจริงโดยใช้ชีวมิติ ซึ่งเป็นเทคนิคในการตรวจสอบความสมเหตุสมผลของผู้ใช้บริการโดยใช้ลักษณะทางกายภาพหรือพฤติกรรมการแสดงออก ในปัจจุบันมีการประยุกต์เพื่อใช้งานเพิ่มมากขึ้นโดยเฉพาะการใช้งานในองค์กรต่าง ๆ เช่น การใช้การตรวจหาลายนิ้วมือเป็นต้น แต่การประยุกต์ใช้กับระบบสารสนเทศบนเครือข่ายอินเทอร์เน็ตยังมีไม่มากนัก เทคโนโลยีของชีวมิติมีการนำไปประยุกต์ใช้กับกระบวนการทางกฎหมายหรือการบังคับใช้กฎหมายมานานแล้ว ตัวอย่างเช่น ฐานข้อมูลชีวมิติหน่วยงานสืบสวนกลาง กระทรวงกลาโหมประเทศสหรัฐอเมริกา (Kohlwaey, Sussman, Trost, & Maurer, 2011) ที่นำไปใช้ทางด้านความมั่นคงของประเทศ มีการคาดการณ์ว่าในอีกไม่กี่ปีข้างหน้าจะมีสารสนเทศด้านชีวมิติเพื่อใช้ในการตรวจสอบจะมีจำนวนหลายร้อยจนถึงหลายพันล้านข้อมูลบุคคลจึงจำเป็นต้องมีการพิจารณาถึงเทคโนโลยีที่จำเป็นต้องนำมาใช้ในการจัดการกับข้อมูลจำนวนมหาศาล และมีแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง อีกทั้งต้องการสมรรถนะการประมวลผลของคอมพิวเตอร์เพิ่มขึ้นอย่างมากด้วย

แนวทางหนึ่งที่สามารถจะนำมาประยุกต์ใช้คือการประยุกต์ใช้การพิสูจน์ตัวจริงโดยใช้ชีวมิติกับแพลตฟอร์มของการประมวลผลแบบคลาวด์ โดยที่การประมวลผลแบบคลาวด์นั้น

มหาวิทยาลัยรังสิต Rangsit University

สามารถช่วยแก้ปัญหาทางด้านความยืดหยุ่นในการขยายระบบสารสนเทศได้อย่างพลวัต การขยายความจุของหน่วยเก็บสำรองข้อมูลเพื่อรองรับปริมาณของข้อมูลชีวมิติที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง หรือขยายความสามารถของการประมวลผลแบบขนานเพื่อเพิ่มสมรรถนะการประมวลผลให้เพิ่มขึ้น นอกจากนี้ยังสามารถประยุกต์เพื่อใช้งานกับร่วมกับอุปกรณ์เคลื่อนที่หรือเครื่องคอมพิวเตอร์ทั่วไป ผู้ใช้บริการสามารถเข้าถึงระบบสารสนเทศจากสถานที่ต่าง ๆ ได้อย่างสะดวกมากขึ้น การศึกษาการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์โดยใช้อุปกรณ์เคลื่อนที่หรือเครื่องคอมพิวเตอร์ทั่วไปจึงมีความจำเป็นในปัจจุบัน ผู้วิจัยจึงตระหนักถึงความสำคัญและมีความประสงค์ในการศึกษาการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

1.2 วัตถุประสงค์การวิจัย

1.2.1 เพื่อออกแบบโครงร่างกรอบแนวคิดระบบการพิสูจน์ตัวจริงเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้ชีวมิติที่ใช้ใบหน้าและชีวมิติชนิดอื่น

1.2.2 เพื่อนำเสนอกระบวนการออกแบบระบบโครงร่างกรอบแนวคิดมาพัฒนาระบบ

1.2.3 เพื่อนำเสนอการออกแบบระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

1.2.4 เพื่อพัฒนาระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ต้นแบบจากโครงร่างกรอบแนวคิด

1.2.5 เพื่อประเมินผลระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ต้นแบบจากผู้ใช้

มหาวิทยาลัยรังสิต Rangsit University

1.3 คำถามการวิจัย / สมมติฐานการวิจัย

การวิจัยนี้มีการตั้งสมมติฐานไว้ดังนี้

สมมติฐาน H0: ไม่มีชีวมิติอื่นที่ใช้ร่วมกับชีวมิติที่ใช้ใบหน้าที่ช่วยให้มีอัตราการผิดพลาดของการรู้จำลดลง

สมมติฐาน H1: มีชีวมิติอื่นที่ใช้ร่วมกับชีวมิติที่ใช้ใบหน้าที่ช่วยให้มีอัตราการผิดพลาดของการรู้จำลดลง

สมมติฐาน H2: ไม่มีคุณลักษณะของชีวมิติอื่นที่จะนำมาใช้ร่วมกับชีวมิติที่ใช้ใบหน้าเพื่อใช้ในการพิสูจน์ตัวจริงในการเข้าใช้บริการประมวลผลแบบคลาวด์

สมมติฐาน H3: มีคุณลักษณะของชีวมิติอื่นที่จะนำมาใช้ร่วมกับชีวมิติที่ใช้ใบหน้าเพื่อใช้ในการพิสูจน์ตัวจริงในการเข้าใช้บริการประมวลผลแบบคลาวด์

สมมติฐาน H4: ไม่สามารถหาค่าความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ของระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติอื่นร่วมกับชีวมิติที่ใช้ใบหน้าได้

สมมติฐาน H5: สามารถหาค่าความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ของระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติอื่นร่วมกับชีวมิติที่ใช้ใบหน้าได้

การวิจัยนี้มีคำถามการวิจัย 3 ข้อคำถาม ดังนี้

1) ระบบการพิสูจน์ตัวจริงเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้ชีวมิติที่ใช้ใบหน้าเพียงอย่างเดียวให้มีอัตราการผิดพลาดลดลงได้อย่างไร

2) ชีวมิติที่จะนำมาใช้เพื่อการพิสูจน์ตัวจริงเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ร่วมกับระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติที่ใช้ใบหน้ามีคุณลักษณะอย่างไร

3) ชีวมิติที่จะนำมาใช้เพื่อการพิสูจน์ตัวจริงร่วมกับระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติที่ใช้ใบหน้า (Fusion Biometric) ควรกำหนดหาค่าความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่เท่าไร

มหาวิทยาลัยรังสิต Rangsit University

1.4 กรอบแนวคิดการวิจัย

การศึกษานี้เป็นการศึกษาระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ โดยใช้กระบวนการวิจัยเชิงพัฒนา และเป็นการวิจัยเชิงทดลอง โดยมีภาพรวมของระบบดังรูปที่ 1.1 ระบบโดยรวมแบ่งได้เป็น 3 ระดับชั้นคือ ระดับแอปพลิเคชันบนเครื่องคอมพิวเตอร์ของผู้ใช้ ระดับแอปพลิเคชันของระบบการพิสูจน์ตัวจริง และระดับฐานข้อมูล

ระดับแอปพลิเคชัน (Client Layer) บนเครื่องคอมพิวเตอร์ของผู้ใช้ จะไม่มีการติดตั้งแอปพลิเคชันไว้ที่ฝั่งผู้ใช้ เนื่องจากโปรแกรมจะทำงานที่ฝั่งเครื่องให้บริการ ผู้ใช้สามารถเข้าถึง

ระบบได้จากการใช้โปรแกรมเว็บเบราเซอร์เพื่อป้อนข้อมูลส่วนบุคคลได้แก่ ชื่อบัญชีผู้ใช้ รหัสผ่าน อีเมล ภาพใบหน้า เสียงพูด และอื่น ๆ แล้วนำเข้าสู่ระบบและแสดงผลลัพธ์จากการพิสูจน์ตัวจริง

ระดับแอปพลิเคชันของระบบการพิสูจน์ตัวจริง (Application Layer) เป็นส่วนของแอปพลิเคชันที่ติดตั้งไว้ที่เครื่องให้บริการ (Server) บนการประมวลผลแบบคลาวด์ ทำหน้าที่คัดกรองข้อมูลก่อนการประมวลผล การคัดแยกคุณลักษณะเด่นที่ต้องการ หรือการสร้างแบบจำลอง แล้วจัดเก็บไว้ในระบบฐานข้อมูล เพื่อใช้ในการเปรียบเทียบของการพิสูจน์ตัวจริง

ระดับฐานข้อมูล (Database Layer) ทำหน้าที่บริการจัดการกับข้อมูลชีวมิติทั้งการเพิ่ม การลบ การแก้ไข หรือการสืบค้นข้อมูล เป็นต้น โดยข้อมูลจะถูกจัดเก็บไว้ที่หน่วยจัดเก็บข้อมูลที่อยู่บนการประมวลผลแบบคลาวด์ (Cloud Storage)

รูปที่ 1.1 ภาพรวมกรอบงานที่นำเสนอ

การพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ โดยใช้เครื่องคอมพิวเตอร์สามารถแบ่งเป็น 3 เฟสดังรูปที่ 1.2 ดังนี้

รูปที่ 1.2 เฟสของการพิสูจน์ตัวจริงโดยใช้ชีวมิติ

ที่มา: Rukhiran, Pukdesree, & Netinant, 2022

1) เฟสการลงทะเบียนข้อมูล (Registration Phase)

ขั้นตอนนี้เป็นขั้นตอนในการเก็บรวบรวมข้อมูลของผู้ใช้ผ่านกระบวนการลงทะเบียน ผู้ใช้จะป้อนข้อมูลพื้นฐานส่วนบุคคลและข้อมูลชีวมิติ ข้อมูลชีวมิติทั้งสองแบบคือภาพใบหน้าและข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท

1.1) ขั้นที่ 1 การรับข้อมูล (Capturing) ผู้ใช้ที่ต้องการลงทะเบียนทำการป้อนข้อมูลส่วนบุคคล เช่น ชื่อบัญชีผู้ใช้ รหัสโดยใช้ อีเมล และข้อมูลชีวมิติได้แก่ภาพใบหน้าและข้อมูลเสียงโดยใช้เว็บแอปพลิเคชันที่ได้พัฒนาขึ้นสามารถเข้าใช้งานได้จากอุปกรณ์หลายชนิด

1.2) ขั้นที่ 2 การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) ข้อมูลที่ชีวมิติที่รับเข้ามาจำเป็นต้องมีการแยกคุณลักษณะเด่นที่ต้องการไว้ ส่วนข้อมูลใดที่ไม่จำเป็นก็จะทำการนำออกไป ตัวอย่างเช่น ภาพหน้าคน ก็จะทำการตัดเฉพาะส่วนที่เป็นใบหน้าเท่านั้นที่จะมีผลต่อการพิสูจน์

ตัวจริง ส่วนผมหรือส่วนอื่น ๆ ก็จะถูกตัดออกไป ข้อมูลชีวมิติทั้งสองแบบคือภาพใบหน้าและข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท

การเตรียมข้อมูลภาพใบหน้าก่อนการประมวลผล (Face Preprocessing) ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การตรวจหาบริเวณดวงตาซึ่งมักเป็นบริเวณที่มีสีเข้มกว่าบริเวณอื่นโดยใช้ขั้นตอนวิธี Haar-cascade และจะมีการปรับขนาด (Scaling) การหมุนภาพ (Rotating) และการแปลงภาพ (Translating) นอกจากนี้จะทำการตัดส่วนของภาพให้เหลือเฉพาะบริเวณใบหน้าเท่านั้นส่วนประกอบอื่นเช่น หน้าผาก คาง ใบหู และภาพพื้นหลังอื่น ๆ ออก ขั้นที่ 2 การใช้เทคนิคฮิสโตแกรม (Histogram of Oriented Gradients) ในการเพิ่มคุณภาพของภาพต้นฉบับโดยการจัดวางตำแหน่งภาพ การปรับความสว่างและความคมชัดให้ด้านซ้ายและด้านขวาของภาพใบหน้า ขั้นที่ 3 การทำเครื่องหมายรูปวงรีเพื่อเป็นการเน้นภาพใบหน้า และจะกำจัดผมและพื้นหลังบางส่วนออกจากภาพใบหน้า ผลลัพธ์ที่ได้คือเฉพาะในรูปภาพใบหน้าเท่านั้น

การเตรียมข้อมูลเสียงก่อนการประมวลผล (Voice Preprocessing) เป็นกระบวนการย่อยของกระบวนการการคัดแยกคุณลักษณะเด่น โดยจะมีการปรับความสมดุลความถี่ของเสียงที่รับมาจากอุปกรณ์ไมโครโฟนให้อยู่ในระดับสัญญาณเสียงที่หูของมนุษย์สามารถรับรู้ได้อย่างเหมาะสม

1.3) การคัดแยกคุณลักษณะเด่น (Feature Extraction) เป็นนำผลลัพธ์ที่ได้จากขั้นตอนก่อนหน้านี้ทั้งส่วนของข้อมูลชีวมิติภาพใบหน้ามาทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองเฉพาะส่วนของตำแหน่ง หรือขนาดของอวัยวะ เช่น ตา จมูก หรือปาก การวิจัยนี้ใช้ขั้นตอนวิธี LBPH (Local Binary Pattern Histogram) ส่วนข้อมูลชีวมิติเสียงจะมาทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองคือเวกเตอร์ของเสียง Mel-frequency Cepstral Coefficients (MFCCs) ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การคัดแยกคุณลักษณะเด่นของข้อมูลเสียง (MFCC Extraction) ขั้นตอนวิธี MFCC จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติ ขั้นที่ 2 การคำนวณค่าเดลตา (Delta) จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติเช่นกัน ดังนั้นเมื่อรวมกันทั้งเวกเตอร์ของเสียงจาก MFCC กับเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติจาก Delta จะได้เวกเตอร์ของเสียงที่มีคุณลักษณะจำนวน 40 มิติ ขั้นที่ 3 ข้อมูลชีวมิติเสียงจะถูกคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์คือ เทมเพลตของชีวมิติเสียง

มหาวิทยาลัยรังสิต Rangsit University

1.4) การจัดเก็บลงในฐานข้อมูล (Storing in Database) เป็นการนำเทมเพลตหรือแบบจำลองไปจัดเก็บไว้ในฐานข้อมูลซึ่งอยู่บนระบบการประมวลผลแบบคลาวด์ เพื่อนำไปใช้ในขั้นตอนถัดไป

2) เฟสการเรียนรู้ของเครื่อง (Training Phase)

เป็นขั้นตอนที่นำเอาข้อมูลที่ได้จากการแยกคุณลักษณะเด่นที่ต้องการ (Feature Extraction) ของแต่ละบุคคลมาเป็นข้อมูลเพื่อสอนให้คอมพิวเตอร์เรียนรู้ด้วยตนเองว่าลักษณะของโครงสร้างรูปภาพใบหน้าของแต่ละคนมีคุณลักษณะอย่างไร เช่น ระยะห่างของตำแหน่งต่าง ๆ ของอวัยวะบนใบหน้า หรือตำแหน่งของอวัยวะต่าง ๆ บนในหน้า เป็นต้น รวมทั้งคุณลักษณะเด่นของเสียงของแต่ละบุคคลด้วยเช่นกัน สำหรับการเรียนรู้ภาพใบหน้า (Facial Training) จะเป็นการนำเอาคุณลักษณะเด่นของภาพใบหน้าที่ได้มาจากเฟสที่ 1 มาสอนให้คอมพิวเตอร์เรียนรู้แล้วทำการสร้างเป็นโมเดลสำหรับการเรียนรู้เสียง (Voice Training) การวิจัยนี้ใช้ขั้นตอนวิธีแบบจำลองส่วนผสมเกาส์เซียน (Gaussian Mixture Model) ซึ่งผลลัพธ์จากขั้นตอนการเรียนรู้ของเครื่องคอมพิวเตอร์นี้จะได้แบบจำลองหรือโมเดลสำหรับการเรียนรู้ของเครื่องคอมพิวเตอร์

3) เฟสการพิสูจน์ตัวจริง (Authentication Phase)

กระบวนการรู้จำเป็นกระบวนการที่สามารถใช้เพื่อยืนยันตัวตนหรือการตรวจสอบตัวบุคคลโดยการใช้ข้อมูลชีวมิติ เช่น คุณลักษณะเด่นของใบหน้าหรือเสียงเปรียบเทียบกับคุณลักษณะเด่นของใบหน้าหรือเสียงที่จัดเก็บไว้ในฐานข้อมูล สำหรับการบวนการการรู้จำภาพใบหน้าการวิจัยนี้ใช้ เทคนิค LBPH (Local Binary Pattern Histogram) สำหรับการรู้จำเสียงการวิจัยนี้ใช้การแจกแจงความน่าจะเป็นแบบผสมตามขั้นตอนวิธี MFCC ผลคะแนนที่ได้จากการเปรียบเทียบของชีวมิติทั้งสองแบบจะนำคะแนนมารวมกันเพื่อใช้กำหนดว่าการพิสูจน์ตัวจริงผ่านหรือไม่โดยผู้วิจัยกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่ร้อยละ 60 เนื่องจากผลการทดลองเชิงประจักษ์จากการวิจัยนี้พบว่า การใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันในการพิสูจน์ตัวจริงเพื่อเข้าใช้การบริการประมวลผลแบบคลาวด์มีค่าอยู่ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบในการพิสูจน์ตัวจริงโดยใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันเพื่อใช้บริการบนการประมวลผลแบบคลาวด์ได้ในอัตราร้อยละ 60

มหาวิทยาลัยรังสิต Rangsit University

1.5 นิยามศัพท์

การประมวลผลแบบคลาวด์ (Cloud Computing) หมายถึง รูปแบบหนึ่งของการใช้ทรัพยากรของการคำนวณที่มีการรวบรวมไว้ โดยใช้ระบบเครือข่ายโดยที่ผู้ใช้เข้าไปบริหารจัดการระบบหรือมีปฏิสัมพันธ์กับผู้ให้บริการน้อยมาก

ประชากร (Population) หมายถึง สมาชิกทุกหน่วยของสิ่งที่สนใจศึกษา ประชากรอาจจะเป็นอาจเป็นได้ทั้ง ตัวบุคคล สิ่งของ เวลา หรือสถานที่ เป็นต้น

กลุ่มตัวอย่าง (Sample) หมายถึง ส่วนหนึ่งของประชากรที่นำมาศึกษาซึ่งเป็นตัวแทนของประชากร การที่กลุ่มตัวอย่างจะเป็นตัวแทนที่ดีของประชากรเพื่อการอ้างอิงไปยังประชากรอย่างน่าเชื่อถือได้นั้น จะต้องมีการเลือกตัวอย่างและขนาดตัวอย่างที่เหมาะสม ซึ่งจะต้องอาศัยสถิติเข้ามาช่วยในการสุ่มตัวอย่างและการกำหนดขนาดของกลุ่มตัวอย่าง

การสุ่มตัวอย่าง (Sampling) หมายถึง กระบวนการได้มาซึ่งกลุ่มตัวอย่างที่มีความเป็นตัวแทนที่ดีของประชากร

การให้บริการซอฟต์แวร์บนการประมวลผลแบบคลาวด์ (Software as a Service -SaaS) หมายถึง การให้บริการซอฟต์แวร์แก่ผู้ใช้บริการบนการประมวลผลแบบคลาวด์โดยใช้โครงสร้างพื้นฐานของผู้ให้บริการ

การให้บริการโครงสร้างพื้นฐานบนการประมวลผลแบบคลาวด์ (Infrastructure as a Service - IaaS) หมายถึง เป็นการให้บริการโครงสร้างพื้นฐาน หรือทรัพยากรอื่น ๆ ให้แก่ผู้ใช้บริการบนการประมวลผลแบบคลาวด์

การให้บริการแพลตฟอร์มบนการประมวลผลแบบคลาวด์ (Platform as a Service - PaaS) หมายถึง การให้บริการแพลตฟอร์มแก่ผู้ใช้บริการบนการประมวลผลแบบคลาวด์โดยใช้โครงสร้างพื้นฐานของผู้ให้บริการ

มหาวิทยาลัยรังสิต Rangsit University

ไพรเวทคลาวด์ (Private Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์มีไว้ให้บริการเฉพาะสมาชิกในองค์กรหรือหน่วยงานเท่านั้น

คอมมิวนิตีคลาวด์ (Community Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์มีไว้ให้บริการสำหรับสมาชิกในกลุ่มชุมชนที่มีความเห็น นโยบายหรือข้อตกลงร่วมกัน

พลับบลิคคลาวด์ (Public Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์แบบสาธารณะ ซึ่งเปิดให้ผู้ใช้งานทั่วไปสามารถเข้ามาใช้งานได้

ไฮบริดลาวด์ (Hybrid Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ประกอบด้วยการรวมโครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ตั้งแต่สองชนิดที่แตกต่างกัน เช่น ไพรเวทคลาวด์ คอมมิวนิตีคลาวด์ หรือ พลับบลิคคลาวด์

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 2

ทบทวนวรรณกรรมที่เกี่ยวข้อง / ทฤษฎีที่เกี่ยวข้อง

เนื้อหาในบทนี้ผู้วิจัยนำเสนอการทบทวนวรรณกรรมที่เกี่ยวข้อง และทฤษฎีที่เกี่ยวข้องกับการวิจัยประกอบด้วย การประมวลผลแบบคลาวด์ (Cloud Computing) กระบวนการพิสูจน์ตัวจริง (Authentication Process) เครื่องมือการประมวลผลภาพด้วย OpenCV ซึ่งเป็นไลบรารีทางซอฟต์แวร์ที่ใช้ในการประมวลผลภาพ และการทบทวนวรรณกรรม

2.1 การประมวลผลแบบคลาวด์ (Cloud Computing)

การประมวลผลแบบคลาวด์เป็นรูปแบบหนึ่งของการเข้าใช้บริการระบบคอมพิวเตอร์โดยใช้ทางระบบเครือข่าย โดยที่ผู้ใช้บริการไม่จำเป็นต้องรู้ว่าทรัพยากรของคอมพิวเตอร์ตั้งอยู่ที่ใด มีโครงสร้างพื้นฐานของระบบสารสนเทศอย่างไร ผู้ใช้บริการเพียงกำหนดความต้องการในการใช้บริการ จากนั้นบริการบนการประมวลผลแบบคลาวด์จะดำเนินการเพื่อให้ผลลัพธ์ตามที่ผู้ใช้ต้องการ ตัวอย่างเช่น บริการด้านสารสนเทศของกูเกิ้ลแอปพลิเคชัน เช่น อีเมล ไดรฟ์ ค้นหา และบริการอื่น ๆ เป็นต้น ดังรูปที่ 2.1

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 2.1 ภาพแสดงการประมวลผลแบบคลาวด์

ที่มา: Johnston, 2009

2.1.1 นิยาม/ความหมาย (Definition)

นิยามของการประมวลผลแบบคลาวด์มีหลายนิยาม เช่น

1) บริษัท Gartner กล่าวว่า ระบบการประมวลผลแบบคลาวด์คือ แนวทางการประมวลผลที่พลังของโครงสร้างทางไอทีขนาดใหญ่ที่ขยายตัวได้ถูกนำมาเสนอยังลูกค้าภายนอกจำนวนมหาศาลในรูปแบบของบริการ (Gartner, 2013)

2) ฟอเรสเตอร์กรุ๊ป กล่าวว่า การประมวลผลแบบคลาวด์คือ กลุ่มของโครงสร้างพื้นฐานที่ถูกบริหารจัดการและขยายตัวได้อย่างมาก ซึ่งมีขีดความสามารถในการรองรับโปรแกรมประยุกต์ต่าง ๆ ของผู้ใช้และเก็บค่าบริการตามการใช้งาน

3) National Institute of Standards and Technology (NIST) กล่าวว่า การประมวลผลแบบคลาวด์เป็นรูปแบบหนึ่งของการใช้ทรัพยากรของการคำนวณที่มีการรวบรวมไว้ (ตัวอย่างเช่น เครื่องให้บริการ ระบบเครือข่าย หน่วยเก็บสำรองข้อมูล แอปพลิเคชัน และบริการต่าง ๆ) โดยใช้ระบบเครือข่ายโดยที่ผู้ใช้เข้าไปบริหารจัดการระบบหรือมีปฏิสัมพันธ์กับผู้ให้บริการน้อยมาก

4) Wikipedia กล่าวว่า การประมวลผลแบบคลาวด์ หมายถึงทรัพยากรสำหรับการประมวลผลที่จัดเตรียมและจัดการโดยบุคคลหรือองค์กรที่สาม (Third Party) โดยทรัพยากรเหล่านี้ถูกจัดเตรียมไว้ที่ศูนย์บริการข้อมูลคอมพิวเตอร์ (Data Center) จากนั้น ผู้ใช้ของการประมวลผลแบบคลาวด์สามารถเข้าไปใช้งานทรัพยากรเหล่านี้โดยการซื้อ(หรือเช่า)ได้ตามที่ต้องการ โดยที่ผู้ใช้ไม่ต้องคำนึงเลยว่าทางผู้ให้บริการทรัพยากรจะ บริหารจัดการทรัพยากรอย่างไร ใช้ความสามารถขยายตัวด้วยวิธีการอะไร

ในการศึกษานี้ผู้วิจัยเน้นไปที่การให้นิยามและความหมายของ NIST ที่ได้ให้คำจำกัดความว่า การประมวลผลแบบคลาวด์มีคุณลักษณะที่สำคัญห้าส่วน มีรูปแบบการให้บริการ 3 แบบ และรูปแบบการนำไปใช้งาน 4 แบบมีรายละเอียดดังนี้

มหาวิทยาลัยรังสิต Rangsit University

2.1.2 คุณลักษณะที่สำคัญ (Importance Characteristics)

NIST ได้ให้คำนิยามคุณลักษณะที่สำคัญของการคำนวณแบบคลาวด์ไว้ 5 คุณลักษณะ ดังรูปที่ 2.2 มีรายละเอียดดังนี้

รูปที่ 2.2 นิยามการประมวลผลแบบคลาวด์ของ NIST

ที่มา: Liu et al., 2011

การบริการตัวเองตามคำขอ (On-Demand Self-Service) เป็นคุณลักษณะที่ผู้ใช้สามารถร้องขอหรือกำหนดสมรรถนะการคำนวณได้ด้วยตนเอง การประมวลผลแบบคลาวด์จะดำเนินการให้โดยอัตโนมัติ โดยผู้ใช้ไม่ต้องมีปฏิสัมพันธ์กับผู้ให้บริการเช่น เวลาในประมวลผลของเครื่องให้บริการ ปริมาณของหน่วยเก็บสำรองข้อมูล เป็นต้น

การเข้าถึงโดยใช้เครือข่ายได้หลายแบบ (Ubiquitous Network Access) เป็นคุณลักษณะที่ผู้ใช้สามารถเข้าถึงบริการประมวลผลแบบคลาวด์โดยใช้เครือข่ายได้โดยใช้แพลตฟอร์มได้หลากหลายแบบ เช่น โทรศัพท์เคลื่อนที่ แท็ปเล็ต แล็ปท็อปคอมพิวเตอร์ หรือคอมพิวเตอร์ส่วนบุคคล

การรวบรวมทรัพยากร (Resource Pooling) เป็นคุณลักษณะที่ผู้ให้บริการประมวลผลแบบคลาวด์สามารถรวบรวมทรัพยากรต่าง ๆ ของการคำนวณ เช่น หน่วยเก็บสำรองข้อมูล หน่วยประมวลผล หน่วยความจำ หรือแบนด์วิดท์ของเครือข่าย เป็นต้น เพื่อให้บริการแก่ผู้ใช้บริการ

มหาวิทยาลัยรังสิต Rangsit University

หลาย ๆ คนได้ โดยสามารถแบ่งปันทรัพยากรตามที่ผู้ใช้แต่ละคนต้องการโดยที่ผู้ใช้ไม่ต้องรู้ว่าทรัพยากรเหล่านี้ตั้งอยู่ที่ใด

ความยืดหยุ่น (Rapid Elasticity) เป็นคุณลักษณะในการจัดเตรียมทรัพยากรสำหรับการประมวลผลแบบคลาวด์ได้อย่างยืดหยุ่น สามารถเพิ่มหรือลดทรัพยการได้โดยอัตโนมัติเพื่อให้เทียบเท่ากับความต้องการของผู้ใช้ และผู้ใช้สามารถดำเนินการได้เมื่อใดก็ได้

การวัดการใช้บริการ (Measured Service) เป็นคุณลักษณะที่ผู้ใช้บริการสามารถเฝ้าสังเกตและวัดการใช้ทรัพยากรที่ตนเองได้บริการได้ตลอดเวลาทำให้สามารถประเมินค่าใช้จ่ายในการใช้บริการได้ด้วยตนเอง นอกจากนี้ผู้ให้บริการก็สามารถเฝ้าสังเกตและวัดการใช้ทรัพยากรของผู้ใช้บริการแต่ละรายได้ตลอดเวลา ทำให้การคิดค่าบริการเป็นไปอย่างโปร่งใสและเป็นธรรมทั้งสองฝ่าย

นอกจากนี้จากการศึกษาพบว่ายังมีการนิยามคุณลักษณะของการคำนวณแบบคลาวด์ไว้เพิ่มเติมอีกดังนี้

1) องค์กรสามารถพัฒนาได้อย่างคล่องตัวเพิ่มมากขึ้น (Agility) เนื่องจากการประมวลผลแบบคลาวด์เพิ่มความยืดหยุ่นของผู้ใช้ด้วยการจัดสรรทรัพยากรได้ใหม่ สามารถเพิ่มหรือขยายทรัพยากร โครงสร้างพื้นฐานทางเทคโนโลยีได้อย่างคล่องตัว

2) สามารถต้นทุนและลดอุปสรรคการลงทุน (Cost Reduction) โดยการพิจารณาจากค่าใช้งานในการดำเนินงาน (Operational Expenditure) แทนการซื้อเครื่องบริการ (Server) พร้อมทั้งอุปกรณ์ต่าง ๆ เข้ามาใช้ในองค์กร เนื่องจากโครงสร้างพื้นฐานต่าง ๆ ของระบบสารสนเทศจะเป็นหน้าที่ของผู้ให้บริการคำนวณแบบคลาวด์ในการจัดเตรียมทั้งส่วนของเครื่องบริการ (Server) ระบบเครือข่าย ความปลอดภัย ค่าจ้างเจ้าหน้าที่ ค่าใช้จ่ายต่าง ๆ ตลอดจนค่าดำเนินการของระบบทั้งหมด นอกจากนี้ค่าใช้จ่ายในการดำเนินการสามารถกำหนดแบบละเอียดได้ตามการใช้งานของผู้ใช้บริการ เช่น ตามจำนวนหน่วยประมวลผล หน่วยความจำ หน่วยความจำสำรอง หรือความเร็วของระบบเครือข่ายที่ใช้งาน อย่างไรก็ตามจากการศึกษาพลว่าการประหยัดต้นทุนขึ้นอยู่กับประเภทของกิจกรรมที่รองรับและประเภทของโครงสร้างพื้นฐานที่มีอยู่ภายในองค์กรด้วย

3) ความเป็นอิสระของอุปกรณ์และตำแหน่ง (Device and Location Independent) ผู้ใช้สามารถเข้าถึงและใช้บริการระบบเทคโนโลยีสารสนเทศบนการคำนวณแบบคลาวด์ได้โดยใช้เว็บเบราเซอร์จากที่ใดก็ได้โดยไม่คำนึงถึงตำแหน่งหรือสถานที่ที่จะใช้งาน และผู้ใช้สามารถใช้อุปกรณ์

อิเล็กทรอนิกส์ต่าง เช่น คอมพิวเตอร์ส่วนบุคคล โน้ตบุ๊ก คอมพิวเตอร์ หรือโทรศัพท์มือถือ เนื่องจากโครงสร้างพื้นฐานที่อยู่นอกสถานที่มีผู้ให้บริการครอบคลุมพื้นที่หลักในหลาย ๆ ประเทศ เพื่อให้ผู้ใช้สามารถเข้าถึงการคำนวณแบบคลาวด์ได้ทางอินเทอร์เน็ต ช่วยให้ผู้ใช้สามารถเชื่อมต่อการคำนวณแบบคลาวด์ได้จากทุกที่

4) การบำรุงรักษาสภาพแวดล้อมของระบบการคำนวณแบบคลาวด์ (Maintenance) ทำได้ง่ายขึ้นเนื่องจากข้อมูลซอฟต์แวร์ หรือโครงสร้างพื้นฐานของระบบสารสนเทศถูกจัดเก็บไว้บนเครื่องบริการ (Server) ภายนอกที่ดูแลโดยผู้ให้บริการคำนวณแบบคลาวด์โดยองค์กรไม่ต้องลงทุนในการสร้างศูนย์ข้อมูล (Data Center) การบำรุงรักษาระบบการคำนวณแบบคลาวด์ได้รับการจัดการและปรับปรุงโดยทีมบำรุงรักษาของผู้ให้บริการคลาวด์ซึ่งช่วยลดต้นทุนได้อันเนื่องมาจากการประมวลผลบนคลาวด์เมื่อเปรียบเทียบกับการสร้างศูนย์ข้อมูลในองค์กร (Data Center)

5) การรองรับผู้ใช้ได้หลายราย (Multitenancy) เป็นการรวมศูนย์ของโครงสร้างพื้นฐานในสถานที่มีต้นทุนต่ำ ช่วยให้สามารถแบ่งปันทรัพยากรและค่าใช้จ่าย (Resource Sharing) ในกลุ่มผู้ใช้จำนวนมาก ซึ่งช่วยให้อัตราการใช้ประโยชน์ของทรัพยากรเพิ่มขึ้น โดยที่ผู้ใช้บริการไม่จำเป็นต้องทำลงทุนด้านค่าใช้ รวมถึงการบริหารจัดการทรัพยากรต่าง ๆ และอุปกรณ์เพื่อให้ตรงตามลักษณะการใช้บริการที่มีผู้ใช้จำนวนมากได้ ทั้งนี้เนื่องจากจากการศึกษาพบว่าทรัพยากรในระบบสารสนเทศถูกใช้ประโยชน์และการปรับปรุงประสิทธิภาพให้สามารถใช้งานได้เพียงร้อยละ 10 ถึงร้อยละ 20 เท่านั้น

6) ผลผลิต (Productivity) อาจเพิ่มขึ้นเมื่อผู้ใช้บริการหลายคนสามารถทำงานกับข้อมูลเดียวกันพร้อมกัน แทนที่จะรอให้ผู้ใช้คนแรกบันทึกและส่งข้อมูลนี้ต่อให้ผู้ใช้คนถัด ๆ ไป โดยจะมีการบันทึกข้อมูลเวลาไว้ด้วยเพื่อใช้ในการตรวจสอบ และผู้ใช้บริการแต่ละคนไม่จำเป็นต้องติดตั้งซอฟต์แวร์แอปพลิเคชัน รวมถึงขั้นตอนการอัพเกรดซอฟต์แวร์หรือฮาร์ดแวร์ลงในคอมพิวเตอร์ของตนเอง

7) ความพร้อมใช้งาน (Availability) เพิ่มมากขึ้นด้วยการใช้เครื่องบริการ (Server) หลาย ๆ เครื่องช่วยกันทำงาน ซึ่งทำให้การประมวลผลแบบคลาวด์ที่ออกแบบมาอย่างดีมีความเหมาะสมสำหรับความต่อเนื่องทางธุรกิจและการกู้คืนข้อมูลหลังภัยพิบัติ

8) ความสามารถในการปรับขนาดและความยืดหยุ่น (Scalability and Elasticity) แบบพลวัตร ช่วยให้สามารถการจัดเตรียมทรัพยากรได้อย่างละเอียด บนพื้นฐานการบริการตนเองที่ใกล้เคียงกับเวลาจริงที่ใช้บริการ ในปัจจุบันเครื่องเสมือนที่ใช้งานบนการคำนวณแบบคลาวด์สามารถทำงานได้อย่างรวดเร็ว แต่ความเร็วอาจจะแตกต่างกันตามปัจจัยที่เกี่ยวข้อง ตัวอย่างเช่น ประเภทของเครื่องเสมือน ตำแหน่ง ระบบปฏิบัติการ และผู้ให้บริการประมวลผลแบบคลาวด์

มหาวิทยาลัยรังสิต Rangsit University

ซึ่งช่วยให้สามารถขยายขนาดสมรรถนะของระบบได้เมื่อมีความต้องการใช้งานเพิ่มขึ้นหรือลดลง หากไม่มีการใช้ทรัพยากร ประโยชน์ที่ได้จากการประหยัดเวลาของความสามารถในการปรับขนาดระบบการประมวลผลแบบคลาวด์ยังหมายถึงเวลาของผลิตภัณฑ์สามารถออกสู่ตลาดเร็วขึ้น ความยืดหยุ่นทางธุรกิจที่มีเพิ่มมากขึ้น และความสามารถในการปรับตัว เนื่องจากการเพิ่มหรือลดทรัพยากรใช้เวลาไม่นานอย่างที่เคยเป็นในอดีต

2.1.3 แบบจำลองการให้บริการประมวลผลแบบคลาวด์ (Cloud Service Models)

จากแนวคิดและสถาปัตยกรรมเชิงบริการ (Service-Oriented Architecture) ที่มีการแนวคิดสนับสนุนให้ "ทุกอย่างในรูปแบบบริการ" หรือ “Everything as a Service” (ตัวย่อ EaaS หรือ XaaS) หน่วยงาน NIST ได้กำหนดนิยามการให้บริการของการคำนวณแบบคลาวด์ไว้ 3 ประเภท ได้แก่ Infrastructure as a Service (IaaS) Platform as a Service (PaaS) และ Software as a Service (SaaS) ดังรูปที่ 2.3 โมเดลเหล่านี้นำเสนอบริการที่เป็นนามธรรมในรูปแบบที่เป็นระดับชั้น (Stack Layers) ประกอบด้วย โครงสร้างพื้นฐาน แพลตฟอร์ม และซอฟต์แวร์ในการให้บริการ โดยแต่ละระดับชั้นสามารถเป็นอิสระและไม่ขึ้นต่อกันได้

รูปที่ 2.3 แบบจำลองการให้บริการประมวลผลแบบคลาวด์

ที่มา: Mell & Grance, 2011

มหาวิทยาลัยรังสิต Rangsit University

การให้บริการซอฟต์แวร์บนการประมวลผลแบบคลาวด์ (Software as a Service - SaaS)

เป็นการให้บริการซอฟต์แวร์แก่ผู้ใช้บริการบนการประมวลผลแบบคลาวด์โดยใช้โครงสร้างพื้นฐานของผู้ให้บริการ ผู้ใช้บริการสามารถเข้าถึงและใช้ซอฟต์แวร์โดยใช้อุปกรณ์ต่าง ๆ โดยใช้ระบบเครือข่าย โดยที่ผู้ใช้บริการไม่ต้องเข้าไปจัดการหรือควบคุมโครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ เช่น เครือข่าย เครื่องบริการ ระบบปฏิบัติการ หน่วยจัดเก็บข้อมูล หรือ การตั้งค่าของแต่ละซอฟต์แวร์

การให้บริการแพลตฟอร์มบนการประมวลผลแบบคลาวด์ (Platform as a Service - PaaS)

เป็นการให้บริการแพลตฟอร์มแก่ผู้ใช้บริการบนการประมวลผลแบบคลาวด์โดยใช้โครงสร้างพื้นฐานของผู้ให้บริการ ผู้ใช้บริการสามารถสร้างหรือเรียกใช้ซอฟต์แวร์ หรือพัฒนาซอฟต์แวร์ขึ้นใหม่ การใช้ไลบรารี และเครื่องมือที่สนับสนุนโดยผู้ให้บริการบนแพลตฟอร์มที่ใช้งานได้ โดยที่ผู้ใช้บริการไม่ต้องเข้าไปจัดการหรือควบคุมโครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ เช่น เครือข่าย เครื่องบริการ ระบบปฏิบัติการ หน่วยจัดเก็บข้อมูล หรือ การตั้งค่าของแต่ละซอฟต์แวร์ที่เรียกใช้ได้

การให้บริการโครงสร้างพื้นฐานบนการประมวลผลแบบคลาวด์ (Infrastructure as a Service –IaaS)

เป็นการให้บริการโครงสร้างพื้นฐาน เช่น หน่วยประมวลผล หน่วยเก็บสำรองข้อมูล เครือข่าย หรือทรัพยากรจำเป็นอื่น ๆ ให้แก่ผู้ใช้บริการบนการประมวลผลแบบคลาวด์ เพื่อให้ผู้ใช้สามารถเรียกใช้ซอฟต์แวร์ต่าง ๆ ได้ทั้งส่วนของระบบปฏิบัติการหรือซอฟต์แวร์ประยุกต์ โดยที่ผู้ใช้บริการไม่ต้องเข้าไปจัดการหรือควบคุมโครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ แต่ผู้ใช้บริการสามารถตั้งค่าของระบบปฏิบัติการ ระบบปฏิบัติการ หน่วยจัดเก็บข้อมูล หรือ การเรียกใช้ซอฟต์แวร์ประยุกต์ที่เรียกใช้ได้

นอกจากนี้ยังมีการให้คำนิยามเพิ่มเติมจากแหล่งอื่น ๆ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงตามยุคสมัยและตามกาลเวลา ตัวอย่างเช่น

มหาวิทยาลัยรังสิต Rangsit University

การให้บริการผ่านอุปกรณ์เคลื่อนที่ (Mobile Backend as a Service - MBaaS)

ปัจจุบันแนวโน้มการใช้บริการผ่านอุปกรณ์เคลื่อนที่ได้รับความสนใจจากผู้บริโภคระดับองค์กรและระดับผู้ใช้งานเป็นอย่างมาก รวมถึงนักพัฒนาเว็บแอปและแอปพลิเคชันบนอุปกรณ์เคลื่อนที่มีการเชื่อมโยงแอปพลิเคชันให้บริการต่าง ๆ เช่น การจัดการผู้ใช้ การแจ้งเตือนแบบพุช การผสานรวมกับบริการเครือข่ายสังคมออนไลน์กับที่เก็บข้อมูลบนการประมวลผลแบบคลาวด์และบริการคอมพิวเตอร์บนการประมวลผลแบบคลาวด์ด้วยเอพีไอ (Application Programming Interface - API) และชุดพัฒนาซอฟต์แวร์ (Software Development Toolkit - SDK)

การให้บริการฟังก์ชัน (Function as a Service - Faas)

เป็นการให้บริการฟังก์ชันบนการคำนวณแบบคลาวด์ โดยเป็นการเรียกใช้โพรซีเยอร์หรือฟังก์ชันจากระยะไกลที่ของเครื่องบริการ (Server) ที่ให้บริการ ซึ่งใช้ประโยชน์จากการประมวลผลแบบไร้เครื่องบริการ (Server) เพื่อเปิดใช้งานและการปรับใช้ฟังก์ชันแต่ละรายการในการคำนวณแบบคลาวด์เพื่อตอบสนองต่อเหตุการณ์ต่าง ๆ การให้บริการฟังก์ชันนี้อาจเรียกว่าการคำนวณแบบไร้เครื่องบริการ (Server) ได้เช่นกัน เนื่องจากผู้ใช้บริการซึ่งอาจเป็นองค์กรทางธุรกิจหรือบุคคลที่เป็นเจ้าของระบบไม่จำเป็นต้องซื้อ เช่า หรือจัดหาเครื่องบริการ (Server) หรือเครื่องเสมือนเพื่อให้ชุดคำสั่ง ส่วนหลังทำงาน ด้านการรักษาความปลอดภัยของการให้บริการฟังก์ชันผู้ให้บริการสามารถปรับปรุงเพิ่มทรัพยากรที่เน้นการรักษาความปลอดภัยได้เนื่องจากเป็นรูปแบบการรวมศูนย์ของข้อมูลและผู้ให้บริการสามารถทุ่มเททรัพยากรในการบริหารและการจัดการกับการรักษาความปลอดภัยที่ผู้ใช้บริการไม่สามารถจัดการได้หรือขาดทักษะทางเทคนิคในการแก้ไขได้ด้วยตนเอง อย่างไรก็ตามหลาย ๆ องค์กรมีความกังวลเกี่ยวกับการสูญเสียการควบคุมข้อมูลที่มีความละเอียดอ่อนและการขาดการรักษาความปลอดภัยของข้อมูลที่มีความสำคัญเนื่องจากข้อมูลเหล่านี้ไม่ถูกจัดเก็บและจัดการโดยองค์กรแต่ถูกจัดเก็บและจัดการโดยผู้ให้บริการคำนวณแบบคลาวด์อย่างไรก็ตามความซับซ้อนของการรักษาความปลอดภัยจะเพิ่มขึ้นอย่างมากเมื่อข้อมูลถูกกระจายไปทั่วพื้นที่ที่กว้างขึ้นหรือผ่านอุปกรณ์จำนวนมากขึ้น เช่น ระบบที่มีผู้เช่าบริการที่ต้องแบ่งปันทรัพยากรโดยผู้เช่าบริการที่ไม่เกี่ยวข้องกัน

มหาวิทยาลัยราชภัฏรังสิต Rangsit University

2.1.4 รูปแบบการใช้งานการประมวลผลแบบคลาวด์ (Cloud Deployment Models)

รูปที่ 2.4 รูปแบบการใช้งานการประมวลผลแบบคลาวด์

ที่มา: Mell & Grance, 2011

รูปแบบการใช้งานการประมวลผลแบบคลาวด์ (Cloud Deployment Models) สามารถแบ่งออกได้เป็น 4 ประเภท ดังรูปที่ 2.4 ดังนี้

ไพรเวทคลาวด์ (Private Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์มีไว้ให้บริการเฉพาะสมาชิกในองค์กรหรือหน่วยงานเท่านั้น ผู้ที่เป็นจ้าของหรือผู้บริหารจัดการอาจเป็นหน่วยงานเอง บุคคลที่ 3 หรือหน่วยงานร่วม

คอมมิวนิตีคลาวด์ (Community Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์มีไว้ให้บริการสำหรับสมาชิกในกลุ่มชุมชนที่มีความเห็น นโยบายหรือข้อตกลงร่วมกัน ผู้ที่เป็นจ้าของหรือผู้บริหารจัดการอาจมีได้หลายหน่วยงาน บุคคลที่3 หรือหน่วยงานร่วมเพื่อให้บริการแก่สมาชิกของชุมชน

พลับบลิคคลาวด์ (Public Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์แบบสาธารณะ ซึ่งเปิดให้ผู้ใช้งานทั่วไปสามารถเข้ามาใช้งานได้ ผู้ที่เป็นจ้าของหรือผู้บริหารจัดการอาจเป็นองค์กรภาคธุรกิจ สถาบันการศึกษา หรือหน่วยงานรัฐบาล

มหาวิทยาลัยรังสิต Rangsit University

ไฮบริดคลาวด์ (Hybrid Cloud) หมายถึง โครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ประกอบด้วยการรวมโครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ตั้งแต่สองชนิดที่แตกต่างกัน เช่น ไพรเวทคลาวด์ คอมมิวนิตีคลาวด์ หรือ พลับบลิคคลาวด์ ซึ่งอาจใช้เทคโนโลยีที่เป็นมาตรฐานทั่วไปหรือเทคโนโลยีของบริษัทต่าง ๆ ที่สามารถเคลื่อนย้ายข้อมูลหรือแอปพลิเคชันระหว่างโครงสร้างพื้นฐานของการประมวลผลแบบคลาวด์ได้

อย่างไรก็ตามผลการศึกษาของ Schneier (2009) พบว่าระบบการคำนวณแบบคลาวด์มีข้อจำกัดในบางประเด็นเช่นกัน การคำนวณแบบคลาวด์มีราคาถูกกว่าเพราะประหยัดจากขนาดและอาจต้องใช้ผู้ให้บริการภายนอก (Outsource) ผู้ใช้บริการอาจจะมีตัวเลือกการปรับแต่งที่จำกัดหรือผู้ให้บริการคลาวด์อาจให้บริการที่ไม่ตรงกับความต้องการรวมถึงประเด็นทางกฎหมายที่เกี่ยวข้อง องค์กรธุรกิจจำเป็นต้องชั่งน้ำหนักระหว่างประโยชน์ของการคำนวณแบบคลาวด์กับความเสี่ยงที่อาจเกิดขึ้น ในระบบการคำนวณแบบคลาวด์นั้นการควบคุมโครงสร้างพื้นฐานส่วนหลังบ้านจะจำกัดเฉพาะผู้จำหน่ายระบบคลาวด์เท่านั้น ผู้ให้บริการระบบคลาวด์มักตัดสินใจเกี่ยวกับนโยบายการจัดการซึ่งจะกลั่นกรองสิ่งที่ผู้ใช้ระบบคลาวด์สามารถทำได้ในการปรับใช้ ผู้ใช้การคำนวณแบบคลาวด์ยังถูกจำกัดเพื่อควบคุมและจัดการแอปพลิเคชัน ข้อมูล และบริการ

2.1.5 เทคโนโลยีที่อยู่เบื้องหลังการคำนวณแบบคลาวด์ (Background Technologies)

เทคโนโลยีที่อยู่เบื้องหลังและเป็นพื้นฐานและมีบทบาทสำคัญของการคำนวณแบบคลาวด์มีดังนี้

1) เทคโนโลยีฮาร์ดแวร์เสมือน (Hardware Virtualization Technology)
2) พื้นที่เก็บข้อมูลบล็อกเครือข่ายเสมือน (Virtualized Network Block Storage)
3) แซนด์บ็อกซ์ (Sandbox)
4) เวลาแฝง (Latency)

2.1.5.1) เทคโนโลยีฮาร์ดแวร์เสมือน (Hardware Virtualization Technology)

เทคโนโลยีฮาร์ดแวร์เสมือนเป็นองค์ประกอบหลักในการประมวลผลแบบคลาวด์ เนื่องจากช่วยให้สามารถแยกส่วนของฮาร์ดแวร์พื้นฐานออกจากระบบปฏิบัติการได้ และช่วยให้ผู้ให้บริการ

มหาวิทยาลัยรังสิต Rangsit University

ฮาร์ดแวร์บนการประมวลผลแบบคลาวด์อนุญาตให้ผู้ใช้บริการสามารถติดตั้งและใช้งานระบบปฏิบัติการชนิดต่าง ๆ ที่ต้องการได้อย่างสะดวกมากขึ้น

Douglas และ Gehrmann (2019) ได้เสนอภาพรวมเทคนิคและปัญหาพื้นฐานของเทคโนโลยีฮาร์ดแวร์เสมือนว่าสามารถแบ่งออกได้เป็นสองแบบคือ

1) ระบบเครื่องเสมือน (System Virtualization) หมายถึงระบบคอมพิวเตอร์ทั้งระบบเป็นระบบเครื่องเหมือนซึ่งช่วยให้ระบบเครื่องเสมือนหลายระบบสามารถทำงานพร้อมกันโดยแยกจากกันเป็นอิสระโดยสิ้นเชิง ไฮเปอร์ไวเซอร์หรือเครื่องมือตรวจสอบสถานะเครื่องเสมือนจะช่วยให้ระบบปฏิบัติการบนเครื่องเสมือนสามารถเข้าถึงหน่วยประมวลผล หน่วยความจำ อุปกรณ์ต่าง ๆ ระบบเครือข่าย ระบบปฏิบัติการบนเครื่องเสมือนจึงคิดว่ามีเครื่องคอมพิวเตอร์ของตัวเอง

2) พาราเวอร์ชวลไลเซวัน (Para-virtualization) เป็นคุณลักษณะที่ช่วยให้ระบบปฏิบัติการบนเครื่องเสมือนให้สามารถทำงานร่วมกับไฮเปอร์ไวเซอร์ได้ และมีส่วนประสานกับผู้ใช้ที่มีความปลอดภัยและมีประสิทธิภาพมากกว่าส่วนประสานระบบปฏิบัติการบนเครื่องเสมือนแบบทั่วไป

ไฮเปอร์ไวเซอร์สามารถแบ่งได้เป็นสองประเภท ดังนี้

1) ชนิดที่ 1 (Type 1) ไฮเปอร์ไวเซอร์ที่ทำงานไปยังส่วนฮาร์ดแวร์ของเครื่องคอมพิวเตอร์โดยตรงและทำหน้าที่ประมวลผลชุดคำสั่งของระบบปฏิบัติการ บนเครื่องเสมือนโดยตรง

2) ชนิดที่ 2 (Type 2) ไฮเปอร์ไวเซอร์ที่ทำงานผ่านระบบปฏิบัติการของเครื่องคอมพิวเตอร์หลัก

ชนิดของไฮเปอร์ไวเซอร์แสดงดังตารางที่ 2.1 แสดง เพื่อให้การทำงานของการจำลองระบบเครื่องเสมือนมีประสิทธิภาพจึงต้องการการสนับสนุนการทำงานของฮาร์ดแวร์จากหน่วยประมวลผล ปัจจุบันนี้หน่วยประมวลผลรุ่นใหม่ ๆ จากหลายบริษัทมีการสนับสนุนแล้ว ตัวอย่างเช่น เทคโนโลยี Intel Virtualization (Intel-VT) จากบริษัทอินเทล เทคโนโลยี AMD-V จากบริษัท AMD หรือ เทคโนโลยี TrustZone จากบริษัท ARM เป็นต้น

ระบบเครื่องเสมือนยังสามารถเพิ่มประสิทธิภาพได้โดยใช้กระบวนการ Pre-virtualization โดยที่ชุดคำสั่งระบบปฏิบัติการบนเครื่องเสมือนจะถูกตรวจสอบก่อนการประมวลผลโดยไฮเปอร์ไวเซอร์ แล้วถูกปรับปรุงชุดคำสั่งในขณะใช้งาน (Runtime) กระบวนการนี้ซึ่งคล้ายกับ

มหาวิทยาลัยรังสิต Rangsit University

การทำงานของตัวแปลภาษา (คอมไพเลอร์) แบบ Just-In-Time ช่วยเพิ่มประสิทธิภาพการทำงานได้เป็นอย่างมาก เทคโนโลยีเครื่องเสมือนมีการพัฒนาจากหลายบริษัท ตัวอย่างเช่น Xen ซึ่งเป็นเทคโนโลยีเครื่องเสมือนแบบโอเพนซอร์ส (Opensource) ส่วน VMWare เป็นเทคโนโลยีเครื่องเสมือนที่ใช้ในเชิงเชิงพาณิชย์ และ KVM เป็นเทคโนโลยีเครื่องเสมือนแบบโอเพนซอร์ส (Opensource) ที่ได้รับความสนใจมากในชุมชนลินุกซ์

ตารางที่ 2.1 ตารางแสดงชนิดของไฮเปอร์ไวเซอร์

	Xen	KVM	VMWare	Hyper-V
Open source	Yes	Yes	No	No
Type (1/ 2)	1.5	1.5	2	2
Hardware	x86 / x86_64	x86 / x86_64	x86 / x86_64	x86_64
Virtual hardware	Qemu x86 / x86_64	Qemu x86 / x86_64	x86 / x86_64	x86 / x86_64
Features	Nested virtualization, live migration	Nested virtualization, live migration		
Association	Citrix	Red Hat / Intel	VMWare	Microsoft

ที่มา: Douglas & Gehrmann, 2019

Xen

เป็นไฮเปอร์ไวเซอร์แบบโอเพนซอร์ส (Opensource) มีการเปิดตัวรุ่นแรกในปี 2545 ถือได้ว่าเป็นไฮเปอร์ไวเซอร์ที่ความครบถ้วนและมีเสถียรภาพ นอกจากนี้มีการสนับสนุนในการทำไปใช้เชิงพานิชย์ได้ด้วย ผู้ให้บริการระบบเครื่องเสมือนที่มีการสนับสนุน Xen ตัวอย่างเช่น Red Hat, Novell และ Oracle นอกจากนี้ Xen ยังให้บริการเครื่องเสมือนโดย Xen ในรุ่นแรก ๆ จัดเป็นไฮเปอร์ไวเซอร์แบบ Para-virtualization จนกระทั่งเวอร์ชัน 4.0 จึงได้มีการเพิ่มความสามารถสำหรับการจำลองระบบเครื่องเสมือน (System Virtualization) เพื่อจัดการไดร์เวอร์ของอุปกรณ์ต่าง ๆ โดยใช้ระบบปฏิบัติการแบบพิเศษที่มีการให้สิทธิพิเศษมากขึ้น โดยที่ระบบปฏิบัติการจะจัดการคำร้องขอการใช้ไดร์เวอร์ของอุปกรณ์ทั้งหมดและได้ปรับไดร์เวอร์อุปกรณ์ให้เหมาะสมสำหรับฮาร์ดแวร์ที่พร้อมใช้งาน ระบบปฏิบัติบนเครื่องเสมือนจะได้รับการปรับปรุงเพื่อให้สามารถทำงานกับส่วนประสานเหล่านี้ได้

มหาวิทยาลัยรังสิต Rangsit University

VMware

VMware เป็นไฮเปอร์ไวเซอร์เชิงพาณิชย์แบบพาราเวอร์ชวลไลเซวัน (Para-virtualization) VMware ESX ติดตั้งและทำงานบนเครื่องคอมพิวเตอร์จริง (Bare Metal) และไม่ติดตั้งระบบปฏิบัติการเพิ่มเนื่องจาก VMware ESX มาพร้อมกับเคอร์เนลของลินุกซ์ที่จะถูกบูทขึ้นมาทำงานก่อนและมีหน้าที่โหลดไดร์เวอร์ของอุปกรณ์พิเศษและคุณสมบัติอื่น ๆ ที่ไฮเปอร์ไวเซอร์ต้องการ เคอร์เนลลินุกซ์และไดร์เวอร์เหล่านี้ช่วยให้การเข้าถึงอุปกรณ์ทั้งหมดของระบบกับระบบปฏิบัติการบนเครื่องเสมือน สำหรับคุณสมบัติ “Scan-Before-Execution” ของ VMware ESX นั้นคือชื่อเรียกของกระบวนการ Pre-virtualization ที่เป็นเทคโนโลยีการจำลองเครื่องเสมือนแบบรันไทม์ ช่วยให้ระบบปฏิบัติการบนเครื่องเสมือนทำงานบน VMWare โดยไม่ต้องมีการแก้ไขหรือปรับปรุง

KVM

KVM เป็นเทคโนโลยีการจำลองเครื่องเสมือนโดยจะทำการโหลดเคอร์เนลลินุกซ์ไปยังไฮเปอร์ไวเซอร์ ส่วนระบบปฏิบัติการบนเครื่องเสมือนแต่ละระบบจะกลายเป็นโปรเซสที่ทำงานในแบบวิธีผู้ใช้ (User-mode) ของไฮเปอร์ไวเซอร์ KVM จะถือว่าระบบปฏิบัติการบนเครื่องเสมือนแต่ละระบบกำลังรันบนหน่วยประมวลผลที่รองรับฮาร์ดแวร์สำหรับการจำลองเครื่องเสมือน อย่างไรก็ตามหน่วยประมวลผลรุ่นก่อนหน้านี้อาจจะไม่สามารถทำงานร่วมกับ KVM ได้ KVM ประกอบด้วยสองส่วน ได้แก่โมดูล KVM ที่ใช้ในการจำลองหน่วยความจำเสมือนและ QEMU ซึ่งเป็นโปรแกรมจำลอง I/O ของการจำลองเครื่องเสมือน

2.1.5.2) พื้นที่เก็บข้อมูลผ่านเครือข่ายแบบเสมือนจริง (Virtualized Network Block Storage)

พื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายเป็นการจับคู่ทางนามธรรมระหว่างสถานที่ตั้งทางกายภาพของที่จัดเก็บข้อมูลจริงและผู้ใช้งาน ช่วยให้เกิดความเป็นอิสระต่อกับระหว่างสถานที่ตั้งทางกายภาพของที่จัดเก็บข้อมูลจริงและผู้ใช้งาน นั่นคือสถานที่ตั้งทางกายภาพของที่จัดเก็บข้อมูลจริงและผู้ใช้งานไม่จำเป็นต้องอยู่ในสถานที่จริงที่เดียวกัน นอกจากนี้ยังช่วยให้การบริการและการจัดการพื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายสามารถทำได้สะดวกและสามารถรองรับ

มหาวิทยาลัยรังสิต Rangsit University

พื้นที่เก็บข้อมูลที่มาจากผู้ขายและระบบพื้นที่เก็บข้อมูลเสมือนจริงที่แตกต่างกันได้ (Heterogeneous) ประโยชน์ของพื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายโดยสรุปได้ดังนี้

1) การย้ายข้อมูลแบบไม่กระทบการทำงาน (Data Migration) ด้วยระบบเครื่องเสมือนช่วยให้สามารถย้ายข้อมูลไปยังตำแหน่งต่าง ๆ ได้แม้ว่าจะมีการใช้งานอยู่ก็ตาม ช่วยให้การจัดระเบียบข้อมูลในพื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายมีความเป็นอิสระมากขึ้น

2) ปรับปรุงการใช้ประโยชน์ (Utilization) เช่นเดียวกับการประมวลผลแบบคลาวด์ ข้อดีอีกอย่างหนึ่งของการใช้พื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายคือความสามารถในการใช้ทรัพยากร การจัดเก็บขอมูลที่มีอยู่ให้มีความเหมาะสมที่สุด

3) การจัดการแบบง่าย (Management) ประโยชน์อีกอย่างหนึ่งที่ได้รับจากการประมวลผลแบบคลาวด์ก็คือการบริหารและการจัดการแบบรวมศูนย์ ข้อมูลเสมือนจริงพื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายอาจจะอยู่ในสถานที่ทางกายภาพที่แตกต่างกันแต่ผู้ดูแลระบบสามารถเข้าไปบริหารและจัดการกับทรัพยากรพื้นที่เก็บข้อมูลเสมือนจริงผ่านเครือข่ายแบบรวมศูนย์ได้สะดวกและง่ายขึ้น

2.1.5.3) แซนด์บ็อกซ์ (Sandbox)

แซนด์บ็อกซ์เป็นกลไกการรักษาความปลอดภัยที่ใช้กันโดยทั่วไป โดยจะมีการรวมส่วนของโปรแกรมต่าง ๆ ไว้ในแซนด์บ็อกซ์ และจะมีการแยกส่วนของทรัพยากรออกจากกัน การรวมแอปพลิเคชันต่าง ๆ ไว้ในแซนด์บ็อกซ์ที่แยกออกจากโครงสร้างพื้นฐานเหล่านี้ ช่วยให้แอปพลิเคชันภายในแซนด์บ็อกซ์สามารถแชร์โครงสร้างพื้นฐานร่วมได้แม้ว่าแอปพลิเคชันอาจมีระดับความเชื่อถือที่แตกต่างกัน นอกจากนี้แซนด์บ็อกซ์ยังช่วยให้สามารถนำซอฟต์แวร์ที่อยู่ในช่วงของการพัฒนา (Developing Software) ทดสอบมาใช้งานร่วมกับซอฟต์แวร์ที่งานจริง (Production Software) ได้เนื่องจากแต่ละแซนด์บ็อกซ์จะมีการห่อหุ้ม (Encapsulating) ระบบต่าง ๆ ไว้ภายในระบบจะไม่ก่อให้เกิดผลกระทบที่ไม่พึงประสงค์กันและกัน แซนด์บ็อกซ์ยังช่วยให้เราสามารถแยกเครื่องเสมือนให้กับนักพัฒนาซอฟต์แวร์แต่ละกลุ่มออกจากแอปพลิเคชันอื่น ๆ ที่ทำงานอยู่ในเครื่องบริการ (Server) หรือเครื่องโฮสต์เดียวกันได้

มหาวิทยาลัยรังสิต Rangsit University

2.1.5.4) เวลาแฝง (Latency)

เทคโนโลยีการประมวลผลแบบคลาวด์มีจุดเด่นคือสามารถรองรับการปรับขยายขนาดของระบบในด้านต่าง ๆ ได้ในอนาคตคือ ทั้งด้านความสามารถในการประมวลผล ขนาดความจุของหน่วยความจำ ขนาดความจุพื้นที่จัดเก็บ และอัตราการรับส่งข้อมูลของเครือข่าย อย่างไรก็ตามเนื่องจากระบบการคำนวณแบบคลาวด์นั้นทรัพยากรของระบบนั้นสามารถอยู่ในสถานที่ตั้งทางกายภาพที่ห่างไกลเป็นอย่างมากได้ ดังนั้นเวลาแฝง (Latency) ก็อาจเป็นปัญหาสำคัญได้อย่างแน่นอน David Patterson ได้กล่าวถึง การแคช การจำลองแบบ และการทำนาย

1) การสร้างที่พักข้อมูล (Caching) การสร้างที่พักข้อมูลเป็นสร้างพื้นที่เพื่อใช้ในการจัดเก็บข้อมูลที่มีการใช้งานซ้ำ ๆ และใช้งานบ่อย ๆ แนวคิดนี้ได้รับการยอมรับว่าเป็นแนวทางหนึ่งที่สามารถช่วยให้เข้าถึงหรือมีการสืบค้นข้อมูลที่ต้องการได้รวดเร็วขึ้นและช่วยลดเวลาแฝง แนวคิดการสร้างที่พักข้อมูลมีการประยุกต์ใช้งานในหลาย ๆ ด้านตัวอย่างเช่น การให้บริการเว็บ โดยในบริบทของการคำนวณแบบคลาวด์นั้นหากต้องการความเร็วในการเขาถึงข้อมูลในที่พักข้อมูลควรสร้างที่พักข้อมูลบนหน่วยความจำ (Memcache) เนื่องจากการใช้หน่วยความจำเป็นที่พักข้อมูลนั้นมีความเร็วในการเข้าถึงข้อมูลได้อย่างรวดเร็วกว่าสื่อจัดเก็บข้อมูลชนิดอื่นเป็นอย่างมาก

2) การทำซ้ำ (Replication) เป็นการทำซ้ำระบบการคำนวณแบบคลาวด์เพิ่มขึ้นตั้งแต่หนึ่งชุดขึ้นไป การทำซ้ำไม่เพียงแต่ช่วยให้เกิดความทนทานของข้อมูล (Data Durability) เนื่องจากมีข้อมูลซ้ำกันมากกว่าหนึ่งชุดและอยู่คนละที่กันดังนั้นหากข้อมูลจากที่ใดที่หนึ่งไม่สามารถใช้งานหรือให้บริการได้ ผู้ใช้บริการสามารถเข้าใช้งานข้อมูลที่ยังคงเหลืออยู่อีกที่หนึ่งได้ นอกจากนี้การทำซ้ำยังช่วยปรับปรุงการให้บริการข้อมูลได้รวดเร็วขึ้นกล่าวคือหากผู้ใช้อยู่ใกล้กับชุดข้อมูลไหนก็สามารถเรียกใช้ข้อมูลจากชุดข้อมูลที่อยู่มากที่สุดก่อนซึ่งเป็นการช่วยลดเวลาแฝง (Latency) ลงไปได้ อีกทั้งข้อมูลก็ยังสามารถใช้แนวทางการสร้างที่พักข้อมูล (Caching) ร่วมด้วย

3) การคาดการณ์ล่วงหน้า (Prediction) เป็นแนวทางในการคาดการณ์การใช้ข้อมูลล่วงหน้าก่อนที่จะมีการเรียกใช้งานข้อมูลจริง ตัวอย่างเช่น การคาดการณ์การสืบค้นข้อมูล (Query) เพื่อเรียกใช้ข้อมูลจากฐานข้อมูลมาไว้ล่วงหน้า การใช้คิวรีและซีเควน (Sequence) ในชุดคำสั่งที่มีการทำซ้ำ (Loop) เพื่อค้นคืนข้อมูลที่อยู่เรียงต่อเนื่องกันเป็นต้น หรือเป็นการคาดการณ์ข้อมูลที่จะถูกเรียกใช้มาเก็บไว้ในที่พักข้อมูลในหน่วยความจำ (Memcache) ไว้ก่อนล่วงหน้าโดยอาจใช้ข้อมูลทางสถิติว่าข้อมูลใดที่จะถูกเรียกใช้งานต่อไป ซึ่งแนวทางการคาดการณ์ล่วงหน้านี้กสามารถช่วยลดเวลาแฝง (Latency) ลงได้เช่นกัน

2.2 การพิสูจน์ตัวจริง (Authentication)

2.2.1 ความสำคัญของการพิสูจน์ตัวจริง (Importance of Authentication)

ปัจจุบันระบบสารสนเทศมีจำนวนเพิ่มเป็นอย่างมากแต่ละระบบต่าง ๆ ก็มีข้อมูลหรือสารสนเทศที่มีความสำคัญ ซึ่งอาจเป็นข้อมูลส่วนบุคคลหรือข้อมูลขององค์กร เพื่อเป็นการป้องกันผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ระบบสารสนเทศ ระบบสารสนเทศส่วนใหญ่จึงมีความจำเป็นต้องมีการพิสูจน์ตัวจริงของผู้ที่ก่อนจะเข้ามาใช้งานระบบสารสนเทศก่อน

การพิสูจน์ตัวจริงเป็นกระบวนการของการเปรียบเทียบข้อมูลส่วนบุคคลของผู้ที่ต้องการเข้าสู่ระบบสารสนเทศเพื่อใช้งานกับข้อมูลส่วนบุคคลที่มีการลงทะเบียนไว้แล้วซึ่งเก็บไว้ในฐานข้อมูล ถ้ากระบวนการพิสูจน์ตัวจริงประสบความสำเร็จผู้ใช้จะได้รับอนุญาตให้เข้าสู่ระบบสารสนเทศ แต่หากการพิสูจน์ตัวจริงไม่สำเร็จหรือล้มเหลวผู้ใช้จะไม่ได้รับอนุญาตให้เข้าสู่ระบบสารสนเทศและได้รับข้อความแจ้งเตือนให้ป้อนข้อมูลประจำตัวที่ถูกต้อง ตัวอย่างเช่น ผู้ใช้ต้องการเข้าระบบสารสนเทศขององค์กรอาจต้องใช้อุปกรณ์เฉพาะ การพิสูจน์ตัวจริงโดยใช้รหัสโดยใช้หรือการพิสูจน์ตัวจริงโดยใช้ชีวมิติ

ปัจจุบันอุปกรณ์เคลื่อนที่มีการใช้งานอย่างแพร่หลายมากขึ้น จะเห็นได้จากยอดขายจำนวนอุปกรณ์เคลื่อนที่มีเพิ่มขึ้นอย่างต่อเนื่อง นอกจากนี้ยังมีการเพิ่มขึ้นของการประยุกต์ใช้การประมวลผลแบบคลาวด์ร่วมกับอุปกรณ์เคลื่อนที่ (Mobile Cloud Computing - MCC) ที่ผู้ใช้บริการสามารถใช้งานการประมวลผลแบบคลาวด์บนอุปกรณ์เคลื่อนที่ได้ทั้งบริการแพลตฟอร์ม ซอฟต์แวร์ หรือโครงสร้างพื้นฐานของคอมพิวเตอร์ เช่น การใช้พื้นที่บนหน่วยเก็บสำรองข้อมูลบนการประมวลผลแบบคลาวด์โดยใช้อุปกรณ์เคลื่อนที่ อย่างไรก็ตามจากนิยามหรือแนวคิดของการประมวลผลแบบคลาวด์เป็นลักษณะของการแบ่งปันทรัพยากรไม่ว่าจะเป็นข้อมูล สารสนเทศ ซอฟต์แวร์ แพลตฟอร์ม หรือโครงสร้างพื้นฐานซึ่งอาจกลายเป็นช่องโหว่หรือปัญหาด้านความปลอดภัยของทรัพยากรโดยการเข้าถึงทรัพยากรจากผู้ใช้บริการโดยไม่ได้รับอนุญาต ดังนั้นการพิสูจน์ตัวจริงจึงมีความสำคัญอย่างยิ่งในการประมวลผลแบบคลาวด์และการใช้งานอุปกรณ์เคลื่อนที่

รูปที่ 2.5 แผนภาพระบบชีวมิติ (Biometric System Diagram)

ที่มา: Damato, 2007

รูปที่ 2.5 แสดงแผนภาพระบบชีวมิติ (Biometric System Diagram) สามารถแบ่งได้เป็น 2 แบบวิธี (Mode) คือ 1) แบบวิธีการพิสูจน์ยืนยัน (Verification/Authentication Mode) เป็นการป้องกันบุคคลอื่นที่อาจมีลักษณะเฉพาะคล้ายกัน โดยจะเป็นการเปรียบเทียบชีวมิติที่รับค่ามากับเทมเพลตของชีวมิติที่จัดเก็บไว้ในฐานข้อมูลแบบ หนึ่งต่อหนึ่ง (One-to-one) เพื่อเป็นการพิสูจน์ยืนยันตัวตนของบุคคล โดยมีขั้นตอนคือหนึ่งแบบจำลองที่อ้างอิง (Reference Model) ของผู้ใช้แต่ละคนจะถูกสร้างและจัดเก็บไว้ในฐานข้อมูลของแบบจำลอง ขั้นที่สองตัวอย่างจะถูกจับคู่กับแบบจำลองที่อ้างอิงเพื่อให้คะแนนและคำนวณขีดแบ่ง (Threshold) ขั้นที่สามเป็นขั้นตอนการทดสอบ (Testing) โดยมีการบ่งชี้เทมเพลตที่จะใช้ในการเปรียบเทียบ และ 2) แบบวิธีการระบุตัวตน (Identification Mode) เป็นการเปรียบเทียบชีวมิติกับเทมเพลตที่เก็บไว้ในฐานข้อมูลชีวมิติแบบหนึ่งต่อหลาย (One-to-many) เพื่อระบุตัวตนของบุคคลโดยใช้ค่าขอบเขต (Threshold) ที่กำหนดไว้

จากรูปที่ 2.5 สามารถแสดงกระบวนการของระบบชีวมิติซึ่งแบ่งได้เป็น 2 เฟส (Phase) คือ 1) เฟสการลงทะเบียน (Registration Phase) ข้อมูลชีวมิติของแต่ละคนจะถูกนำเข้าระบบและจัดเก็บไว้โดยอุปกรณ์ อุปกรณ์รับรู้ (Sensor) ขั้นต่อมาข้อมูลชีวมิติจะถูกเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) โดยระบบจะทำการกำจัดสิ่งที่ไม่ต้องการบันทึกออกไปเพื่อเพิ่ม

คุณภาพของข้อมูลชีวมิติ ขั้นถัดมาคุณลักษณะที่ต้องการของข้อมูลชีวมิติจะถูกสกัดออกมาแล้วนำมาสร้างเป็นเทมเพลต โดยเทมเพลตเป็นผลที่ได้จากการคัดแยกคุณลักษณะเด่นที่ต้องการออกมาและกำจัดคุณลักษณะที่ไม่ต้องการออกไปเพื่อช่วยลดขนาดของไฟล์ข้อมูล และ 2) เฟสการจับคู่ (Matching Phase) เป็นการนำเทมเพลตที่ได้มาเปรียบเทียบและวิเคราะห์กับเทมเพลตที่ถูกจัดเก็บไว้ในฐานข้อมูลโดยใช้ขั้นตอนวิธีที่กำหนดไว้ ตัวอย่างเช่น ขั้นตอนวิธีแฮมมิงดิสแทนส์ (Hamming Distance)

การเลือกใช้ชีวมิติแบบใดนั้นขึ้นกับว่าจะประเมินชีวมิติชนิดใดและเป็นไปความต้องการของผู้ใช้ การเลือกว่าจะใช้ชีวมิติชนิดใดควรพิจารณา สมรรถนะ การยอมรับ การหลีกเลี่ยงความแข็งแกร่ง ปริมาณ ขนาด การป้องปรามจากการโจรกรรม ส่วนความต้องการของผู้ใช้ควรพิจารณา อุปกรณ์รับรู้ที่มีให้ใช้งาน อุปกรณ์ที่มีให้ใช้งาน เวลาในการประมวลผลและความน่าเชื่อถือ ค่าใช้จ่าย พื้นที่ที่อุปกรณ์รับรู้ทำงานได้ และการใช้พลังงาน

2.2.2 ประเภทของการพิสูจน์ตัวจริง (Authentication Types)

การพิสูจน์ตัวจริงโดยใช้อุปกรณ์เฉพาะ (Device/Token-based Authentication)

เป็นการพิสูจน์ตัวจริงโดยใช้อุปกรณ์ฮาร์ดแวร์เฉพาะที่สามารถเคลื่อนย้ายได้ง่าย ตัวอย่างเช่น บัตรอัจฉริยะ บัตรพนักงาน บัตรเครดิต ใบขับขี่ หนังสือเดินทาง หรือบัตรเอทีเอ็ม เป็นต้น บัตรเอทีเอ็มใช้การพิสูจน์ตัวจริงโดยใช้ข้อมูลที่บันทึกไว้ในแถบแม่เหล็กด้านหลังบัตรและการป้อนรหัสโดยใช้เข้าสู่ระบบสารสนเทศของธนาคารเพื่อดำเนินธุรกรรม หากผู้ใช้บริการไม่มีบัตรเอทีเอ็มและป้อนรหัสโดยใช้ไม่ถูกต้องระบบสารสนเทศของธนาคารจะไม่ให้ผู้ใช้บริการเข้าใช้บริการใด ๆ หรือการใช้บัตรพนักงานในการเข้าถึงระบบสารสนเทศขององค์กร หากผู้ใดไม่มีบัตรดังกล่าวก็ไม่สามารถเข้าสู่ระบบสารสนเทศได้

การพิสูจน์ตัวจริงโดยใช้รหัส (Password Authentication)

การใช้รหัสโดยใช้ในการการพิสูจน์ตัวจริงได้รับความนิยมใช้งานอย่างแพร่หลายเนื่องจากเป็นวิธีการที่ไม่ซับซ้อนมากนัก ผู้ใช้เพียงแค่ป้อนชื่อบัญชีผู้ใช้หรือรหัสโดยใช้เพื่อพิสูจน์ตัวจริงโดยส่วนมากจะอยู่ในรูปแบบของตัวอักษร สัญลักษณ์หรือตัวเลข ถ้าผู้ใช้บริการป้อนบัญชีผู้ใช้และ

มหาวิทยาลัยรังสิต Rangsit University

รหัสผ่านโดยใช้ถูกต้องจึงจะสามารถเข้าสู่ระบบสารสนเทศได้ อย่างไรก็ตามวิธีการนี้มีข้อจำกัดและพบปัญหาการโจรกรรมข้อมูลบัญชีผู้ใช้และรหัสผ่านโดยใช้อย่างต่อเนื่อง

การพิสูจน์ตัวจริงโดยใช้ชีวมิติ (Biometric Authentication)

การใช้ชีวมิติในการพิสูจน์ตัวจริงเป็นการนำคุณลักษณะขององค์ประกอบทางร่างกายหรือพฤติกรรมของผู้ใช้บริการเป็นข้อมูลนำเข้าเพื่อใช้ในการพิสูจน์ตัวจริง ตัวอย่างเช่น ลายนิ้วมือ ดวงตา ใบหน้า โครงสร้างมือ หรือเสียงพูด ซึ่งข้อมูลชีวมิติเป็นข้อมูลที่แสดงถึงคุณลักษณะทางกายภาพหรือพฤติกรรมของแต่ละบุคคลจึงเป็นข้อมูลที่ถูกโจรกรรมหรือลอกเลียนแบบได้ยาก อย่างไรก็ตามวิธีการนี้ก็อาจมีการลอกเลียนแบบข้อมูลชีวมวลมิติได้

ปัจจัยเจ็ดประการที่ต้องพิจารณาในการเลือกใช้ชีวมิติ

Jain, Ross และ Nandakumar (2011) นำเสนอปัจจัยเจ็ดประการที่ต้องพิจารณาในการเลือกใช้ชีวมิติให้มีความเหมาะสมต่อการนำไปประยุกต์ใช้งาน มีรายละเอียดดังนี้

1) ความแพร่หลาย (Universality) หมายถึงผู้ใช้งานระบบทุกคนควรที่จะครอบครองหรือเป็นเจ้าของคุณสมบัติของตนเอง

2) ความเป็นเอกลักษณ์ (Uniqueness) หมายถึง คุณลักษณะควรมีความแตกต่างกันอย่างเพียงพอต่อการระบุตัวบุคคลแต่ละบุคคล

3) ความคงทน (Permanence) หมายถึง ขั้นตอนวิธีของการจับคู่จะยังคงทำงานได้อย่างถูกต้องแม้ว่าคุณลักษณะอาจมีการเปลี่ยนแปลงได้ตามกาลเวลา

4) การวัดได้ (Measurability) หมายถึง ความสะดวกในการได้มาหรือการประเมินของคุณลักษณะ

5) สมรรถนะ (Performance) หมายถึง ความถูกต้อง ความเร็ว และความแข็งแกร่งของเทคโนโลยีที่นำมาใช้

6) การยอมรับ (Acceptability) หมายถึง ผู้ใช้ยอมรับในการใช้เทคโนโลยีชีวมิติในการถูกจับภาพหรือถูกประเมิน

7) การหลีกเลี่ยง (Circumvention) หมายถึง ความง่ายในการเลียนแบบลักษณะของปัจเจกบุคคล

มหาวิทยาลัยรังสิต Rangsit University

2.2.3 เทคนิคการพิสูจน์ตัวจริงโดยใช้ชีวมิติ (Biometric Authentication Techniques)

การพิสูจน์ตัวจริงโดยใช้ชีวมิติสามารถแบ่งได้เป็น 2 ประเภทคือ คุณลักษณะเฉพาะทางกายภาพ (Physical Features) และคุณลักษณะเฉพาะทางพฤติกรรม (Behavioral Features)

1) คุณลักษณะเฉพาะทางกายภาพ (Physical Features)

คุณลักษณะเฉพาะทางกายภาพเป็นการใช้คุณลักษณะทางกายภาพของบุคคลในการพิสูจน์ตัวจริง ตัวอย่างเช่น ลายนิ้วมือ เส้นลายมือ การรู้จำภาพใบหน้า ดีเอ็นเอ โครงร่างเส้นเลือดบนฝ่ามือ ลักษณะโครงสร้างของมือ การรู้จำโดยใช้ม่านตาหรือเรตินา หรือกลิ่น เป็นต้น การวิจัยครั้งนี้มุ่งเน้นการใช้คุณลักษณะทางกายภาพของบุคคลในการพิสูจน์ตัวจริงโดยใช้การรู้จำภาพใบหน้าตามแนวคิดปัจจัยเจ็ดประการที่ต้องพิจารณาในการเลือกใช้ชีวมิติที่นำเสนอโดย Jain et al. (2011)

2) คุณลักษณะเฉพาะทางพฤติกรรม (Behavioral Features)

คุณลักษณะเฉพาะทางพฤติกรรมเป็นการนำรูปแบบทางพฤติกรรมของบุคคลในการพิสูจน์ตัวจริง ตัวอย่างเช่น จังหวะการพิมพ์ ท่าทางการเดิน หรือเสียง เป็นต้น การวิจัยครั้งนี้มุ่งเน้นการใช้คุณลักษณะทางพฤติกรรมของบุคคลในการพิสูจน์ตัวจริงโดยใช้การเสียงแนวคิดปัจจัยเจ็ดประการที่ต้องพิจารณาในการเลือกใช้ชีวมิติที่นำเสนอโดย Jain et al. (2011)

กระบวนการพิสูจน์ตัวจริงด้วยภาพใบหน้า (Facial Authentication Process)

การรู้จำภาพใบหน้าเป็นวิธีการตรวจสอบตัวตนรูปแบบหนึ่งของชีวมิติที่ใช้ส่วนองค์ประกอบของภาพใบหน้าที่ได้จากกล้องถ่ายภาพดิจิทัลหรือกล้องวีดิทัศน์ดิจิทัลเพื่อใช้ในการระบุหรือพิสูจน์ยืนยันบุคคล ดังรูปที่ 2.6 มีขั้นตอนการดำเนินงานดังนี้

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 2.6 กระบวนการพิสูจน์ตัวจริงด้วยภาพใบหน้า

ที่มา: Rukhiran et al., 2022

1) เฟสการลงทะเบียน (Registration Phase)

การรับข้อมูล (Capturing) เป็นขั้นตอนการรับข้อมูลภาพใบหน้าจากกล้องถ่ายภาพ การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) เป็นขั้นตอนการคัดกรองให้ได้คุณลักษณะเด่นที่ต้องการบางส่วนและการวัดระยะขององค์ประกอบบนใบหน้า จุดของคุณลักษณะใบหน้า เช่น ตา ปาก จมูก หรือสันของกระดูก ขั้นตอนนี้เป็นขั้นตอนในการเก็บรวบรวมข้อมูลของผู้ใช้ผ่านกระบวนการลงทะเบียน ผู้ใช้จะป้อนข้อมูลพื้นฐานส่วนบุคคลและข้อมูลชีวมิติ ข้อมูลชีวมิติภาพใบหน้า

1.1) ขั้นที่ 1 การรับข้อมูล (Capturing) ผู้ใช้ที่ต้องการลงทะเบียนทำการป้อนข้อมูลส่วนบุคคล เช่น ชื่อบัญชีผู้ใช้ รหัสโดยใช้ อีเมล และข้อมูลชีวมิติได้แก่ภาพใบหน้าและข้อมูลเสียงโดยใช้เว็บแอปพลิเคชันที่ได้พัฒนาขึ้นบนอุปกรณ์ต่าง ๆ ที่มีโปรแกรมเว็บเบราเซอร์

1.2) ขั้นที่ 2 การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) ข้อมูลที่ชีวมิติที่รับเข้ามาจำเป็นต้องมีการแยกคุณลักษณะเด่นที่ต้องการไว้ ส่วนข้อมูลใดที่ไม่จำเป็นก็จะทำการนำออกไป ตัวอย่างเช่น ภาพหน้าคน ก็จะทำการตัดเฉพาะส่วนที่เป็นใบหน้าเท่านั้นที่จะมีผลต่อการพิสูจน์ตัวจริง ส่วนผมหรือส่วนอื่น ๆ ก็จะถูกตัดออกไป ข้อมูลชีวมิติทั้งสองแบบคือภาพใบหน้าและข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท

มหาวิทยาลัยรังสิต Rangsit University

การเตรียมข้อมูลภาพใบหน้าก่อนการประมวลผล (Face Preprocessing) ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การตรวจหาบริเวณดวงตาซึ่งมักเป็นบริเวณที่มีสีเข้มกว่าบริเวณอื่นโดยใช้ขั้นตอนวิธี Haar-cascade และจะมีการปรับขนาด (Scaling) การหมุนภาพ (Rotating) และการแปลงภาพ (Translating) นอกจากนี้จะทำการตัดส่วนของภาพให้เหลือเฉพาะบริเวณใบหน้าเท่านั้นส่วนประกอบอื่นเช่น หน้าผาก คาง ใบหู และภาพพื้นหลังอื่น ๆ ออก ขั้นที่ 2 การใช้เทคนิคฮิสโตแกรม (Histogram of Oriented Gradients) ในการเพิ่มคุณภาพของภาพต้นฉบับโดยการจัดวางตำแหน่งภาพ การปรับความสว่างและความคมชัดให้ด้านซ้ายและด้านขวาของภาพใบหน้า ขั้นที่ 3 การทำเครื่องหมายรูปวงรีเพื่อเป็นการเน้นภาพใบหน้า และจะกำจัดผมและพื้นหลังบางส่วนออกจากภาพใบหน้า ผลลัพธ์ที่ได้คือเฉพาะในรูปภาพใบหน้าเท่านั้น

1.3) การคัดแยกคุณลักษณะเด่น (Feature Extraction) เป็นนำผลลัพธ์ที่ได้จากขั้นตอนก่อนหน้านี้ทั้งส่วนของข้อมูลชีวมิติภาพใบหน้ามาทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองเฉพาะส่วนของตำแหน่ง หรือขนาดของอวัยวะ เช่น ตา จมูก หรือปาก การวิจัยนี้ใช้ขั้นตอนวิธี LBPH (Local Binary Pattern Histogram)

1.4) การจัดเก็บลงในฐานข้อมูล (Storing in Database) เป็นการนำเทมเพลตหรือแบบจำลองไปจัดเก็บไว้ในฐานข้อมูลซึ่งอยู่บนระบบการประมวลผลแบบคลาวด์ เพื่อนำไปใช้ในขั้นตอนถัดไป

2) เฟสการเรียนรู้ของเครื่อง (Training Phase)

เป็นขั้นตอนที่นำเอาข้อมูลที่ได้จากการแยกคุณลักษณะเด่นที่ต้องการ (Feature Extraction) ของแต่ละบุคคลมาเป็นข้อมูลเพื่อสอนให้คอมพิวเตอร์เรียนรู้ด้วยตนเองว่าลักษณะของโครงสร้างรูปภาพใบหน้าของแต่ละคนมีคุณลักษณะอย่างไร สำหรับการเรียนรู้ภาพใบหน้า (Facial Training) จะเป็นการนำเอาคุณลักษณะเด่นของภาพใบหน้าที่ได้มาจากเฟสที่ 1 มาสอนให้คอมพิวเตอร์เรียนรู้แล้วทำการสร้างเป็นโมเดล ซึ่งผลลัพธ์จากขั้นตอนการเรียนรู้ของเครื่องคอมพิวเตอร์นี้จะได้แบบจำลองหรือโมเดลสำหรับการเรียนรู้ของเครื่องคอมพิวเตอร์

มหาวิทยาลัยรังสิต Rangsit University

3) เฟสการพิสูจน์ตัวจริง (Authentication Phase)

กระบวนการการรู้จำเป็นกระบวนการที่สามารถใช้เพื่อยืนยันตัวตนหรือการตรวจสอบตัวบุคคลโดยการใช้ข้อมูลชีวมิติ เช่น คุณลักษณะเด่นของใบหน้าหรือเสียงเปรียบเทียบกับคุณลักษณะเด่นของใบหน้าหรือเสียงที่จัดเก็บไว้ในฐานข้อมูล สำหรับการบวนการการรู้จำภาพใบหน้าการวิจัยนี้ใช้ เทคนิค Local Binary Pattern Histogram (LBPH) ส่วนการรู้จำเสียงการวิจัยนี้ใช้การแจกแจงความน่าจะเป็นแบบผสมตามขั้นตอนวิธี Mel-frequency cepstral coefficients (MFCCs) ผลคะแนนที่ได้จากการเปรียบเทียบของชีวมิติทั้งสองแบบจะนำคะแนนมารวมกันเพื่อใช้กำหนดว่าการพิสูจน์ตัวจริงผ่านหรือไม่โดยผู้วิจัยกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่ร้อยละ 60 เนื่องจากผลการทดลองเชิงประจักษ์จากการวิจัยนี้พบว่า การใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันในการพิสูจน์ตัวจริงเพื่อเข้าใช้การบริการประมวลผลแบบคลาวด์มีค่าอยู่ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบในการพิสูจน์ตัวจริงโดยใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันเพื่อใช้บริการบนการประมวลผลแบบคลาวด์ได้ในอัตราร้อยละ 60

ขั้นตอนวิธีการตรวจหาภาพใบหน้า (Face Detection Algorithm)

Haar-cascade Classifier

ขั้นตอนวิธีการตรวจหาใบภาพหน้า Haar-cascade (Wilson & Fernandez, 2006) เป็นขั้นตอนวิธีการตรวจหาใบหน้าโดยการฝึกสอนให้คอมพิวเตอร์เรียนรู้ในการตรวจหาวัตถุต่าง ๆ รวมทั้งภาพใบหน้าของคนที่อยู่ในภาพ วิธีการนี้นำเสนอโดย Viola & Jones (2001) วิธีการนี้ประกอบด้วย 2 ส่วนคือ Haar และ Cascade

รูปที่ 2.7 กระบวน Haar-like Feature ในการตรวจหาใบหน้า

ที่มา: Viola & Jones, 2001

รูปที่ 2.8 แสดงตัวอย่างของ Haar-like Feature ในการตรวจหาใบหน้า

ที่มา: Jain et al., 2011

Haar-like Feature จะทำการแบ่งส่วนของภาพออกเป็นสี่เหลี่ยมจำนวนสอง สามหรือสี่ส่วน สี่เหลี่ยมแต่ละส่วนจะแทนด้วยสีขาวหรือสีดำ โดยความเป็นไปได้ของการแบ่งเป็นสี่เหลี่ยมดังแสดงในรูปที่ 2.7 คอมพิวเตอร์จะเรียนรู้ Haar-cascade จากภาพที่มีวัตถุที่ต้องการตรวจหาและภาพที่ไม่มีวัตถุที่ต้องการตรวจหา วัตถุประสงค์ของขั้นตอนนี้คือเพื่อดึงเอาคุณลักษณะที่เป็นส่วนประกอบที่แสดงถึงภาพของใบหน้ามาผสมผสาน ดังรูปที่ 2.8 ขั้นตอนวิธีการเรียนรู้ของเครื่องเพื่อตรวจหาวัตถุตามแนวทางของ Haar-cascade ต้องใช้ภาพระดับสีเทา (Grayscale) ความหนาแน่นของสีเทาจะถูกใช้เพื่อตรวจหาคุณลักษณะที่ต้องการโดยการคำนวณจากผลรวมของจำนวนจุดที่มีสีเข้มลบออกด้วยผลรวมของจำนวนจุดที่มีสีขาว การผสมผสานของคุณสมบัติต่าง ๆ ที่แยกออกมาจากขั้นตอนการเรียนรู้ของเครื่องจะถูกใช้ในการตรวจหาภาพใบหน้า การตรวจหาหาภาพใบหน้าจะใช้การจับคู่บล็อกของกลุ่มจุดภาพ (Blocks of Pixels) ทีละบล็อกไปจนหมด ส่วนประกอบของใบหน้าแต่ละส่วนจะถูกรู้จำอย่างถูกต้องในแต่ละบล็อกอย่างต่อเนื่องจนได้เป็นภาพใบหน้า ตัวอย่างเช่น บล็อกมีจำนวน 24x24 จุดภาพ หากผลการจับคู่ของบล็อกทำนำมาทดสอบไม่ตรงกันกระบวนการตรวจหาภาพใบหน้าจะหยุดลง ดังรูปที่ 2.9 F (Face) แสดงถึงการคัดแยกตรวจพบภาพใบหน้าในหน้าต่างที่ใช้ทดสอบก็จะบันทึกไว้ในกระบวนการถัดไป และ NF (Not Face) แสดงถึงการคัดแยกตรวจไม่พบภาพใบหน้าในหน้าต่างที่ใช้ทดสอบก็จะยกเลิกการทดสอบของหน้าต่างนี้ (Reject Window) วิธีการนี้มีสามารถใช้ในการตรวจหาภาพที่ไม่มีใบหน้าได้เช่นกันเนื่องจากการทดสอบจะทำเพียงไม่กี่ครั้งเพื่ออนุมานว่าภาพนั้นไม่มีใบหน้า ส่งผลให้มีการตรวจหาใบหน้าเมื่อแต่ละคุณลักษณะของชุดค่าผสมได้รับการจดจำอย่างถูกต้องในบล็อก

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 2.9 แสดงกระบวนการ Haar-cascade

ที่มา: Viola & Jones, 2001

รูปที่ 2.10 แสดงการผสมผสานคุณสมบัติต่าง ๆ อย่างคร่าว ๆ ของ การจับคู่ในแต่ละบล็อก จากรูปจะเห็นว่าส่วนของบริเวณดวงตาจะมีสีเข้มกว่าสีของบริเวณแก้ม บริเวณตรงกลางของจมูกจะมีสีที่อ่อนกว่า คุณลักษณะเด่นต่าง ๆ เหล่านี้ถูกคัดแยกออกมาจากการเรียนรู้ใช้เพื่อค้นหารูปแบบเพื่อเป็นตัวแทนของใบหน้า กระบวนการนี้จะประมวลผลไปทีละบล็อก ๆ ตั้งแต่บล็อกแรกไปจนถึงบล็อกสุดท้าย และเมื่อทำงานจบในรอบแรกแล้ว จะเริ่มกระบวนการในรอบต่อไปโดยการเพิ่มจำนวนจุดในบล็อกให้มีขนาดใหญ่ขึ้นแล้วจะทำการตรวจสอบหาภาพใบหน้าเช่นนี้ไปเรื่อย ๆ บล็อกที่อยู่ใกล้กันซึ่งอาจจะมีจุดภาพเพียงไม่กี่จุดภาพเท่านั้นที่แตกต่างกันทุกครั้งที่มีการตรวจพบใบหน้าในรูปภาพใบหน้าเดียวกันจะถูกตรวจพบในบล็อคที่ต่างกันได้ ใบหน้าที่ตรวจพบทั้งหมดที่เกี่ยวข้องกับบุคคลเดียวกันจะถูกรวมเข้าด้วยกันและถือเป็นใบหน้าเดียวเมื่อสิ้นสุดกระบวนการทั้งหมด การสะสมของตัวจำแนกประเภทที่ Weak นี้สามารถใช้เพื่อสร้างเครื่องตรวจหาใบหน้าได้อย่างรวดเร็วด้วยความแม่นยำที่เหมาะสมตัวแยกประเภทแบบ Haar-cascade อาจจะได้รับการฝึกฝนเพียงครั้งเดียวก็ได้ ดังนั้นจึงเป็นไปได้ที่จะสร้าง Haar-cascade ของตัวเองหรือใช้ตัวที่ผ่านการฝึกฝน (Pretrained) มาแล้วก็ได้

รูปที่ 2.10 แสดงการผสมผสานคุณสมบัติของ Haar-like Features

ที่มา: Viola & Jones, 2001

ฮิสโตแกรมของการไล่ระดับสี (Histogram of Oriented Gradients - HOG)

รูปที่ 2.11 แสดงฮิสโตแกรมของการไล่ระดับสี (Histogram of Oriented Gradients)
ที่มา: King, 2014

ฮิสโตแกรมของการไล่ระดับสีเป็นอีกหนึ่งวิธีที่ใช้การไล่ระดับสี (Dalal & Triggs, 2005; Déniz-Suárez, García, Salido, & Torre, 2011) เพื่อใช้ในการตรวจหาวัตถุและสามารถใช้ในการตรวจหาใบหน้าในภาพได้เช่นกัน วิธีการนี้ต้องใช้รูปภาพในโทนสีเทา (Grayscale) แต่ละจุดภาพของรูปภาพจะแสดงด้วยตัวเลขจำนวนเต็มเพื่อแสดงระดับความเข้มของสีเทา วิธี HOG จะทำการเปรียบเทียบแต่ละจุดภาพกับจุดภาพที่อยู่รอบ ๆ ตัวเอง โดยปกติแล้วจุดภาพหนึ่ง ๆ จะถูกล้อมรอบด้วยจุดภาพอื่น ๆ อีกแปดจุดภาพ เป้าหมายของฮิสโตแกรมของการไล่ระดับสีคือเพื่อหาทิศทางหรือแนวโน้มของภาพที่มีสีที่เข้มเพิ่มขึ้น จากรูปที่ 2.11 จะเห็นว่ารูปลูกศรสีขาวจะแสดงทิศทางชี้ยังส่วนที่มีสีเข้มกว่า ข้อดีของวิธีนี้คือผลลัพธ์จะไม่ไวต่อการเปลี่ยนแปลงของความสว่าง ตัวอย่างเช่น หากรูปภาพมืดลงจุดภาพทั้งหมดก็จะมืดลง ลูกศรที่แสดงทิศทางที่มืดลงจะไม่เปลี่ยนในภาพที่สว่างกว่า

ขั้นตอนนี้ทำให้เห็นรายละเอียดการวิเคราะห์โครงร่างของใบหน้า จุดมุ่งหมายคือการรู้จำภาพใบหน้าใด ๆ ก็ได้แต่การตรวจหาใบหน้าหนึ่งหน้าจากภาพจะมีรายละเอียดที่ต้องนำมาวิเคราะห์จำนวนมาก ดังนั้นเพื่อเป็นการลดรายละเอียดจึงต้องเก็บเฉพาะทิศทางที่เกี่ยวข้องของภาพใบหน้าที่ต้องการอย่างเฉพาะเจาะจง ขั้นตอนต่อไปคือการแบ่งรูปภาพออกเป็นสี่เหลี่ยมจัตุรัสขนาด 16x16 จุดภาพ แล้วนับจำนวนครั้งที่แต่ละทิศทางถูกค้นพบและจะมีการวาดลูกศรในช่องสี่เหลี่ยมที่มีทิศทางซึ่งพบบ่อยที่สุดเพียงอันเดียว ดังรูปที่ 2.11 แสดงค่าเฉลี่ยของการแสดงทิศทางของลูกศรที่ผ่านการเรียนรู้ของเครื่องโดยใช้ภาพ 3,000 ภาพและใช้ไลบรารี dlib (King, 2009, 2014)

เมื่อเครื่องตรวจหาได้รับการฝึกฝน (Pretraining) แล้วก็พร้อมในการนำไปใช้งาน สำหรับการตรวจหาภาพใบหน้า เครื่องตรวจหาจะตรวจสอบภาพ ค้นหาใบหน้า และตรวจสอบว่าโครงสร้างใบหน้าตรงกับที่ใดที่หนึ่งของภาพหรือไม่ แต่ละครั้งที่รูปแบบ (Pattern) ถูกตรวจหาได้ที่ใดที่หนึ่งในภาพ หมายความว่ามีการตรวจพบใบหน้าแล้ว วิธีนี้ยังสามารถใช้เพื่อค้นหาใบหน้าหลาย ๆ หน้าในรูปภาพเดียวกันได้ด้วย

การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing)

การคัดแยกคุณสมบัติเด่นของภาพใบหน้าออกจากภาพต้นฉบับที่ป้อน เราสามารถใช้ขั้นตอน ๆ ได้หลายวิธีตามที่ได้กล่าวไปในหัวข้อก่อนหน้านี้ได้ ขั้นตอนถัดไปคือกระบวนการก่อนการประมวลผลข้อมูลภาพใบหน้าเพื่อให้ขั้นตอนการฝึกอบรมง่ายขึ้นและเพิ่มโอกาสในการจดจำบุคคลได้อย่างถูกต้องมากขึ้น ข้อมูลสำหรับการฝึกของเครื่องจะถูกทำให้เป็นมาตรฐานเดียวกันไม่ว่าภาพที่ได้มานั้นจะผ่านการซูมหรือมีขนาดที่แตกต่างกันโดยมีกระบวนการหลัก 3 ขั้นตอนคือ

1) การตรวจหาบริเวณดวงตาซึ่งมักเป็นบริเวณที่มีสีเข้มกว่าบริเวณอื่นและจะมีการปรับขนาด (Scaling) การหมุนภาพ (Rotating) และการแปลงภาพ (Translating)

2) การใช้เทคนิคฮิสโตแกรมในการเพิ่มคุณภาพของภาพต้นฉบับ โดยการจัดวางตำแหน่งภาพ การปรับความสว่างและความคมชัด

3) การทำเครื่องหมายรูปวงรีเพื่อเป็นการเน้นภาพใบหน้า และจะกำจัดผมและพื้นหลัง

เริ่มต้นจากการปรับตำแหน่งของใบหน้าควรจะต้องอยู่ตรงกลางภาพเหมือนกัน โดยสามารถวิเคราะห์ได้จากการกำหนดตำแหน่งของดวงตาทั้งสองข้างและจมูกมักถูกใช้เป็นจุดสังเกตสำหรับใบหน้าที่อยู่ตรงกลาง ดังนั้นจุดมุ่งหมายคือทำให้ดวงตาอยู่ในระดับเดียวกันและจมูกอยู่ในตำแหน่งเดียวกันสำหรับทุก ๆ ทั้งหมด เราสามารถใช้เครื่องแยกประเภท (Classifier) Haar-cascade เพื่อตรวจหาจมูกและดวงตาได้ นอกจากนี้ยังสามารถใช้เครื่องตรวจหาจุดสังเกตใบหน้าซึ่งมีอยู่ในไลบรารี dlib ซึ่งอิงตามผลงานของ Kazemi & Sullivan (2011) เครื่องมือที่ใช้ตรวจหาจุดเด่น (Landmark Detector) ได้รับการฝึกอบรมให้จดจำจุดเฉพาะ 68 จุดบนใบหน้าดังแสดงไว้ในรูปที่ 2.12 วิธีนี้ได้รับการฝึกอบรมด้วยรูปภาพจำนวนมากที่เคยติดป้ายกำกับด้วยตนเองแล้วสำหรับจุดสังเกตแต่ละแห่ง

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 2.12 รูปแสดงคุณลักษณะเด่นของภาพใบหน้า
ที่มา: Rosebrock, 2017

เครื่องตรวจหาใบหน้า (Face Detector) สามารถใช้เพื่อควบคุมให้ภาพอยู่กึ่งกลางได้ ตัวอย่างเช่น บนจุดสังเกตหมายเลข 37, 46 ซึ่งอยู่ในดวงตาและหมายเลข 34 ซึ่งอยู่ด้านล่างของจมูก ภาพใบหน้าสามารถหมุนได้จนกว่าจุดสังเกต 37 และ 46 จะอยู่ระดับเดียวกัน การปรับเปลี่ยนนี้ช่วยให้สามารถเปรียบเทียบภาพใบหน้าที่ไม่ได้หันหน้าตรงมาที่กล้อง เช่น เอียงหน้ามาด้านข้าง เป็นต้น

จากนั้นเมื่อรูปภาพทั้งหมดอยู่ในสภาวะเดียวกันคือเห็นหน้าตรงทุกใบหน้าแล้ว ก็สามารถปรับขนาดภาพให้เป็นขนาดทั่วไปได้ และยังสามารถตัดขอบภาพรอบใบหน้าได้อีกด้วย จากข้อแนะนำพบว่าควรใช้ขนาดภาพใบหน้าที่เล็ก เช่น 96x96 จุดภาพ เนื่องจากรูปภาพจะขนาดที่เล็กกว่าและทำให้ขั้นตอนการเรียนรู้ของเครื่องทำได้เร็วขึ้น จุดมุ่งหมายคือการหาขนาดที่เหมาะสมซึ่งมีขนาดเล็กที่สุด เพื่อปรับปรุงเวลาในการคำนวณและเก็บข้อมูลให้เพียงพอสำหรับการจดจำบุคคล ต้องทำการทดสอบหลายครั้งเพื่อหาขนาดที่เหมาะสม

ขั้นตอนวิธีการรู้จำภาพใบหน้า (Facial Recognition's Algorithm)

Jain et al. (2011) นำเสนอขั้นตอนวิธีการรู้จำภาพใบหน้า (Facial Recognition's Algorithm) ไว้ 3 แนวทางหลัก ประกอบด้วย Appearance-Based Techniques, Model-Based Techniques และ Texture-Based Approaches ดังรูปที่ 2.13 มีรายละเอียดดังนี้

รูปที่ 2.13 แสดงขั้นตอนวิธีการรู้จำภาพใบหน้า

ที่มา: Jain et al., 2011

Appearance-Based Techniques เป็นเทคนิคที่ใช้พื้นฐานของลักษณะที่ปรากฏ เทคนิคนี้จะสร้างการแสดงพื้นที่ใบหน้าทั้งหมดแบบย่อของภาพใบหน้าที่ได้มาโดยจับคู่ภาพใบหน้าที่มีมิติสูง (High-Dimensional) ลงในพื้นที่ย่อยที่มีมิติต่ำกว่า (Lower-Dimensional) พื้นที่ย่อยนี้ถูกกำหนดโดยชุดของเวกเตอร์พื้นฐานที่เป็นตัวแทน ซึ่งจะถูกเรียนรู้โดยใช้ชุดฝึกของรูปภาพ การจัดผังคำอาจจะเป็นเส้นตรงหรือไม่เป็นเชิงเส้นก็ได้ แต่รูปแบบที่ใช้กันทั่วไป เช่น การวิเคราะห์องค์ประกอบหลัก (PCA) การวิเคราะห์การเลือกปฏิบัติเชิงเส้น (LDA) และการวิเคราะห์องค์ประกอบอิสระ (ICA) ซึ่งเกี่ยวข้องกับการประมาณการเชิงเส้น

Model-Based Techniques เป็นเทคนิคที่ใช้พื้นฐานการสร้างแบบจำลอง โดยจะมีการสร้างโมเดลใบหน้าแบบสองมิติ (2D) หรือสามมิติ (3D) ที่สามารถช่วยการจับคู่ภาพใบหน้าเมื่อมีรูปแบบท่าทางต่าง ๆ ได้สะดวกขึ้น ตัวอย่างของโมเดลใบหน้า 2 มิติประกอบด้วย Face Bunch Graphs (FBG) และ Active Appearance Model (AAM) ส่วนโมเดลใบหน้า 3 มิติประกอบด้วย Morphable Model

Texture-based Approaches เป็นวิธีการที่พยายามค้นหาคุณลักษณะภายในภาพที่มีประสิทธิภาพ และไม่แปรผันต่อท่าทางหรือทิศทางของใบหน้าในภาพ รวมถึงแสงสว่าง ประกอบด้วยสองแนวทางได้แก่ Gradient Orientations และ Local Binary Patterns (LBP)

มหาวิทยาลัยรังสิต Rangsit University

การวิจัยนี้ใช้การรู้จำภาพใบหน้าโดยใช้ Texture-based Approaches ซึ่งเป็นวิธีการสามารถค้นหาคุณลักษณะภายในภาพที่มีประสิทธิภาพ และไม่แปรผันต่อท่าทางหรือทิศทางของใบหน้าในภาพ หรือแสงสว่าง รวมทั้งเมื่อวิเคราะห์ถึงทรัพยากรทั้งส่วนของฮาร์ดแวร์และซอฟต์แวร์ที่มีอยู่ ผู้วิจัยจึงเลือกใช้วิธีการ Local Binary Patterns (LBP) มาใช้ในการวิจัยในครั้งนี้

รูปที่ 2.14 แสดงขั้นตอนวิธีการรู้จำภาพใบหน้าแบบ LBP

ที่มา: Jain et al., 2011

Local Binary Patterns (LBP) เป็นวิธีการที่ใช้การรู้จำวัตถุต่าง ๆ รวมถึงการรู้จำภาพใบหน้าที่มีประสิทธิภาพโดยจะทำการค้นหาคุณลักษณะภายในของสิ่งต่าง ๆ กระบวนการทำงานของ LBP จะได้มาจากการเปรียบเทียบจุดภาพที่ใกล้เคียงกันของภาพขนาด 3 × 3 โดยจะเปรียบเทียบความค่าความเข้มของจุดภาพทั้ง 8 จุดภาพที่อยู่รอบ ๆ จุดภาพที่อยู่กึ่งกลาง ถ้าจุดภาพใดมีความเข้มมากกว่าจุดภาพที่อยู่กึ่งกลางจะให้ผลมีค่าเป็น 1 ถ้าจุดภาพใดมีความเข้มน้อยกว่าจุดภาพที่อยู่กึ่งกลางจะให้ผลมีค่าเป็น 0 รูปที่ 2.14 แสดงตัวอย่างวิธีการ LBP สมมติให้ค่าของจุดภาพตำแหน่งกึ่งกลางมีค่าเท่ากับ 3 เมื่อเปรียบเทียบความเข้มกับจุดภาพ 8 จุดภาพที่อยู่รอบ ๆ จะได้ผลการเปรียบเทียบจำนวน 8 บิต ตัวอย่างเช่น 11000111 นำมาคูณกับน้ำหนักของตัวเลขแต่ละหลักตามสมการที่ (2-1)

$$\text{LBP} = \sum [\text{Comparing_Result x Weight}] \qquad (2\text{-}1)$$

$$\text{LBP} = \sum [11000111] \text{ x } [2^0 \text{ x } 2^1 \text{ x } 2^2 \text{ x } 2^3 \text{x } 2^4 \text{ x } 2^5 \text{ x } 2^6 \text{ x } 2^7] = 227$$

มหาวิทยาลัยรังสิต Rangsit University

กระบวนการเปรียบเทียบความเข้มของจุดภาพนี้จะถูกดำเนินการไปเรื่อย ๆ จนครบทุกจุดภาพของภาพ ผลของวิธีการ LBP จะได้เป็นเมทริกซ์ทั้งหมดของความแตกต่างความเข้มของจุดภาพที่อยู่รอบ ๆ จุดภาพกึ่งกลางที่แสดงคุณลักษณะเด่นของภาพใบหน้าของแต่ละบุคคล นอกจากนี้มีการนำเสนอ Multiscale (MLBP) ซึ่งเป็นวิธีการเพิ่มความความสามารถจาก LBP ปกติ โดยสามารถกำหนดค่า P และค่า R โดยค่า R (Radius) หมายถึงรัศมีนับจากจุดภาพกึ่งกลางไปยังจุดภาพที่อยู่รอบ ๆ โดยปกติ R จะมีค่าเป็น 1 หมายถึงรัศมีนับจากจุดภาพกึ่งกลางไปยังจุดภาพที่อยู่รอบ ๆ จำนวน 1 จุดภาพ ส่วนค่า P (Pixel) หมายถึงจำนวนจุดภาพที่อยู่รอบ ๆ ที่จะนำมาเปรียบเทียบกับจุดภาพกึ่งกลาง ตัวอย่างเช่น ถ้าค่า P = 4 หมายถึงจะนำจุดภาพที่อยู่รอบ ๆ จำนวน 4 จุดภาพที่จะนำมาเปรียบเทียบกับจุดภาพกึ่งกลาง เป็นต้น ตัวอย่างการกำหนดค่า P และค่า R พร้อมกัน เช่น P=8 R=1.0 หมายถึงจะนำจุดภาพที่อยู่รอบ ๆ จำนวน 8 จุดภาพที่จะนำมาเปรียบเทียบกับจุดภาพกึ่งกลางและรัศมีนับจากจุดภาพกึ่งกลางไปยังจุดภาพที่อยู่รอบ ๆ จำนวน 1 จุดภาพ หรือ P=12 R=2.0 หมายถึงจะนำจุดภาพที่อยู่รอบ ๆ จำนวน 12 จุดภาพที่จะนำมาเปรียบเทียบกับจุดภาพกึ่งกลางและรัศมีนับจากจุดภาพกึ่งกลางไปยังจุดภาพที่อยู่รอบ ๆ จำนวน 2 จุดภาพ เป็นต้น

อย่างไรก็ตามหากมีการกำหนดค่า P สูง หมายถึงจะมีการจำนวนจุดภาพที่ต้องนำมาเปรียบเทียบกับจุดภาพกึ่งกลางจำนวนมากจะส่งผลให้เพิ่มเวลาในการประมวลผลและเพิ่มขนาดของเมทริกซ์ที่ใช้ในการเก็บผลลัพธ์ หากมีการกำหนดค่า R สูง หมายถึงจะมีระยะห่างหรือรัศมีของจุดภาพที่ต้องนำมาเปรียบเทียบกับจุดภาพกึ่งกลางเพิ่มขึ้นจะส่งผลให้เกิดการเปรียบของจุดภาพที่อยู่ห่างกันโดยไม่ได้แสดงคุณลักษณะภายในจุดภาพของภาพที่อยู่ติดกันอย่างเหมาะสม

หลังจากการเปรียบเทียบทุก ๆ จุดภาพของภาพใบหน้าตามวิธีการ LBP แล้วภาพใบหน้าจะถูกแบ่งออกเป็นหน้าต่างขนาดเล็กจำนวนมากแล้วแต่ละหน้าต่างจะถูกคำนวณโดยต่อด้วยวิธีการฮิสโตแกรม โดยมีเป้าหมายคือเพื่อหาทิศทางหรือแนวโน้มของภาพที่มีสีที่เข้มเพิ่มขึ้นข้อดีของวิธีนี้คือผลลัพธ์จะไม่ไวต่อการเปลี่ยนแปลงของความสว่าง จากนั้นเวกเตอร์คุณลักษณะเด่นของภาพใบหน้าทั้งหมดจะถูกสร้างขึ้นโดยการนำฮิสโตแกรมของแต่ละหน้าต่างมาเรียงต่อกันจะได้เป็นเวกเตอร์สุดท้าย ภาพใบหน้าสองภาพสามารถจับคู่ได้โดยการคำนวณความคล้ายคลึงหรือระยะทางที่แตกต่างกันระหว่างเวกเตอร์คุณลักษณะเด่น

มหาวิทยาลัยรังสิต Rangsit University

กระบวนการพิสูจน์ตัวจริงด้วยเสียง (Voice Authentication Process)

กระบวนการพิสูจน์ตัวจริงด้วยเสียงประกอบขั้นตอนดังรูปที่ 2.15 ได้แก่ การลงทะเบียนข้อมูลเสียงของผู้ใช้งาน (Enrollment Input Speech) การบันทึกเสียง (Voice Recording) การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) การคัดแยกคุณลักษณะเด่น (Feature Extraction) การจัดเก็บลงในฐานข้อมูล (Database) การเปรียบเทียบคุณลักษณะเด่น (Comparing) และผลลัพธ์จากการเปรียบเทียบคือ การพิสูจน์ว่าเป็นผู้ใช้งานจริง (Genuine) หรือ การไม่เป็นผู้ใช้งาน (Impostor)

รูปที่ 2.15 แสดงกระบวนการรู้จำเสียง

ที่มา: Rukhiran et al., 2022

มหาวิทยาลัยรังสิต Rangsit University

1) เฟสการลงทะเบียน (Registration Phase)

ขั้นตอนนี้เป็นขั้นตอนในการเก็บรวบรวมข้อมูลของผู้ใช้ผ่านกระบวนการลงทะเบียน ผู้ใช้จะป้อนข้อมูลพื้นฐานส่วนบุคคลและข้อมูลชีวมิติเสียงจากอุปกรณ์ไมโครโฟน โดยจะผ่านการเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) เป็นขั้นตอนการคัดกรองให้ได้คุณลักษณะเด่นของเสียงที่ต้องการ

1.1) ขั้นที่ 1 การรับข้อมูล (Capturing) ผู้ใช้ที่ต้องการลงทะเบียนทำการป้อนข้อมูลส่วนบุคคล เช่น ชื่อบัญชีผู้ใช้ รหัสโดยใช้ อีเมล และข้อมูลชีวมิติข้อมูลเสียง โดยใช้เว็บแอปพลิเคชันที่ได้พัฒนาขึ้นบนอุปกรณ์ต่าง ๆ ที่มีโปรแกรมเว็บเบราเซอร์

1.2) ขั้นที่ 2 การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) ข้อมูลที่ชีวมิติที่รับเข้ามาจำเป็นต้องมีการแยกคุณลักษณะเด่นที่ต้องการไว้ ส่วนข้อมูลใดที่ไม่จำเป็นก็จะทำการนำออกไป ข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท

การเตรียมข้อมูลเสียงก่อนการประมวลผล (Voice Preprocessing) เป็นกระบวนการย่อยของกระบวนการการคัดแยกคุณลักษณะเด่น โดยจะมีการปรับความสมดุลความถี่ของเสียงที่รับมาจากอุปกรณ์ไมโครโฟนให้อยู่ในระดับสัญญาณเสียงที่หูของมนุษย์สามารถรับรู้ได้อย่างเหมาะสม

1.3) การคัดแยกคุณลักษณะเด่น (Feature Extraction) เป็นนำผลลัพธ์ที่ได้จากขั้นตอนก่อนหน้านี้ ข้อมูลชีวมิติเสียงจะมาทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองคือเวกเตอร์ของเสียง MFCC ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การคัดแยกคุณลักษณะเด่นของข้อมูลเสียง (MFCC Extraction) โดยใช้ขั้นตอนวิธี MFCC จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติ ขั้นที่ 2 การคำนวณค่าเดลตา (Delta) จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติเช่นกัน ดังนั้นเมื่อรวมกันทั้งเวกเตอร์ของเสียงจาก MFCC กับเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติจากเดลตาจะได้เวกเตอร์ของเสียงที่มีคุณลักษณะจำนวน 40 มิติ ขั้นที่ 3 ข้อมูลชีวมิติเสียงจะถูกคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์คือ เทมเพลตของชีวมิติเสียง

1.4) การจัดเก็บลงในฐานข้อมูล (Storing in Database) เป็นการนำเทมเพลตหรือแบบจำลองไปจัดเก็บไว้ในฐานข้อมูลซึ่งอยู่บนระบบการประมวลผลแบบคลาวด์ เพื่อนำไปใช้ในขั้นตอนถัดไป

มหาวิทยาลัยรังสิต Rangsit University

2) เฟสการสอนเครื่องคอมพิวเตอร์ (Training Phase)

เป็นขั้นตอนที่นำเอาข้อมูลที่ได้จากการแยกคุณลักษณะเด่นที่ต้องการ (Feature Extraction) ของแต่ละบุคคลมาเป็นข้อมูลเพื่อสอนให้คอมพิวเตอร์เรียนรู้ด้วยตนเองว่าลักษณะเด่นเสียงที่ได้มาจากเฟสที่ 1 มาสอนให้คอมพิวเตอร์เรียนรู้แล้วทำการสร้างเป็นโมเดล สำหรับการเรียนรู้เสียง (Voice Training) การวิจัยนี้ใช้ขั้นตอนวิธีแบบจำลองส่วนผสมเกาส์เซียน (Gaussian Mixture Model) ซึ่งผลลัพธ์จากขั้นตอนการเรียนรู้ของเครื่องคอมพิวเตอร์นี้จะได้แบบจำลองหรือโมเดลสำหรับการเรียนรู้ของเครื่องคอมพิวเตอร์

3) เฟสการรู้จำเสียง (Voice Recognition)

กระบวนการการรู้จำเป็นกระบวนการที่สามารถใช้เพื่อยืนยันตัวตนหรือการตรวจสอบตัวบุคคลโดยการใช้ข้อมูลชีวมิติ เช่น คุณลักษณะเด่นของเสียงเปรียบเทียบกับคุณลักษณะเด่นของเสียงที่จัดเก็บไว้ในฐานข้อมูล สำหรับการรู้จำเสียงการวิจัยนี้ใช้การแจกแจงความน่าจะเป็นแบบผสมตามขั้นตอนวิธี MFCC ผลคะแนนที่ได้จากการเปรียบเทียบของชีวมิติทั้งสองแบบจะนำคะแนนมารวมกันเพื่อใช้กำหนดว่าการพิสูจน์ตัวจริงผ่านหรือไม่โดยผู้วิจัยกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่ร้อยละ 60 เนื่องจากผลการทดลองเชิงประจักษ์จากการวิจัยนี้พบว่า การใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันในการพิสูจน์ตัวจริงเพื่อเข้าใช้การบริการประมวลผลแบบคลาวด์มีค่าอยู่ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบในการพิสูจน์ตัวจริงโดยใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันเพื่อใช้บริการบนการประมวลผลแบบคลาวด์ได้ในอัตราร้อยละ 60

มหาวิทยาลัยรังสิต Rangsit University

การรู้จำเสียง (Voice Recognition)

การรู้จำโดยใช้เสียงเป็นการนำพฤติกรรมแบบหนึ่งของบุคคลในการพิสูจน์ตัวจริง ซึ่งต้องอาศัยองค์ความรู้ด้านภาษา วิทยาการคอมพิวเตอร์ และวิศวกรรมอิเล็กทรอนิกส์ มาประยุกต์เข้าด้วยกันเพื่อพัฒนาวิธีการหรือเทคโนโลยีที่สามารถรู้จำ เข้าใจภาษาของมนุษย์แล้วแปลงให้คอมพิวเตอร์เข้าใจได้ ระบบการรู้จำด้วยเสียงแบ่งได้เป็น 2 ประเภทคือ แบบที่ใช้การเรียนรู้ (Speaker Dependent) ระบบต้องมีการเรียนรู้เสียงของผู้ที่เป็นเจ้าของเสียงที่สามารถเพิ่มความถูกต้องของการพิสูจน์ตัวจริง และแบบที่ไม่ใช้การเรียนรู้ (Speaker Independent)

การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing)

การคัดแยกคุณลักษณะเด่นที่ต้องการ (Feature Extraction)

กระบวนการการคัดแยกคุณลักษณะเด่นใช้ขั้นตอนวิธี MFCC เป็นการคัดแยกลักษณะเด่นเฉพาะของหน่วยเสียงแต่ละหน่วยเสียงที่แตกต่างกันออกมาแล้วให้ระบบทำการรู้จำลักษณะเด่นของหน่วยเสียงแต่ละหน่วยเสียงไว้ เมื่อสัญญาณที่เข้ามาภายหลังมีลักษณะเด่นที่เหมือนหรือใกล้เคียงกับลักษณะเด่นของหน่วยเสียงใด ระบบรู้จำจะสามารถบอกได้ว่าเป็นหน่วยเสียงที่รับมานั้นใกล้เคียงกับหน่วยเสียงกลุ่มใดมากที่สุดและสามารถลดจำนวนข้อมูลโดยที่ข้อมูลจำนวนมากจะถูกแปลงเป็นชุดข้อมูลที่มีจำนวนน้อยลง และยังคงคุณสมบัติสำคัญของข้อมูลเดิมไว้ได้อย่างถูกต้อง ดังรูปที่ 2.16 มีขั้นตอนดังนี้

ขั้นที่ 1 การคัดแยกคุณลักษณะเด่นของข้อมูลเสียง (MFCC Extraction) โดยใช้ขั้นตอนวิธี MFCC จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติ

ขั้นที่ 2 การคำนวณค่าเดลตา (Delta) จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติเช่นกัน ดังนั้นเมื่อรวมกันทั้งเวกเตอร์ของเสียงจาก MFCC กับเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติจากค่าเดลตา (Delta) จะได้เวกเตอร์ของเสียงที่มีคุณลักษณะจำนวน 40 มิติ

ขั้นที่ 3 ข้อมูลชีวมิติเสียงจะถูกคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์คือเทมเพลตของชีวมิติเสียง

รูปที่ 2.16 แผนภาพกระบวนการ MFCC

ที่มา: Magre, Janse, & Deshmukh, 2014

มหาวิทยาลัยรังสิต Rangsit University

MFCC เซปสตรัม (Cepstrum) คือ การแปลงโคไซน์แบบไม่ต่อเนื่อง (Discrete Cosine Transform) ของลอการิทึมจากสเปกตรัมสัญญาณ ในช่วงสั้น ๆ สัมประสิทธิ์เซปสตรัมบนสเกลเมล (Coefficients) เป็นเทคนิคที่ปรับปรุงมาจากเซปสตรัม (Cepstrum) ด้วยการปรับสเกลของสเปกตรัมให้อยู่บนสเกลที่เหมาะสมสำหรับการรับฟังของมนุษย์โดยสังเกตจากลักษณะของสัญญาณเสียง สัญญาณเสียงในช่วงความถี่ต่ำ (Mel-Frequency Mel-spectrum) มีความสำคัญมากกว่าช่วงความถี่สูงจึงได้มีการออกแบบสเกลของสเปกตรัมให้สามารถเก็บรายละเอียดของสัญญาณเสียงช่วงความถี่ต่ำได้มากกว่า เรียกการออกแบบนี้ว่า เมลสเกล (Mel scale) โดยมีจะทำการคำนวณหาค่าสัมประสิทธิ์เซปตรัมบนสเกลเมล (Coefficients) ดังรูปที่ 2.17

รูปที่ 2.17 กระบวนการคัดแยกคุณลักษณะเด่นของ MFCC
ที่มา: Arslan & Yildiz, 2018

การจัดเก็บในฐานข้อมูล (Storing in Database) เป็นขั้นตอนการจัดเก็บแบบจำลองของเสียงจากขั้นตอนก่อนหน้าลงในฐานข้อมูล เพื่อใช้ในการเปรียบเทียบพิสูจน์ตัวจริง

มหาวิทยาลัยรังสิต Rangsit University

กระบวนการการรู้จำเสียงประกอบด้วยขั้นตอนดังนี้ (Rao & Manjunath, 2017)

1) Pre-Emphasis เป็นขั้นตอนเพื่อสร้างสมดุลของสเปกตรัมของเสียงที่เปล่งออกมาซึ่งมีความคลาดเคลื่อนของบริเวณที่มีความถี่สูง หากเป็นเสียงโดยทั่วไปที่เปล่งออกมาแหล่งกำเนิดสายเสียงมีความชันประมาณ -12 dB/Octave Slope อย่างไรก็ตามเมื่อพลังงานเสียงเปล่งออกมาจากริมฝีปากจะทำให้สเปกตรัมเพิ่มขึ้นประมาณ +6 dB/Octave Slope ผลที่อาจเกิดขึ้นคือสัญญาณเสียงพูดเมื่อบันทึกด้วยไมโครโฟนจากระยะไกลมีความชันลดลงประมาณ -6 dB/ Octave Slope เมื่อเทียบกับสเปกตรัมที่แท้จริงของเสียงพูด สมการที่ (2-2)

$$H(z) = 1 - bz^{-1} \tag{2-2}$$

โดยที่ b คือพารามิเตอร์ที่ใช้ควบคุมความชันของการกรองเสียงที่เปล่งออกมา โดยทั่วไปมีค่าอยู่ระหว่าง 0.4 ถึง 1.0

2) Frame Blocking And Windowing: สัญญาณเสียงพูดเป็นสัญญาณที่เปลี่ยนแปลงตามเวลาอย่างช้า ๆ เพื่อให้คุณลักษณะทางเสียงที่มีเสถียรภาพ การวิเคราะห์สัญญาณเสียงจึงควรทำในช่วงเวลาที่สั้น ๆ (Window) อย่างเพียงพอเพื่อให้สัญญาณเสียงมีความเสถียรภาพ การวัดสเปกตรัมในช่วงเวลาสั้นจะดำเนินการกับสัญญาณเสียงความยาวประมาณ 20 มิลลิวินาที และอาจเพิ่มขึ้นได้ทุก ๆ 10 มิลลิวินาที การเพิ่มกรอบเวลาทุก ๆ 10 มิลลิวินาทีจะทำให้สามารถติดตามลักษณะเฉพาะของเสียงพูดของแต่ละคนได้ โดยทั่วไปกรอบเวลาการวิเคราะห์ (Window) ความยาว 20 มิลลิวินาทีเพียงพอที่จะให้ผลการวิเคราะห์ที่ดีความละเอียดสเปกตรัมของเสียงเหล่านี้ และสั้นเพียงพอที่จะติดตามลักษณะเฉพาะที่สำคัญของเสียงพูดได้

3) DFT Spectrum: แต่ละ Window Frame จะถูกแปลงให้เป็นสเปกตรัมขนาดใหญ่ขึ้นโดยใช้วิธีการ DFT (Discrete Fourier Transform) ตามสมการที่ (2-3)

$$x(k) = \sum_{n=0}^{N-1} x(n) e^{\frac{-j2\pi nk}{N}} \quad ; \quad 0 \leq k \leq N-1 \tag{2-3}$$

โดยที่ N แทนจำนวนจุดภาพที่นำมาเปรียบเทียบ

มหาวิทยาลัยรังสิต Rangsit University

4) Mel Spectrum: เมลสเปกตรัมเป็นผลที่ได้จากการนำสัญญาณที่ผ่านการระบวนการแปลงฟูริเยร์ (Fourier Transformed Signal) ผ่านชุดตัวกรองแบนด์พาสชื่อว่า Mel-Filter Bank สำหรับ Mel หมายถึงหน่วยวัดที่มีพื้นฐานมาจากความถี่ที่หูของมนุษย์รับรู้ได้ Mel จะไม่สอดคล้องเชิงเส้นตรงกับความถี่ทางกายภาพของโทนเสียงเป็นเส้นตรง เนื่องจากระบบการได้ยินของมนุษย์ไม่ได้รับรู้ระดับเสียงเป็นเส้นตรง มาตราวัดของ Mel เป็นการประมาณการระยะห่างของความถี่เชิงเส้นที่ต่ำกว่า 1 KHz และระยะห่างแบบลอการิทึม (Logarithmic Spacing) ที่สูงกว่า 1 KHz การประมาณของ Mel จากความถี่ทางกายภาพสามารถแสดงได้จากสมการ (2-4)

$$f\ Mel = 2595 \log_{10}(1 + \frac{f}{700}) \tag{2-4}$$

โดยที่ f หมายถึงความถี่ทางกายภาพของเสียงมีหน่วยเป็น Hz และ f_{Mel} หมายถึงความถี่ของเสียงที่มนุษย์รับรู้ได้ ฟิลเตอร์แบงก์ (Filter Banks) สามารถนำมาใช้ได้ทั้งโดเมนด้านเวลาหรือโดเมนด้านความถี่ แต่โดยทั่วไปจะถูกนำมาใช้โดเมนด้านความถี่ ความถี่กึ่งกลางของตัวกรองโดยปกติจะมีระยะห่างเท่า ๆ กันบนแกนความถี่ จะมีการใช้ ฟังก์ชันไม่เป็นเชิงเส้น (Nonlinear Function) ในการสร้างแกนที่มีความเอนเอียง (Warped Axis) เพื่อเลียนแบบการรับรู้หูของมนุษย์ ตัวกรองที่ใช้บ่อยที่สุดคือรูปสามเหลี่ยมและในบางกรณีจะเป็นแบบ ตัวอย่างเช่น วิธีการแฮมมิง (Hamming)

เมลสเปกตรัมของสเปกตรัมขนาดใหญ่ X(k) คำนวณได้จากผลคูณของแต่ละส่วนของ Magnitude Spectrum กับ Triangular Mel Weighting Filters ตามสมการที่ (2-5)

$$s(m) = \sum_{k=0}^{N-1}[|X(k)|^2 |\ H_m(k)]\ ;\ \ 0 \leq \mathrm{m} \leq \mathrm{M\text{-}1} \tag{2-5}$$

โดยที่ M เป็นผลรวมของ Triangular Mel Weighting Filters และ *Hm(k)* เป็นค่าน้ำหนักที่กำหนดให้กับที่เก็บสเปกตรัมพลังงานตำแหน่งที่ k^{th} ร่วมกับกลุ่มเอาต์พุตที่ตำแหน่ง m^{th} ตามสมการที่ (2-6)

มหาวิทยาลัยรังสิต Rangsit University

$$H_m(k) = \begin{cases} 0 & ,k < f(m-1) \\ \frac{2(k-f(m-1))}{f(m)-f(m-1)} & ,f(m-1) \le k \le f(m) \\ \frac{2(f(m+1)-k)}{f(m+1)-f(m)} & ,f(m) < k \le f(m+1) \\ 0 & ,k > f(m+1) \end{cases} \quad (2\text{-}6)$$

โดยที่ m มีค่าอยู่ระหว่าง 0 ถึง M - 1

5) Discrete Cosine Transforms (DCT): ตามที่ระดับพลังงานเสียงในแถบที่อยู่ติดกันมีแนวโน้มที่จะมีความสัมพันธ์กันดังนั้นวิธีการ DCT จะนำมาใช้ในการแปลงค่าสัมประสิทธิ์ความถี่เมล Mel เพื่อทำให้เกิดชุดของสัมประสิทธิ์ของเซ็ปสตรอล (Ceptron Coefficients) สเปกตรัม Mel มักจะถูกใช้เพื่อแสดงระดับการบันทึกก่อนการคำนวณ DCT ซึ่งส่งผลให้เกิดสัญญาณในโดเมนเซ็ปทรัลที่มีจุดสูงสุดของความถี่ (Quefrequency) ที่สอดคล้องกับพิทช์ของสัญญาณและจำนวนของรูปแบบที่แทนจุดสูงสุดของความถี่ต่ำ (Quefrequency) เนื่องจากข้อมูลสัญญาณส่วนใหญ่แสดงโดยบางส่วนของสัมประสิทธิ์ MFCC ระบบสามารถทำให้แข็งแกร่งได้โดยแยกเฉพาะค่าสัมประสิทธิ์ที่ไม่สนใจหรือตัดทอนส่วนประกอบ DCT ลำดับที่สูงกว่า และจะได้ค่าสุดท้าย MFCC จากการคำนวณตามสมการ (2-7)

$$c(n) = \sum_{m=0}^{M-1} \log_{10}\big(s(m)\big) \cos\left(\frac{\pi n(m-0.5)}{M}\right) \text{ ; n = 0,1,2,..., C-1} \quad (2\text{-}7)$$

โดยที่ *c(n)* คือค่าสัมประสิทธิ์เซ็ปสตรอล (Cepstral Coefficients) และ C คือจำนวนของ MFCC โดยทั่วไปแล้ว MFCC จะใช้ค่าสัมประสิทธิ์เซ็ปสตรอล (Cepstral Coefficients) จำนวน 8 ถึง 13 ค่า โดยที่ค่าสัมประสิทธิ์ตำแหน่งที่ศูนย์มักไม่นำมาใช้เนื่องจากค่านี้แสดงถึงค่าเฉลี่ยของล็อกเอนเนอร์ยี (Log-energy) ของสัญญาณอินพุตที่แสดงข้อมูลเฉพาะของผู้พูดเพียงเล็กน้อยเท่านั้น

6) MFCC Features: โดยทั่วไปสัมประสิทธิ์เซ็ปสตรอล (Cepstral Coefficients) มีคุณลักษณะแบบคงที่ เนื่องจากจะมีเฉพาะข้อมูลจากเฟรมที่กำหนดเท่านั้น ข้อมูลเพิ่มเติมเกี่ยวกับพลวัตชั่วขณะของสัญญาณได้มาจากการคำนวณอนุพันธ์อันดับหนึ่งและสองของสัมประสิทธิ์เซ็ปสตรอล โดยที่อนุพันธ์อันดับหนึ่งเรียกว่าสัมประสิทธิ์เดลต้า (Delta Coefficients) และอนุพันธ์อันดับสองเรียกว่าสัมประสิทธิ์เดลต้า-เดลต้า (Delta-Delta Coefficients) ค่าสัมประสิทธิ์เดลต้าเป็น

มหาวิทยาลัยรังสิต Rangsit University

ค่าที่บอกเกี่ยวกับอัตราการพูด และค่าสัมประสิทธิ์เดลต้า–เดลต้าให้ข้อมูลเกี่ยวกับการเร่งความเร็วของคำพูดซึ่งหาค่าได้มาจากอนุพันธ์อันดับหนึ่งของสัมประสิทธิ์เดลต้า สมการที่ (2-8) ใช้ในการคำนวณพารามิเตอร์แบบพลวัตคือ

$$\Delta c_{m(n)} = \frac{\sum_{i=-T}^{T} k_i c_m(n+i)}{\sum_{i=-T}^{T} |i|} \tag{2-8}$$

โดยที่ cm(n) หมายถึง คุณลักษณะที่ m^{th} ของตำแหน่งเฟรมที่ n^{th} ส่วน k_i ค่านำหนักที่ตำแหน่งที่ i และ T คือจำนวนเฟรมที่เรียงต่อเนื่องกันสำหรับการคำนวณ โดยทั่วไปมีค่าเท่ากับ 2

รูปที่ 2.18 การรวมชีวมิติ (Biometric Fusion)

ที่มา: Jain et al., 2011

มหาวิทยาลัยรังสิต Rangsit University

การรวมชีวมิติ (Biometric Fusion)

ในกระบวนการพิสูจน์ตัวจริง (Authentication Process) เมื่อผู้ใช้ป้อนข้อมูลชีวมิติทั้งข้อมูลเสียงและข้อมูลภาพใบหน้าเข้าสู่ระบบ ระบบจะทำการเปรียบเทียบเทมเพลตข้อมูลชีวมิติที่รับเข้ามากับเทมเพลตชีวมิติที่ระบบได้ทำการเรียนรู้มาแล้ว ผลการเปรียบเทียบของชีวมิติจะออกมาในรูปแบบค่าของคะแนนการพยากรณ์ (Confident Score) เป็นตัวเลขร้อยละของความใกล้เคียงกัน แล้วนำผลคะแนนของการเปรียบเทียบชีวมิติทั้งสองแบบมาหาค่าผลรวมสุดท้ายของการ

เปรียบเทียบ (Fusion Score) ดังรูปที่ 2.18 ซึ่งมี 2 แนวทาง ประกอบด้วย การค่าชีวมิติก่อนการเปรียบเทียบ (Prior Matching) และ การค่าชีวมิติหลังการเปรียบเทียบ (After Matching)

การค่าชีวมิติก่อนการเปรียบเทียบ (Prior Matching) เป็นการนำค่าชีวมิติแต่ละแบบนำมารวมกันก่อนการนำไปเปรียบเทียบกับค่าของคุณลักษณะเด่นที่ได้บันทึกไว้ในฐานข้อมูล สามารถแบ่งได้เป็น 2 แบบคือค่าชีวมิติที่ได้มาจากเซนเซอร์ที่ทำหน้าที่รับข้อมูลชีวมิติเข้าสู่ระบบ (Sensor Level) และ ค่าชีวมิติที่ได้มาจากการหาคุณลักษณะเด่น (Feature Level) ส่วนการค่าชีวมิติหลังการเปรียบเทียบ (After Matching) เป็นการนำค่าชีวมิติแต่ละแบบนำมารวมกันหลังจากการนำไปเปรียบเทียบกับค่าของคุณลักษณะเด่นที่ได้บันทึกไว้ในฐานข้อมูล สามารถแบ่งได้เป็น 3 แบบคือ ค่าชีวมิติที่ได้มาจากผลการเปรียบเทียบข้อมูลชีวมิติ (Score Level) ค่าชีวมิติที่ได้มาจากผลการเปรียบเทียบข้อมูลชีวมิติ การจัดทำลำดับ (Rank Level) และค่าชีวมิติที่ได้มาจากผลการตัดสินใจของข้อมูลชีวมิติแต่ละชนิด (Decision Level)

รูปที่ 2.19 การหาการรวมชีวมิติแบบ Score Fusion

ที่มา: Jain et al., 2011

การวิจัยนี้ใช้การค่าชีวมิติหลังการเปรียบเทียบ (After Matching) เป็นการนำค่าชีวมิติแต่ละแบบนำมารวมกันหลังจากการนำไปเปรียบเทียบกับค่าของคุณลักษณะเด่นที่ได้บันทึกไว้ในฐานข้อมูล (Score Level) ดังรูปที่ 2.19 หากค่าผลรวมสุดท้ายมีค่ามากกว่าขอบเขตขั้นต่ำที่กำหนดไว้คือร้อยละ 60 ระบบจะถือว่าการพิสูจน์ตัวจริงของผู้เข้าสอบถูกต้องและจะอนุญาตให้เข้าสอบออนไลน์ได้ ดังรูปที่4.7 แต่หากค่าผลรวมสุดท้ายมีค่าน้อยกว่าขอบเขตขั้นต่ำที่กำหนดไว้คือร้อยละ 60 ระบบจะถือว่าการพิสูจน์ตัวจริงของผู้เข้าสอบไม่ถูกต้องและจะไม่อนุญาตให้เข้าสอบออนไลน์

ได้ อย่างไรตามเนื่องจากการป้อนข้อมูลชีวมิติภายใต้สภาพแวดล้อมที่แตกต่างกัน ตัวอย่างเช่น สภาพแสงน้อยหรือมากเกินไป มุมกล้อง ระยะห่างของกล้อง ความคมชัดหรือความคลาดเคลื่อนของเซนเซอร์ รวมถึงอาจมีเสียงรบกวนการป้อนข้อมูลเสียงได้เช่นกัน ซึ่งอาจส่งผลให้ผลการรู้จำมีความคลาดเคลื่อนได้ ระบบนี้จึงได้มีการออกแบบให้รองรับเงื่อนไขความแตกต่างของสภาพแวดล้อมที่อาจแตกต่างกัน โดยยังคงรองรับการพิสูจน์ตัวจริงด้วยการใช้รหัสผ่านเพื่อเข้าสู่ระบบ

2.3 คอมพิวเตอร์วิทัศน์ (Computer Vision)

คอมพิวเตอร์วิทัศน์เป็นสาขาวิชาหนึ่งที่เกี่ยวข้องกับการได้มา การประมวลผล และการวิเคราะห์ภาพจากฟังก์ชันเหล่านี้คอมพิวเตอร์วิทัศน์พยายามดึงข้อมูลที่เป็นประโยชน์ออกจากภาพให้ได้มากที่สุด ซึ่งสามารถนำผลการวิเคราะห์ไปใช้ในการตัดสินใจด้านต่าง ๆ ได้ การประยุกต์ใช้คอมพิวเตอร์วิทัศน์ที่นิยมคือการค้นหาวิธีการที่สามารถทำให้คอมพิวเตอร์มีความสามารถเหมือนมนุษย์ในการทำความเข้าใจภาพและลดข้อมูลที่ไม่เป็นประโยชน์ออกไป คอมพิวเตอร์วิทัศน์สามารถนำไปใช้ในระบบการขับขี่อัตโนมัติ การจดจำวัตถุ ตลอดจนการจัดการคุณภาพของผลิตภัณฑ์ และงานด้านอื่น ๆ

ศาสตร์ด้านคอมพิวเตอร์วิทัศน์มีการเติบโตอย่างมากในช่วงหลายทศวรรษที่ผ่านมา ปัจจุบันมีไลบรารีเพิ่มจำนวนมากขึ้นเพื่อใช้สำหรับแอปพลิเคชันที่เกี่ยวข้องกับระบบคอมพิวเตอร์วิทัศน์ การใช้คอมพิวเตอร์วิทัศน์อย่างแพร่หลายเกิดขึ้นได้ด้วยการผสมผสานขั้นตอนวิธีที่มีความสามารถมากขึ้น ฮาร์ดแวร์ที่ถูกลงและทรงพลังมากขึ้นและคุณสมบัติของกล้องที่ดีกว่าแต่ก่อนเป็นอย่างมาก

2.3.1 OpenCV

OpenCV เป็นไลบรารีทางซอฟต์แวร์ที่ใช้ในการประมวลผลภาพ (Image Processing) สำหรับการเรียนรู้ของเครื่อง (Machine Learning) แบบเปิดเผยชุดคำสั่ง (Open Source) ที่ได้รับอนุญาตจาก BSD-License ทำให้ให้สะดวก ง่ายต่อการใช้งานและสามารถแก้ไขหรือเปิดเผยชุดคำสั่ง ต้นฉบับได้ OpenCV ได้รับการพัฒนาเพื่อรองรับการนำไปประยุกต์ใช้งานของ

แอปพลิเคชันการมองเห็นของคอมพิวเตอร์และเพื่อกระตุ้นการใช้การรับรู้ของเครื่องในแอปพลิเคชันที่ใช้งานได้ในเชิงพาณิชย์ งานวิจัย และงานด้านต่าง ๆ ไลบารีของ OpenCV นั้นมีขั้นตอนวิธีขั้นสูงมากกว่า 2,500 รายการ รวมถึงชุดที่ครอบคลุมของการมองเห็นของคอมพิวเตอร์พื้นฐานและขั้นสูงและขั้นตอนวิธีการเรียนรู้ของเครื่อง ขั้นตอนวิธีของ OpenCV สามารถนำไปประยุกต์ใช้งานได้หลายด้าน ตัวอย่างเช่น การรู้จำด้วยใบหน้า การระบุออปเจคต่าง ๆ การแยกแบบจำลองวัตถุ 3 มิติ การผลิตภาพวัตถุ 3 มิติจากกล้องสามสมิติผ่านระบบคลาวด์ การตัดต่อภาพเพื่อสร้างภาพที่มีความละเอียดสูง การค้นหาภาพที่คล้ายคลึงกันจากฐานข้อมูลภาพ การลบตาแดงออกจากภาพที่ถ่ายที่ใช้แฟลช การจดจำทิวทัศน์ และการสร้างเครื่องหมายเพื่อซ้อนทับกับภาพจริง เป็นต้น นอกจากนี้ OpenCV เป็นส่วนที่สำคัญในแอปพลิเคชันด้านการมองเห็นแบบเรียลไทม์โดยใช้ประโยชน์จากชุดคำสั่ง MMX และ SSE ที่มีอยู่ในหน่วยประมวลผล และยังมีการพัฒนาส่วนประสานกับคูดา (CUDA) และ Open CL อย่างต่อเนื่อง ซึ่งช่วยเพิ่มสมรรถนะการประมวลผลภาพ (Image Processing) ให้มีความรวดเร็วมากยิ่งขึ้น

ไลบรารีของ OpenCV ถูกพัฒนาด้วยภาษา C และ C++ โดยมีจุดมุ่งหมายเพื่อเป็นไลบรารีที่สามารถข้ามแพลตฟอร์มและข้ามภาษาได้ ไลบรารีของ OpenCV สนับสนุนภาษาเขียนโปรแกรมหลายภาษา ตัวอย่างเช่น Python C++ หรือ Java และสนับสนุนระบบปฏิบัติการ ตัวอย่างเช่น Windows, Linux, Mac OS X, Android และ iOS เป็นต้น ขั้นตอนวิธีของ OpenCV ได้รับการปรับให้เหมาะสมและมีประสิทธิภาพด้วยการใช้ภาษา C ซึ่งช่วยให้สามารถใช้ประโยชน์จากคุณสมบัติของหน่วยประมวลผลหลักและหน่วยประมวลผลด้านกราฟิก ตัวอย่างเช่น คูดา (CUDA) ซึ่งเป็นแพลตฟอร์มสำหรับการประมวลผลแบบขนานบน GPU ของ NVIDIA คอมพิวเตอร์สมัยใหม่มีการใช้คูดา (CUDA) มากกว่า 375 ล้านตัวซึ่งช่วยให้นักพัฒนาสามารถเรียกใช้ขั้นตอนวิธีของตนบน GPU ได้อย่างมีประสิทธิภาพสูงมากขึ้น

OpenCV มีการเชื่อมโยงกับ GitHub ซึ่งเครื่องที่ให้บริการเก็บชุดคำสั่งต้นฉบับ ผู้ใช้สามารถใช้บริการ ทำสำเนา แยก หรือดาวน์โหลดต้นฉบับได้ นอกจากนี้ผู้ที่มีส่วนเกี่ยวข้องใช้ในการแจ้งปัญหาและการแจ้งปัญหาเกี่ยวกับการทำงานที่ขาดหายไปหรือข้อผิดพลาดเกิดขึ้นบน GitHub ด้วย นักพัฒนาสามารถร้องขอการมีส่วนร่วมในโครงการได้ หากผู้พัฒนาที่ไม่ต้องการแก้ไขชุดคำสั่งต้นฉบับก็สามารถเข้าถึง OpenCV ได้จากหน้าเว็บของ OpenCV หรือ Sourceforge

มหาวิทยาลัยรังสิต Rangsit University

2.3.2 มุมมองเชิงบริบทของ OpenCV (Context View of OpenCV)

มุมมองเชิงบริบทของ OpenCV เป็นแผนภาพเพื่อกำหนดความสัมพันธ์ (Relationships) การมีปฏิสัมพันธ์ (Interactions) และการขึ้นต่อกัน (Dependencies) ระหว่าง OpenCV และสภาพแวดล้อมในบริบทของการประยุกต์ใช้งาน มุมมองเชิงบริบทนี้แสดงภาพรวมอย่างกว้าง ๆ ของทั้งระบบและดังนั้นจึงมีประโยชน์สำหรับผู้ที่เกี่ยวข้องทั้งหมด โมเดลมุมมองเชิงบริบทสำหรับ OpenCV แสดงในรูปที่ 2.20

รูปที่ 2.20 มุมมองเชิงบริบทสำหรับ OpenCV

ที่มา: Johannsson, Kashyap, & Manjappa, 2016

OpenCV มีโครงสร้างเป็นแบบโมดูลหลาย ๆ โมดูล ดังรูปที่ 2.21 ซึ่งมีข้อดีคือช่วยให้มีความยืดหยุ่นการการพัฒนาหรือการนำไปประยุกต์ใช้ได้อย่างรวดเร็ว บางส่วนของโมดูลจะมีความเป็นอิสระต่อกัน (Loosely Coupled) ช่วยให้กรณีที่เกิดปัญหากับบางโมดูลจะไม่กระทบต่อโมดูลอื่นในระบบ อย่างไรก็ตามบางส่วนของโมดูลจะมีความขึ้นต่อกัน (Tightly Coupled) เพื่อช่วยให้เกิด

การใช้แบ่งปันทรัพยากรร่วมกันได้ระหว่างโมดูลอีกทั้งยังช่วยลดความซ้ำซ้อนของโมดูลต่าง ๆ อีกด้วย ตัวอย่างบางส่วนของโมดูล

ฟังก์ชันหลัก (Core Functionality) เป็นโมดูลหลักที่มีขนาดเล็กใช้เพื่อกำหนดโครงสร้างข้อมูลพื้นฐาน รวมถึง Mat ซึ่งเป็นอาร์เรย์แบบหลายมิติที่จัดเก็บข้อมูลอย่างหนาแน่นและฟังก์ชันพื้นฐานที่ใช้โดยโมดูลอื่น ๆ ทั้งหมด

1) โมดูลการประมวลผลภาพ (Image Processing) ชื่อ imgproc เป็นโมดูลการประมวลผลภาพที่รวมการกรองภาพเชิงเส้นและไม่เป็นเชิงเส้น (Includes Linear and Non-Linear Image Filtering) การแปลงภาพเชิงเรขาคณิต ประกอบด้วย การปรับขนาดภาพ (Resize) การสัมพันธ์กันและการบิดเบี้ยวของเปอร์สเปคทีฟ (Affine and Perspective Warping) การรีแมปแบบตารางทั่วไป การแปลงพื้นที่สี (Color Space Conversion) การปรับฮิสโตแกรม (Histograms) เป็นต้น

2) โมดูลการวิเคราะห์ภาพวีดิทัศน์ (Video Analysis) ชื่อ video เป็นโมดูลการวิเคราะห์ภาพวีดิทัศน์ ประกอบด้วยส่วนของการประมาณการเคลื่อนไหว การลบพื้นหลัง และขั้นตอนวิธีการติดตามวัตถุ

3) โมดูลการปรับเทียบกล้องและการสร้างภาพ 3 มิติ (Camera Calibration and 3D Reconstruction) ชื่อ calib3d เป็นโมดูลประกอบด้วยขั้นตอนวิธีเรขาคณิตแบบหลายมุมมองพื้นฐาน การสอบเทียบกล้องถ่ายภาพแบบเดี่ยวและแบบสามมิติ การประมาณการท่าทางวัตถุ ขั้นตอนวิธีการโต้ตอบแบบสามมิติ และองค์ประกอบของการสร้างออปเจ็ค 3D ขึ้นมาใหม่

4) โมดูลกรอบคุณสมบัติ 2 มิติ (2D Features Framework) ชื่อ features2d เป็นโมดูลทำหน้าที่ตรวจหาลักษณะเด่น ตัวอธิบายความหมาย และตัวจับคู่ตัวอธิบายความหมาย

5) โมดูลการตรวจหาวัตถุ (Object Detection) ชื่อ objdetect เป็นโมดูลทำหน้าที่ตรวจหาวัตถุและอินสแตนซ์ของคลาสที่กำหนดไว้ล่วงหน้า ตัวอย่างเช่น ใบหน้า ตา แก้วน้ำ คน รถ และอื่น ๆ เป็นต้น

6) โมดูลการสร้างส่วนประสานกับผู้ใช้ (High-level GUI) ชื่อ highgui เป็นโมดูลทำหน้าที่เป็นส่วนประสานสามารถใช้สร้างความเรียบง่ายแก่การสร้างส่วนประสานกับผู้ใช้งานได้ง่าย

7) โมดูลวีดีไอโอ (Video I/O) ชื่อ videoio เป็นโมดูลทำหน้าเป็นส่วนประสานสำหรับการจับภาพวิดีโอและตัวแปลงสัญญาณวิดีโอที่ใช้งานได้ง่าย

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 2.21 การขึ้นต่อกันระหว่างโมดูลของ OpenCV

ที่มา: Johannsson et al., 2016

2.3.3 มุมมองการนำไปใช้งาน (Deployment View)

มุมมองการนำไปใช้งานเป็นการมุ่งเน้นไปที่สภาพแวดล้อมขณะการรันไทม์ของระบบ รวมถึงฮาร์ดแวร์ที่จำเป็นและการจับคู่ระหว่างองค์ประกอบซอฟต์ของแวร์กับสภาพแวดล้อมของการนำไปใช้งาน OpenCV สามารถนำไปปรับใช้งานได้หลายแพลตฟอร์ม ตัวอย่างเช่น ในระบบคอมพิวเตอร์ส่วนบุคคล อุปกรณ์พกพาที่ใช้หน่วยประมวลผลอาร์ม (ARM) บนระบบปฏิบัติการไอโอเอส ระบบฝังตัวที่ใช้ระบบปฏิบัติการลินุกส์ หรือเครื่องคอมพิวเตอร์เวิร์กสเตชันที่มีราคาแพง ซึ่งสามารถมีหน่วยประมวลผลหลักและหน่วยประมวลผลกราฟิกได้จำนวนมาก

ตัวอย่างหนึ่งของการนำ OpenCV ไปประยุกต์ใช้งานด้านคอมพิวเตอร์วิทัศน์ ตัวอย่างเช่น การพัฒนาหุ่นยนต์ที่มีระบบการติดตามวัตถุซึ่งต้องมีการใช้คอมพิวเตอร์วิทัศน์ ระบบนี้ทำงานบนระบบปฏิบัติการ Ubuntu ที่ใช้ระบบปฏิบัติการที่ได้รับการออกแบบสำหรับใช้หุ่นยนต์ (Raspberry Operating System) นอกจากนี้ยังมีหน่วยประมวลผลกราฟิกที่มีคุณสมบัติคูดา (CUDA) ช่วยให้การประมวลผลชุดคำสั่งด้านกราฟิกทำได้อย่างรวดเร็วขึ้นเป็นอย่างมาก ขั้นตอนการทำงานของหุ่นยนต์มีระบบการติดตามวัตถุซึ่งต้องมีการใช้คอมพิวเตอร์วิทัศน์ ดังรูปที่ 2.22 มีดังนี้

ขั้นที่ 1 กล้อง XIMEA xiD ทำหน้าที่รับเฟรมภาพ

ขั้นที่ 2 กล้อง XIMEA xiD ส่งเฟรมภาพไปยังหน่วยประมวลผลกราฟิก

ขั้นที่ 3 หน่วยประมวลผลกราฟิกทำหน้าที่ตรวจหาวัตถุ (Object Detection)

ขั้นที่ 4 หน่วยประมวลผลกราฟิกรายงานผลการตรวจหาวัตถุ

ขั้นที่ 5 เก็บรวบรวมข้อมูลจากเซนเซอร์อื่น ๆ ตัวอย่างเช่น เซนเซอร์ตรวจหาวัตถุที่ขัดขวางการเคลื่อนที่ของหุ่นยนต์

ขั้นที่ 6 ระบบทำการตัดสินใจจากผลการตรวจหาวัตถุและข้อมูลจากเซนเซอร์ที่เกี่ยวข้อง

ขั้นที่ 7 ระบบส่งสัญญาณควบคุมไปยังหน่วยควบคุมมอเตอร์ให้ทำงานตามการตัดสินใจ

ขั้นที่ 8 ย้อนกลับไปขั้นที่ 1

รูปที่ 2.22 มุมมองการนำไปใช้งานของ OpenCV

ที่มา: Johannsson et al., 2016

2.3.4 มุมมองด้านประสิทธิภาพ (The Performance Perspective)

ประสิทธิภาพหมายถึงความสามารถของระบบในการจัดให้ผลลัพธ์ที่ต้องการภายในเวลาตอบสนองที่กำหนด ไลบรารีการประมวลผลภาพของ OpenCV จะต้องประมวลผลกับเฟรมภาพ

จำนวนมากต่อวินาที ไลบรารีการประมวลผลภาพนี้สามารถช่วยให้ได้ผลลัพธ์ที่ต้องการมีความถูกต้องและรวดเร็วเป็นการเพิ่มประสิทธิภาพการประมวลผลได้เป็นอย่างมาก นอกจากนี้ OpenCV มีคุณสมบัติหลายประการที่สามารถช่วยเพิ่มประสิทธิภาพและเพิ่มประสิทธิผลการทำงานอย่างไรก็ตามการเพิ่มประสิทธิภาพเหล่านี้ขึ้นอยู่กับปัจจัยสภาพแวดล้อมหลายด้านด้วยเช่นกัน ตัวอย่างเช่น สถาปัตยกรรมหน่วยประมวลผล ระบบปฏิบัติการ และภาษาที่ใช้ในการพัฒนา เป็นต้น

ฟังก์ชันหลายฟังก์ชันของ OpenCV สามารถปรับคุณสมบัติการเพิ่มประสิทธิภาพการทำงานให้เหมาะสมที่แตกต่างกันได้ การใช้ประโยชน์จากคุณสมบัติเหล่านี้จะทำได้หากการทำงานในระยะรันไทม์รองรับ อย่างไรก็ตามฟังก์ชันของ OpenCV ยังมีชุดคำสั่งที่ไม่ได้รับการปรับให้เหมาะสมเนื่องจากระบบที่นำไปใช้งานอาจไม่รองรับคุณสมบัติในการเพิ่มประสิทธิภาพนี้ ฟังก์ชัน cv2.useOptimized() สามารถใช้เพื่อตรวจสอบว่ามีการเปิดใช้งานหรือปิดใช้งานการปรับคุณสมบัติการเพิ่มประสิทธิภาพ และ cv2.setUseOptimized() เพื่อเปิดใช้งานหรือปิดใช้งาน การปรับคุณลักษณะการเพิ่มประสิทธิภาพให้เหมาะสมดังแสดงอยู่ในตารางที่ 2.2

ตารางที่ 2.2 ตารางแสดงคุณสมบัติการเพิ่มประสิทธิภาพใน OpenCV

คุณลักษณะ	คำอธิบาย	ความพร้อมใช้งาน
SSE2/3	ย่อมาจาก Streaming SIMD Extensions 2/3 เป็นกลุ่มของชุดคำสั่งทางด้านมัลติมีเดียที่อยู่ในไลบรารี SIMD ของหน่วยประมวลอินเทล เป็นคุณสมบัติที่ทำให้หนึ่งคำสั่งสามารถประมวลผลข้อมูลได้หลายข้อมูล	Intel Chipsets
NEON	ออกแบบมาเพื่อใช้เฉพาะกับหน่วยประมวลผล ARM เพื่อเร่งความเร็วขั้นตอนวิธีการประมวลผลข้อมูลมัลติมีเดีย ตัวอย่างเช่น การเข้ารหัส/ถอดรหัสวิดีทัศน์ กราฟิก 2D/3D การเล่นเกม การประมวลผลเสียงและภาพ เป็นต้น	ARMv6

มหาวิทยาลัยรังสิต Rangsit University

ตาราง 2.2 ตารางแสดงคุณสมบัติการเพิ่มประสิทธิภาพใน OpenCV (ต่อ)

คุณลักษณะ	คำอธิบาย	ความพร้อมใช้งาน
IPP	Integrated Performance Primitives (Intel® IPP) เป็นไลบรารีสำหรับการพัฒนาแอปพลิเคชันการประมวลผลข้อมูลและการสื่อสาร ฟังก์ชันเหล่านี้ได้รับการปรับแต่งให้มีประสิทธิภาพสูงขึ้นโดยใช้ส่วนขยายของอินเทล Streaming SIMD	OpenCV 3.0 on Intel Chipsets
OpenCL	Open Computing Language (OpenCL) เป็นมาตรฐานเปิดสำหรับการเขียนชุดคำสั่งให้สามารถทำงานข้ามแพลตฟอร์มที่แตกต่างกัน รวมถึงหน่วยประมวลผลหลัก และหน่วยประมวลผลกราฟิก OpenCL ให้แอปพลิเคชันสามารถเข้าถึงหน่วยประมวลผลกราฟิกเพื่อการประมวลผลที่ไม่ใช่กราฟิก (GPGPU) ส่งผลให้มีความเร็วการประมวลผลเพิ่มขึ้นเป็นอย่างมาก	All Platforms
CUDA	CUDA เป็นแพลตฟอร์มการประมวลผลแบบขนานและโมเดลของแอปพลิเคชันการเขียนโปรแกรมส่วนประสาน (API) สร้างโดย NVIDIA เพื่อดำเนินการประมวลผลภาพบน NVIDIA GPUs	NVIDIA GPUs

ที่มา: Johannsson et al., 2016

ผลการทดสอบประสิทธิภาพการประมวลผลคูดา (CUDA) ซึ่งเป็นแพลตฟอร์มการประมวลผลแบบขนานเทียบกับหน่วยประมวลผลหลัก ดังรูปที่ 2.23 พบว่าการประมวลผลภาพโดยใช้คูดาประมวลผลได้เร็วกว่าการประมวลผลโดยใช้หน่วยประมวลผลหลัก 30 เท่า การดำเนินการภาพสามมิติโดยใช้คูดาประมวลผลได้เร็วกว่าการประมวลผลโดยใช้หน่วยประมวลผลหลัก 7 เท่า การตรวจจับภาพคนเดินถนนโดยใช้คูดาประมวลผลได้เร็วกว่า

การประมวลผลโดยใช้หน่วยประมวลผลหลัก 8 เท่า การตรวจหาภาพใบหน้าของ Viola-Jones การประมวลผลภาพโดยใช้ คูดา ประมวลผลได้เร็วกว่าการประมวลผลโดยใช้หน่วยประมวลผลหลัก 6 เท่า และงานด้านการเร่งความเร็ว SURF (Speeded up Robust Features Keypoints) การประมวลผลภาพโดยใช้คูดาประมวลผลได้เร็วกว่าการประมวลผลโดยใช้หน่วยประมวลผลหลัก 12 เท่า

รูปที่ 2.23 รูปแสดงประสิทธิภาพที่เพิ่มขึ้นจากการใช้ CUDA

ที่มา: Johannsson et al., 2016

มหาวิทยาลัยรังสิต Rangsit University

2.4 ทบทวนวรรณกรรม

ตารางที่ 2.3 แสดงการสรุปผลการทบทวนวรรณกรรมที่เกี่ยวข้องกับการวิจัยด้านการศึกษาชีวมิติ มีจำนวน 35 ผลงาน จะพบว่าเป็นงานวิจัยที่ใช้การพิสูจน์ตัวจริงโดยใช้ชีวมิติแบบหลายวิธี (Multi Modal Biometric) จำนวน 26 ผลงาน และเป็นงานวิจัยที่ใช้การพิสูจน์ตัวจริงโดยใช้ชีวมิติแบบวิธีเดียว (Single Modal Biometric) จำนวน 9 ผลงาน นอกจากนี้หากพิจารณาด้านการนำชีวมิติไปประยุกต์ใช้ ได้ดังนี้ การประยุกต์กับงานด้านสุขภาพ (Healthcare) จำนวน 3 ผลงาน ด้านเทคโนโลยีบล็อกเชน (Blockchain) จำนวน 1 ผลงาน ด้านเกี่ยวกับกฎหมาย (Law Enforcement) จำนวน 2 ผลงาน ด้านอินเทอร์เน็ตของสรรพสิ่ง (IoTs) จำนวน 2 ผลงาน ด้านสัตว์เลี้ยงหรือปศุสัตว์ (Livestock) จำนวน 1 ผลงาน ด้านการรักษาความปลอดภัยหรือการเข้ารหัส (Security) จำนวน 17 ผลงาน และด้านการวัดสมรรถนะ (Performance) จำนวน 7 ผลงาน

จากการทบทวนวรรณกรรมพบว่าระบบชีวมิติแบบเดียว (Single Modal Biometric) มีข้อจำกัดในการนำไปประยุกต์ใช้งาน โดยซึ่งแต่ละระบบมีการจัดอันดับตามค่าเจ็ดประการตามที่ Jain et al. (2011) นำเสนอ จากการศึกษาจะพบว่าระบบชีวมิติแบบเดี่ยวแต่ละแบบยังมีจุดอ่อนในเรื่องสภาพแวดล้อมการใช้งานที่ไม่ดี สัญญาณรบกวนจากเซนเซอร์ และปัจจัยอื่น ๆ ที่ส่งผลต่อความแม่นยำ ความน่าเชื่อถือได้ และความแข็งแกร่งของระบบชีวมิติแบบเดี่ยว นอกจากนี้การศึกษาโดยใหญ่จะทำการศึกษาเพื่อเปรียบเทียบวิธีการหรือเทคนิคในการพิสูจน์ตัวจริงด้วยวิธีการต่าง ๆ เพื่อหาวิธีหรือแนวทางการพิสูจน์ตัวจริงที่น่าจะดีที่สุด ปลอดภัยที่สุด ทั้งการพิสูจน์ตัวจริงด้วยตัวเลขส่วนบุคคล (PIN) หรือรหัสโดยใช้ การใช้อุปกรณ์ฮาร์ดแวร์เฉพาะ (Device/Token-based Authentication) หรือการพิสูจน์ตัวจริงโดยใช้ชีวมิติ (Biometric Authentication) นอกจากนี้พบว่าการศึกษาของ Rokita, Krzyzak, & Suen (2008) ที่เสนอความเห็นว่าการพิสูจน์ตัวจริงยังไม่มีวิธีการที่สมบูรณ์ที่สุดจึงควรใช้การพิสูจน์ตัวจริงหลาย ๆ แบบผสมผสานกันโดยใช้จุดเด่นของแต่ละวิธีเพื่อให้ได้การพิสูจน์ตัวจริงที่มีความปลอดภัยมากขึ้นกว่าการใช้วิธีการพิสูจน์ตัวจริงเพียงวิธีใดวิธีหนึ่งเพียงแบบเดียว

จากการทบทวนวรรณกรรมจะเห็นได้ว่าการศึกษาและวิจัยด้านชีวมิติเพียงอย่างเดียวมีแนวโน้มลดลง ส่วนการการศึกษาและวิจัยด้านชีวมิติแบบหลายวิธีมีแนวโน้มเพิ่มขึ้นทั้งนี้อาจมีสาเหตุมาจากปัจจุบันมีแนวโน้มการบุกรุก การโจมตี หรือการขโมยข้อมูลในระบบสารสนเทศผ่านระบบเครือข่ายมีจำนวนเพิ่มขึ้นเป็นอย่างมาก สร้างความเสียหายและผลกระทบเป็นอย่างมาก ทำให้ผู้ใช้งานบางส่วนเกิดความไม่มั่นใจต่อข้อมูลส่วนบุคคลที่อาจเป็นข้อมูลที่มีความสำคัญ ตัวอย่างเช่น ข้อมูลทางด้านสุขภาพ ข้อมูลทางการเงิน หรือข้อมูลที่ต้องการให้เป็นความลับส่วนบุคคล จะเห็นได้ว่างานวิจัยส่วนใหญ่มุ่งเน้นไปที่การศึกษาค้นคว้าด้านการรักษาความปลอดภัยรวมถึงการเข้ารหัส (Security and Encryption) เพื่อเป็นการหาแนวทางการป้องกันการเข้าถึงและการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาตหรือเอาข้อมูลส่วนบุคคลไปใช้อย่างไม่ถูกต้อง อย่างไรก็ตามการคุกคามทางไซเบอร์ (Cyber Crime) ยังคงเป็นภัยคุกคามที่การพัฒนารูปแบบหรือวิธีการอย่างต่อเนื่อง ดังนั้นการศึกษาค้นคว้าและการวิจัยเพื่อเป็นการแนวทางการป้องกันการเข้าถึงและการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาตหรือเอาข้อมูลส่วนบุคคลไปใช้อย่างไม่ถูกต้องยังคงต้องดำเนินการอย่างต่อเนื่องและต้องมความเข้มแข็งเพิ่มมากยิ่งขึ้น

จะเห็นได้ว่างานวิจัยที่ได้ศึกษามาข้างต้นต่างมีความเห็นสอดคล้องกันว่าความปลอดภัยของการเข้าใช้บริการของการประมวลผลแบบคลาวด์เป็นสิ่งที่จำเป็นมากเนื่องจากบริการของ

มหาวิทยาลัยรังสิต Rangsit University

การประมวลผลแบบคลาวด์นั้นสามารถทำได้โดยใช้ทางระบบเครือข่ายอินเทอร์เน็ต การเข้าถึงบริการหรือข้อมูลจากผู้ไม่ที่ไม่ได้รับอนุญาตอาจทำให้เกิดความสูญเสียที่ไม่สามารถประเมินค่าได้ นอกจากนี้พบว่าปัจจุบันการใช้งานอุปกรณ์เคลื่อนที่ ตัวอย่างเช่น มือถือหรือแท็ปเล็ต มีปริมาณเพิ่มขึ้นอย่างมาก ซึ่งก็สามารถใช้ในการเข้าถึงและเข้าใช้บริการของการประมวลผลแบบคลาวด์ได้เช่นกัน กระบวนการพิสูจน์ตัวจริงจึงเป็นกระบวนการหนึ่งที่ใช้ในการป้องกันความปลอดภัยของผู้ที่จะเข้าใช้งานโดยใช้ทางระบบเครือข่าย ระบบชีวมิติแบบหลายรูปแบบ (Multimodal Biometric) ซึ่งเป็นการประยุกต์ใช้ชีวมิติหลายรูปแบบมาผสมผสานกัน โดยช่วยให้สามารถระบุสถานการณ์ความล้มเหลวจุดเดียวสำหรับระบบชีวมิติ และสร้างระบบชีวมิติที่มีประสิทธิภาพมากขึ้น การวิจัยครั้งนี้มุ่งเน้นการใช้ระบบชีวมิติแบบหลายรูปแบบโดยจะเป็นการผสมผสานระหว่างชีวมิติจากเสียงพูดและจากภาพใบหน้า

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Atmakuri (2015)	นำเสนอกรอบงานที่พัฒนาขึ้นโดยใช้การพิสูจน์ตัวจริงโดยใช้ใบหน้าในการเข้าใช้งานระบบคลาวด์	ชีวมิติแบบเดี่ยว ใช้ ใบหน้า	โมไบล์ คลาวด์
Rokita et al. (2008)	เคลื่อนที่ ผู้วิจัยเห็นว่าควรจะมีวิธีการพิสูจน์ตัวจริงมากกว่าหนึ่งวิธีที่สามารถนำมาใช้รวมกันเพื่อเสริมความปลอดภัยของการพิสูจน์ตัวจริงให้เข้มแข็งมากขึ้น ในการศึกษานี้ผู้วิจัยเน้นศึกษาไปที่การพิสูจน์ตัวจริงโดยใช้ใบหน้าและมือ	มัลติโมดัลใช้ใบหน้าและมือ	โมไบล์ คลาวด์
Romo (2014)	ผู้วิจัยได้นำเสนอกรอบงาน (Framework) สำหรับการพิสูจน์ตัวจริงบนอุปกรณ์เคลื่อนที่ ประกอบด้วย 5 ส่วนคือ RFID Manager, Encryption Layer, Policy Manager, Hardware Key และ Device ID	ชีวมิติแบบเดี่ยว ใช้ Physical Smart Key	โมไบล์
Ahn, Chang, Jang, & Choi (2011)	ผู้วิจัยจึงได้นำเสนอแพลตฟอร์มที่ใช้ในการพิสูจน์ตัวจริงโดยใช้ User Profile โดยใช้	ชีวมิติแบบเดี่ยว	คลาวด์

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
	แนวคิด Provisioning in Cloud Computing Environment พิสูจน์ตัวจริง		
Ahn, Chang, Jang, & Choi (2011)	ผู้วิจัยจึงได้นำเสนอแพลตฟอร์มที่ใช้ในการพิสูจน์ตัวจริงโดยใช้ User Profile โดยใช้แนวคิด Provisioning in Cloud Computing Environment พิสูจน์ตัวจริง	ชีวมิติแบบเดี่ยว	คลาวด์
Sharma & Mittal (2013)	ผู้วิจัยได้เน้นไปที่การเปรียบเทียบเทคนิคของการพิสูจน์ตัวจริงเพื่อใช้ในการตรวจสอบการระบุตัวตนของผู้ใช้บริการกับ Cloud Broker ผลการวิจัยสรุปเทคนิคการพิสูจน์ตัวจริงเพื่อใช้กับการประมวลผลแบบคลาวด์นั้นมี 3 วิธีหลักคือ 1) Authentication using Kerberos 2) Authentication using Key Distribution Center และ 3) Authentication using Public Key Infrastructure		คลาวด์
Peer, Bule, Gros, & Štruc (2013)	ผู้วิจัยได้นำการพิสูจน์ตัวจริงโดยใช้ชีวมิติในการใช้บริการประมวลผลแบบคลาวด์ไปปฏิบัติจริงกับระบบการจัดการการเรียนการสอนด้วยแอปพลิเคชัน Moodle	ชีวมิติแบบเดี่ยว	คลาวด์
Shakil, Zareen, Alam, & Jabin, (2020)	นักวิจัยได้เสนอการพิสูจน์ตัวจริงเชิงพฤติกรรมโดยใช้ลายเซ็นของผู้ป่วยแต่ละรายโดยระบบการพิสูจน์ตัวจริงนี้จะทำงานอยู่บนระบบการประมวลผลแบบคลาวด์	ชีวมิติแบบเดี่ยว ใช้ลายเซ็น	คลาวด์
Shakil, Zareen, Alam, & Jabin, (2020)	นักวิจัยได้เสนอการพิสูจน์ตัวจริงเชิงพฤติกรรมโดยใช้ลายเซ็นของผู้ป่วยแต่ละรายโดยระบบการพิสูจน์ตัวจริงนี้จะทำงานอยู่บนระบบการประมวลผลแบบคลาวด์	ชีวมิติแบบเดี่ยว ใช้ลายเซ็น	คลาวด์

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Errattahia, Hannania, & Ouahmane (2018)	นักวิจัยให้ความสำคัญกับการแก้ไขข้อผิดพลาดระบบการรู้จำเสียงแบบอัตโนมัติ เพื่อทำให้ระบบมีประสิทธิภาพใช้งานได้และทนทานต่อการใช้งานในสภาพแวดล้อมต่าง ๆ เพิ่มมากขึ้น	ชีวมิติแบบเดี่ยว ใช้เสียง	
Bah & Ming (2020)	ผู้วิจัยเสนอวิธีการใหม่ในการแก้ไขความเที่ยงตรงของระบบจดจำใบหน้าโดยผสานขั้นตอนวิธี Local Binary Pattern เข้ากับเทคนิคการประมวลผลภาพ ตัวอย่างเช่น การเปรียบเทียบความแตกต่างของแสงความสว่าง หรือการปรับฮิสโตแกรม เพื่อช่วยให้ระบบรู้จำใบหน้ามีความแม่นยำ ความน่าเชื่อถือได้ และความแข็งแกร่งเพิ่มมากยิ่งขึ้น	ชีวมิติแบบเดี่ยว ใช้ใบหน้า	
Mason, Dave, Chatterjee, Allen, Esterline, & Roy (2020)	ผู้วิจัยเสนอแนวทางใหม่ที่ใช้การผสมผสานชีวมิติบริเวณรอบดวงตาร่วมกับหมายเลขดัชนีจากระบบสารสนเทศของผู้ป่วยในระบบข้อมูลด้านการดูแลสุขภาพเพื่อใช้ในการแยกแยะผู้ป่วยแต่ละราย	ชีวมิติแบบเดี่ยว บริเวณรอบดวงตา	
Naidu & Babu (2018)	นำเสนอระบบการรู้จำชีวมิติหลายรูปแบบ ตัวอย่างเช่น ใบหน้า นิ้ว และเสียงเพื่อใช้ในการระบุตัวตน ระบบที่นำเสนอนี้มีความปลอดภัย และความถูกต้องแม่นยำที่ดีกว่าเมื่อเปรียบเทียบกับการระบุตัวตนโดยใช้ชีวมิติแบบเดี่ยว	มัลติโมดัลใช้ใบหน้านิ้วและเสียง	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Choudhury, Kumar, & Laskar (2021)	เสนอกรอบการทำงานสำหรับการผสานชีวมิติที่มีการจัดระดับอันดับที่ปรับเปลี่ยนได้ การจัดอันดับได้รับการปรับใช้โดยใช้เทคนิค แอนท์โคโลนีออปติไมส์เซชัน (Ant Colony Optimization) เพื่อให้เกิดประสิทธิภาพสูงสุด งานวิจัยนี้มีการปรับใช้ชีวมิติหลายรูปแบบโดยใช้การดึงคุณสมบัติของแผ่นเล็บจาก นิ้วชี้ นิ้วกลาง และนิ้วนางมารวมกัน	มัลติโมดัลใช้แผ่นเล็บจาก นิ้วชี้ นิ้วกลาง และนิ้วนาง	
Fei, Zhang, Tian, Teng, & Wen (2021)	นำเสนอการรู้จำชีวมิติโดยใช้คุณสมบัติต่าง ๆ จากมือโดยใช้หลายอินสแตนซ์ร่วมกัน นักวิจัยปรับใช้ข้อมูลเบื้องต้นจากภาพชีวมิติ คุณลักษณะที่คัดแยก และแสดงการทำงานร่วมกันของคุณลักษณะ และการรวมกันคุณลักษณะที่คัดแยกออกมาของชีวมิติแบบหลายอินสแตนซ์	มัลติโมดัลใช้แผ่นเล็บจากมือ	
Sarier (2021)	ซึ่งเป็นการพิสูจน์ตัวจริงโดยใช้ชีวมิติแบบหลายวิธีบนเทคโนโลยีมือถือและใช้ MBA-MEC เป็นรูปแบบการเข้ารหัสข้อมูลที่ใช้โปรโตคอลความปลอดภัย PPBA เพื่อต่อต้านผู้บุก	มัลติโมดัล	โมไบล์
Kumari & Thangaraj (2020)	เสนอเทคนิคชีวมิติแบบหลายวิธี บนเฟรมเวิร์กระบบคลาวด์ ประกอบด้วยการรู้จำภาพใบหน้าและการรู้จำลายนิ้วมือ เทคนิคการเลือกคุณลักษณะที่นำเสนอนี้ใช้เทคนิคแอนท์โคโลนีออปติไมส์เซชัน (Ant Colony	มัลติโมดัลใช้การรู้จำใบหน้าและการรู้จำลายนิ้วมือ	โมไบล์

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
	Optimization) ส่วนกระบวนการแยกคุณลักษณะและการจัดประเภทใช้เทคนิค Particle Swarm Optimization		
Chang, Garg, Ghosh, & Hasan (2021)	เสนอเฟรมเวิร์กแบบรวมข้อมูลชีวมิติแบบหลายรูปแบบชื่อ S-BIOFUSE ซึ่งเป็นรวมกันของ Fuzzy Commitment และ Fuzzy Vault เทคนิคทั้งสองนี้ถูกนำมาใช้เพื่อสร้างรูปแบบการรักษารูปแบบการเข้ารหัสจากข้อมูลชีวมิติทั้งหมดเพื่อเพิ่มความปลอดภัยของข้อมูลชีวมิติ เฟรมเวิร์กที่นำเสนอนี้ทำให้ผู้ที่จะเข้ามาโจมตีหรือขโมยข้อมูลทำได้ยากมากขึ้นเนื่องจากต้องเลียนแบบข้อมูลชีวมิติทั้งหมดที่เป็นข้อมูลต้นฉบับ	มัลติโมดัล	
Vijay & Indumathi (2021)	เสนอชีวมิติแบบหลายรูปแบบประกอบด้วยชีวมิติสามแบบ ได้แก่ ม่านตา (Iris) ลักษณะใบหู (Ear) และ โครงร่างเส้นเลือดของนิ้ว (Finger Vein) ซึ่งคุณสมบัติต่าง ๆ ถูกดึงออกมาโดยใช้วิธีการ Bicomp Masking จากนั้นคะแนนการรู้จำจะถูกคำนวณโดยใช้ตัวจัดหมวดหมู่ชื่อ Multi-SVNN ของชีวมิติทั้งสามลักษณะ	มัลติโมดัลใช้ม่านตา ลักษณะใบหู และโครงร่างเส้นเลือดของนิ้ว	
Kausar (2021)	นำเสนอระบบเข้ารหัสลับที่ยกเลิกได้โดยใช้ม่านตาบนบัตรสมาร์ตการ์ด (Iris-Based Cancelable Crypto System) ข้อมูลที่สำคัญส่วนบุคคลของผู้ป่วยจะถูกเข้ารหัสคีย์แบบสมมาตรและถูกจัดเก็บในรูปแบบที่เข้ารหัสบนสมาร์ทการ์ดเพื่อให้เกิดความปลอดภัยของข้อมูลส่วนบุคคล	มัลติโมดัลใช้ม่านตาบนบัตรสมาร์ตการ์ด	

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Piciucco, Lascio, Maiorana, Santini, & Campisi (2021)	เสนอการผสมผสานการรู้จำชีวมิติและอุปกรณ์สวมใส่เพื่อป้องกันการใช้งานอุปกรณ์เหล่านี้โดยไม่ได้รับอนุญาต โดยเป็นการรวมขั้นตอนวิธี EDA และ BVP Spectrograms เข้ากับ MobileNetv2	มัลติโมดัลใช้อุปกรณ์สวมใส่	
Bisogni, Iovane, Landi, & Nappi (2021)	เสนอระบบชีวมิติที่มุ่งเน้นความปลอดภัยเพื่อนำปมาประยุกต์ใช้กับการอนุญาตและลงชื่อในการทำธุรกรรมบล็อกเชน ระบบชีวมิติที่นำเสนอนี้ใช้การรู้จำภาพใบหน้าและมีการเข้ารหัสโดยใช้ CNN จากนั้นนำไปรวมกับ RSA Key	มัลติโมดัลใช้การรู้จำภาพใบหน้าและเข้ารหัส RSA Key โดยใช้ CNN จากนั้น	Blockchain
BrundhaElci, Punith, Gowda, Shivaprasad, & Buvaneshwaran (2019)	เสนอการประยุกต์ระบบการรู้จำภาพใบหน้าเพื่อใช้กับกล้องวงจรปิดเพื่อการการรู้จำอาชญากรและการติดตามบุคคลได้อย่างรวดเร็วเพื่อลดอัตราการเกิดอาชญากรรม	มัลติโมดัลใช้การรู้จำภาพใบหน้า	
Cherifi, Omar, & Amroun (2021)	เสนอระบบการยืนยันตัวแบบทันทีอย่างต่อเนื่อง โดยบันทึกกิจกรรมต่าง ๆ ของผู้ใช้โดยใช้เซนเซอร์ที่อยู่ในสมาร์ตโฟน ตัวอย่างเช่น ไจโรสโคป (Gyroscope) หรือมาตรความเร่ง (Accelerometer) เพื่อรวบรวมข้อมูลตำแหน่งหรือพิกัดของผู้ใช้ กระบวนการโดยรวมประกอบด้วย การบันทึกข้อมูลกิจกรรมของผู้ใช้ การคัดแยกคุณลักษณะที่สำคัญ การเรียนรู้ของเครื่องโดยใช้ HMM Model และ การพิสูจน์ตัวจริงของผู้ใช้	มัลติโมดัลใช้ข้อมูลกิจกรรมของผู้ใช้ เช่น ไจโรสโคป หรือมาตรความเร่ง	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Falmari & Brindha (2021)	เสนอแนวทางการเข้ารหัสให้กับข้อมูลชีวมิติเพื่อเพิ่มความปลอดภัยให้กับระบบการพิสูจน์ตัวจริงให้มากขึ้น ตัวอย่างเช่น ภาพของม่านตา ภาพใบหน้า หรือภาพลายนิ้วมือ โดยใช้ขั้นตอนวิธีแฮชขนาด 256 บิต ก่อนการส่งข้อมูลชีวมิติไปยังเครือข่าย กุญแจการเข้ารหัสถูกสร้างขึ้นจากภาพชีวมิติต้นฉบับ	มัลติโมดัลและเข้ารหัสข้อมูลชีวมิติ เช่น ภาพม่านตา ภาพใบหน้า หรือภาพลายนิ้วมือ ด้วยขั้นตอนวิธีแฮช	
Yang, Wang, Shahzad, & Zhou (2021)	นำเสนอแนวทางชื่อ Feature- adaptive Random Projection-based โดย โปรเจคชันในที่นี้หมายถึงเมทริกซ์ที่สืบทอดมาจากคุณลักษณะภายในที่มาจากเมทริกซ์พื้นฐานเมทริกซ์ โปรเจคชันหลังจากที่ถูกใช้งานแล้วจะถูกเอาออกจากระบบเพื่อป้องกันการถูกนำข้อมูลในเมทริกซ์ไปใช้อย่างอื่น	มัลติโมดัลใช้ Feature-adaptive Random Projection-based	
Saeed (2021)	เสนอแนวทางใหม่ที่ผสมผสานคุณลักษณะของซอฟท์ชีวมิติ (Soft Biometric) กับคุณลักษณะใบหน้าแบบทั่วไป ซอฟท์ชีวมิติถูกใช้เพื่อสร้างแบบจำลองไมโครเอ็กซ์เพรสชัน (Micro-expression) ส่วนลักษณะของใบหน้าทั่วไปถูกใช้เพื่อสร้างแบบจำลองโครงสร้างใบหน้า ผลการศึกษาพบว่าแนวทางที่นำเสนอนี้สามารถเพิ่มอัตราการรู้จำภาพใบหน้าประมาณร้อยละ 5	มัลติโมดัลใช้ซอฟท์ชีวมิติกับคุณลักษณะใบหน้าแบบทั่วไป	
Stylios, Kokolakis, Thanou, & Chatzis (2021)	เสนอเทคนิคการพิสูจน์ตัวจริงด้วยชีวมิติเชิงพฤติกรรมแบบต่อเนื่องโดยใช้โทรศัพท์มือถือ บทความนี้แสดงให้เห็นจุดอ่อนของโมเดลการเรียนรู้ของเครื่อง ช่วยให้เตรียมการป้องกันและมีมาตรการป้องกัน	มัลติโมดัลใช้ชีวมิติเชิงพฤติกรรมแบบต่อเนื่องโดยใช้โทรศัพท์มือถือ	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
	การโจมตีจากผู้ไม่ประสงค์ดีและมาตรการป้องกันที่เกี่ยวข้อง		
Behera, Behera, Nappi, Bakshi, & Saa (2021)	ระบบที่นำเสนอจะติดตามการเคลื่อนไหวของบุคคลในกล้องวงจรปิดหลายตัว ซึ่งช่วยลดความซับซ้อนของการพิสูจน์ตัวจริงซ้ำ ๆ ในกล้องวงจรปิดหลายตัว ในสถานการณ์เมืองอัจฉริยะที่พบว่าอินเทอร์เน็ตของสรรพสิ่ง (Internet of Biometrics things - IoBT) ถูกใช้อย่างแพร่หลายมากขึ้นโดยเฉพาะกล้องวงจรปิดอัจฉริยะซึ่งมีการรับส่งข้อมูลผ่านเครือข่ายจำนวนมาก	มัลติโมดัลใช้ภาพใบหน้าและการเคลื่อนไหว	คลาวด์
Ajish & AnilKumar (2021)	นำเสนอระบบการลงคะแนนเลือกตั้งโดยใช้การพิสูจน์ตัวจริงแบบชีวมิติซึ่งทำงานบนแอปพลิเคชันมือถือที่มีการเข้ารหัสข้อมูลเพื่อเพิ่มความปลอดภัยของข้อมูลของผู้มีสิทธิเลือกตั้ง แอปพลิเคชันบนมือถือจะประมวลผลข้อมูลภาพที่ผ่านการเข้ารหัสโดยการคัดแยกคุณลักษณะสำคัญและจัดเก็บในรูปแบบของเทมเพลตชีวมิติ แล้วทำการส่งเทมเพลตชีวมิติที่ถูกเข้ารหัสส่งบนเครือข่ายของผู้ให้บริการมือถือไปยังเครื่องบริการ เพื่อทำการประมวลผลในขั้นตอนถัดไป เพื่อเพิ่มความปลอดภัยระหว่างการส่งข้อมูลบนเครือข่ายมือถือ กระบวนการเข้ารหัสข้อมูลใช้ขั้นตอนวิธี Wavelet-based AES ซึ่งผลการศึกษาพบว่ามีสมรรถนะและให้ผลการทำงานดีกว่าการเข้ารหัสข้อมูลวิธีการอื่น	มัลติโมดัลใช้ใบหน้าและ Wavelet-based AES	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Kumar, Joshi, & Singh (2021)	นำเสนอการเข้ารหัสสองชั้นเพื่อความปลอดภัยของเทมเพลตชีวมิติ ขั้นที่หนึ่งข้อมูลจะถูกแบ่งเป็นส่วนย่อย ๆ เพื่อนำมาเป็นตัวแทนของเทมเพลตชีวมิติโดยใช้เทคนิคเวปเล็ตไม่ต่อเนื่องแบบสองมิติ (Two Dimensional Discrete Wavelet) และขั้นตอนที่สองเป็นกระบวนการแทนที่และการเปลี่ยนแปลงจะใช้เทคนิค Three Dimensional Lorenz-Chaotic System โดยทั้งสองขั้นตอนมีการเข้ารหัสข้อมูล ส่วนกระบวนการถอดรหัสจะทำการกระบวนการแบบย้อนลำดับ ผลการศึกษาพบว่าวิธีการที่นำเสนอสามารถเพิ่มความปลอดภัยอย่างเข้มแข็งจากผู้โจมตี	มัลติโมดัลใช้การเข้ารหัสสองชั้นเพื่อความปลอดภัยของเทมเพลตชีวมิติ	
Jia, Xia, Zhang, Zhao, Fei, Kang, Huang, & Guo (2021)	นำเสนองานวิจัยแบบสำรวจที่เกี่ยวข้องกับการพิสูจน์ตัวจริงด้วยชีวมิติโดยใช้โครงสร้างเส้นเลือดที่หลังมือ รายงานผลการศึกษาอธิบายกระบวนการที่เกี่ยวข้องกับการพิสูจน์ตัวจริงด้วยชีวมิติโดยใช้โครงสร้างเส้นเลือดที่หลังมือ ประกอบด้วย การเก็บข้อมูล การออกแบบโครงสร้างฐานข้อมูล กระบวนการก่อนการประมวลผล ขั้นตอนวิธีการคัดแยกคุณลักษณะเด่น ขั้นตอนวิธีการจับคู่ และการรวมคะแนนหาผลสรุป นอกจากนี้ผู้วิจัยได้บรรยายแง่มุมต่างของเทคโนโลยีการพิสูจน์ตัวจริงด้วยชีวมิติโดยใช้โครงสร้างเส้นเลือดที่หลังมือในอนาคต	มัลติโมดัลใช้โครงสร้างเส้นเลือดที่หลังมือ	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
Lee & Jeong (2021)	นำเสนอระบบ BDAS ซึ่งเป็นระบบยืนยันตัวตนด้วยชีวมิติแบบใหม่ที่ประยุกต์ใช้ร่วมกับเทคโนโลยีบล็อกเชน ระบบ BDAS มีกลไก Decentralized และ Distributed ตามแนวคิดของเทคโนโลยีบล็อกเชนและกลไกที่ใช้การตรวจสอบด้วยเพื่อใช้สำหรับการพิสูจน์ตัวจริงด้วยชีวมิติ ผู้วิจัยได้นำเสนอผลการประเมินระบบ BDAS พบว่ามีความน่าเชื่อถือได้และมีความปลอดภัย ในการพิสูจน์ตัวจริงด้วยชีวมิติเมื่อเปรียบเทียบกับกับแนวทางอื่น ๆ	มัลติโมดัลใช้ระบบยืนยันตัวตนด้วยชีวมิติแบบใหม่ที่ประยุกต์ใช้ร่วมกับเทคโนโลยีบล็อกเชน	เทคโนโลยีบล็อกเชน
Srivastva, Singh, & Singh (2021)	นำเสนอระบบการรู้จำชีวมิติโดยใช้ข้อมูลคลื่นไฟฟ้าของหัวใจซึ่งแสดงถึงกิจกรรมทางไฟฟ้าของหัวใจโดยใช้อุปกรณ์อิเล็กโทรดที่วางอยู่บนผิวหนังของคน ผู้วิจัยเสนอโมเดลชื่อ Plexnet ซึ่งเป็นการรวมโมเดลอื่น 4 ชนิดที่ผ่านการปรับแต่งแล้ว โดยผลลัพธ์ที่ได้จากโมเดลทั้ง 4 ชนิดจะนำมารวมกันเพื่อให้ได้เป็นผลลัพธ์ของโมเดลที่นำเสนอ ผลการทดสอบโมเดลที่นำเสนอกับกลุ่มข้อมูลพบว่ามีคะแนนความถูกต้องสูงสุดที่ร้อยละ 99.66 และมีความแข็งแกร่งต่อการใช้งาน	มัลติโมดัลใช้ข้อมูลคลื่นไฟฟ้าของหัวใจ	
Cui, Wang, & Li (2021)	ศึกษาการรู้จำชีวมิติโดยใช้ข้อมูลคลื่นไฟฟ้าของหัวใจซึ่งผู้วิจัยกล่าวว่าวิธีนี้เป็นเรื่องยากมากที่จะปลอมชีวมิตินี้ได้ ผู้วิจัยได้สร้างกลุ่มข้อมูลขึ้นมาเองทั้งจากขณะออกกำลังและขณะพักผ่อนเพื่อให้ได้กลุ่มข้อมูลที่มีการกระจายตัว ผู้วิจัยประเมินผลแนวคิดนี้โดยใช้	มัลติโมดัลใช้ข้อมูลคลื่นไฟฟ้าของหัวใจ	

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 2.3 ตารางสรุปการวิจัยด้านชีวมิติจากการทบทวนวรรณกรรม (ต่อ)

งานวิจัย	คำอธิบายแบบย่อ	ชีวมิติ	แพลตฟอร์ม
	ขั้นตอนวิธีหลายแบบกับกลุ่มข้อมูลที่สร้างขึ้นมา ผลการศึกษาพบว่าแนวคิดที่นำเสนอนี้ให้ผลลัพธ์เป็นน่าพอใจในสถานการณ์ที่อาจจะแตกต่างกันตามสภาพแวดล้อม		
Marquez, Ambrose, Schaefera, Cook, & Bench (2021)	นำเสนองานวิจัยระบบแจ้งเตือนการเป็นสัดที่สามารถช่วยให้เกษตรกรตรวจพบการเป็นสัดของวัวได้ เป็นการศึกษาการใช้ชีวมิติเชิงพฤติกรรมร่วมกับการถ่ายภาพความร้อนด้วยอินฟราเรดเพื่อติดตามการเป็นสัดของโคนมในฟาร์ม ระบบจะวิเคราะห์ตัวบ่งชี้การตกไข่โดยการหดตัวของรูขุมขนที่เห็นได้เด่นชัด	มัลติโมดัลใช้ชีวมิติเชิงพฤติกรรมร่วมกับการถ่ายภาพความร้อนด้วยอินฟราเรด	
Liu et al. (2021)	ผู้วิจัยได้ทบทวนวรรณกรรมที่เกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้ชีวมิติขั้นสูงสำหรับอุปกรณ์สวมใส่ ผู้วิจัยจำแนกชีวมิติออกเป็นสองประเภทตามที่ใช้กันทั่วไป ได้แก่ ชีวมิติทางสรีรวิทยาและชีวมิติเชิงพฤติกรรม	มัลติโมดัลใช้ชีวมิติทางสรีรวิทยาและชีวมิติเชิงพฤติกรรมสำหรับอุปกรณ์สวมใส่	
Kute, Vyas, & Anuse (2021)	เสนอแนวทาง Bregman Divergence Regularization ในการสอนให้ระบบรู้จำชีวมิติด้วยลายนิ้วมือ จากนั้นจะถ่ายโอนการเรียนรู้นี้ไปยังการการเรียนรู้ชีวมิติด้วยใบหน้า ผลการศึกษาพบว่าการถ่ายโอนการเรียนรู้นี้สามารถช่วยเพิ่มสมรรถนะในการระบุตัวผู้ต้องสงสัยได้อย่างถูกต้อง	มัลติโมดัลใช้ลายนิ้วมือและใบหน้า	

Atmakuri (2015) ผู้วิจัยทำการศึกษาโดยมีวัตถุประสงค์เพื่อศึกษาเทคนิคการพิสูจน์ตัวจริงของวิธีการต่าง ๆ ที่มีอยู่และนำเสนอวิธีการใหม่ที่ควรจะดีขึ้น ผู้วิจัยนำเสนอกรอบงานที่พัฒนาขึ้นโดยใช้การพิสูจน์ตัวจริงโดยใช้ใบหน้าในการเข้าใช้งานระบบคลาวด์ และยังให้ความเห็นเพิ่มเติมว่า

การจะเลือกใช้เทคนิคการพิสูจน์ตัวจริงนั้นต้องพิจารณาถึงทรัพยากรที่มีอยู่แล้วในเครื่องอุปกรณ์เคลื่อนที่ นอกจากนี้ผู้วิจัยได้เปรียบเทียบกรอบงานของการพิสูจน์ตัวจริงที่นำเสนอกับเทคนิคการพิสูจน์ตัวจริงด้วยวิธีการอื่นในด้าน 1) ความถูกต้อง (Accuracy) 2) ค่าใช้จ่าย (Cost) 3) ความเสถียรภาพในระยะยาว (Long Term Stability) และ 4) ระดับความปลอดภัย (Security Level) ผู้วิจัยแสดงความคิดเห็นว่ากรอบงานที่นำเสนอมีข้อดีมากกว่าวิธีการพิสูจน์ตัวจริงด้วยวิธีการอื่น ๆ

Rokita et al. (2008) ผู้วิจัยได้ศึกษาและเปรียบเทียบเทคนิคการพิสูจน์ตัวจริงของวิธีการต่าง ๆ รวมทั้งสิ้น 13 วิธีแล้วทำการประเมินการพิสูจน์ตัวจริงแต่ละวิธีโดยแบ่งออกเป็น 7 ด้านตามการศึกษาของ Jain et al. (2011) ได้แก่ ความแพร่หลาย ความเป็นเอกลักษณ์ ความคงทน การวัดได้ สมรรถนะ การยอมรับ และ การหลีกเลี่ยง นอกจากนี้ผู้วิจัยให้ความเห็นว่าการใช้เทคนิคการพิสูจน์ตัวจริงโดยใช้เพียงวิธีการเดียวไม่เพียงพอต่อการรักษาความปลอดภัยได้อย่างเพียงพอเพราะการพิสูจน์ตัวจริงแต่ละวิธีต่างมีจุดเด่น จุดด้อยหรือข้อจำกัดที่แตกต่างกัน อีกทั้งแต่ละวิธีต้องใช้เซนเซอร์ในการรับข้อมูลที่แตกต่างกันซึ่งอาจเป็นข้อจำกัดของอุปกรณ์เคลื่อนที่ ผู้วิจัยเห็นว่าควรจะมีวิธีการพิสูจน์ตัวจริงมากกว่าหนึ่งวิธีที่สามารถนำมาใช้รวมกันเพื่อเสริมความปลอดภัยของการพิสูจน์ตัวจริงให้เข้มแข็งมากขึ้น ในการศึกษานี้ผู้วิจัยเน้นศึกษาไปที่การพิสูจน์ตัวจริงโดยใช้ใบหน้าและมือ ผลการศึกษาพบว่าค่าเฉลี่ยของความถูกต้องอยู่ที่ร้อยละ 99.82 โดยใช้การวิเคราะห์ใบหน้าที่ใช้ตา 8 จุด ปาก 12 จุด และมือ 9 จุด ผู้วิจัยได้นำผลการศึกษาของ Heitmeyer (2000) ที่ศึกษาตัวชี้วัดของชีวมิติจำนวน 6 วิธีโดยใช้ปัจจัยการประเมินผลเช่น การลงทะเบียน (Registration) การเพิ่มข้อมูล (Renewal) ความต้องการของเครื่อง (Machine Requirements) และการยอมรับจากสาธารณะ (Public Perception) ผลการศึกษาพบว่า การพิสูจน์ตัวจริงโดยใช้ใบหน้าให้คะแนนผลการทดลองมากที่สุด ตามด้วย ลายนิ้วมือ และมือตามลำดับ

Romo (2014) ผู้วิจัยได้นำเสนอกรอบงาน (Framework) สำหรับการพิสูจน์ตัวจริงบนอุปกรณ์เคลื่อนที่เรียกว่า Proposed Physical Smart Key ประกอบด้วย 5 ส่วนคือ RFID Manager, Encryption Layer, Policy Manager, Hardware Key และ Device ID ผู้วิจัยได้นำเสนอผลการศึกษาการพิสูจน์ตัวจริงบนอุปกรณ์เคลื่อนที่รวมทั้งหมด 10 วิธี แล้วทำการประเมินเพื่อเปรียบเทียบแต่ละวิธีโดยแบ่งการประเมินเป็น 3 ด้านหลักคือ 1) ประโยชน์ (Usability) 2) การนำไปใช้ (Deplorability) 3) ความปลอดภัย (Security) ผลการศึกษาพบว่าคะแนนด้านประโยชน์ของการนำไปใช้วิธีการพิสูจน์ตัวจริงโดยใช้ลายนิ้วมือและกรอบงานที่นำเสนอมีคะแนนที่ประมาณ 80 คะแนน ด้านการ

นำไปใช้พบว่าการใช้ PIN และรหัสโดยใช้มีคะแนนมากที่สุดที่ 100 คะแนน และคะแนนด้านความปลอดภัยพบว่ากรอบงานที่นำเสนอให้คะแนนมากที่สุดที่ 97 คะแนน และเมื่อพิจารณาคะแนนรวมทั้ง 3 ด้านพบว่ากรอบงานที่นำเสนอให้คะแนนมากที่สุดที่ 84 คะแนน อย่างไรก็ตามผู้วิจัยพบว่าแนวคิดกรอบงานที่นำเสนอยังอาจมีปัญหาเช่นกันกล่าวคือหากผู้ใช้ทำอุปกรณ์สมาร์ทคีย์ (Physical Smart Key) หายหรือถูกโจรกรรมพร้อมกันก็สามารถเข้าถึงและเข้าใช้อุปกรณ์เคลื่อนที่ได้เช่นกัน

Ahn et al. (2011) ผู้วิจัยชี้ให้เห็นว่าการพิสูจน์ตัวจริงมีความจำเป็นสำหรับการเข้าใช้งานการประมวลผลแบบคลาวด์และชี้ให้เห็นถึงปัญหาของกระบวนการการพิสูจน์ตัวจริงเพื่อเข้าใช้การประมวลผลแบบคลาวด์ว่าผู้ใช้บริการต้องป้อนไอดีตามวิธีการพิสูจน์ตัวจริงที่ผู้ให้บริการคลาวด์จัดเตรียมไว้ให้ในทุก ๆ ครั้งที่ต้องการเข้าใช้งานซึ่งเป็นกระบวนการที่เสียเวลาและไม่สะดวกต่อผู้ใช้บริการ ผู้วิจัยจึงได้นำเสนอแพลตฟอร์มที่ใช้ในการพิสูจน์ตัวจริงโดยใช้แนวคิดการจัดเตรียมในสภาพแวดล้อมการประมวลผลแบบคลาวด์ (Provisioning in Cloud Computing Environment) โดยสถาปัตยกรรมที่นำเสนอจะทำการวิเคราะห์สารสนเทศของผู้ใช้และพิสูจน์ตัวจริงโดยใช้ข้อมูลส่วนตัวของผู้ใช้ (User Profile) โดยสามารถข้ามกระบวนการพิสูจน์ตัวจริงของผู้ให้บริการได้ อย่างไรก็ตามแนวคิดที่นำเสนอนี้กลับมีประเด็นด้านความปลอดภัยของสารสนเทศของผู้ใช้ที่จัดเก็บอยู่ในข้อมูลส่วนตัวของผู้ใช้ (User Profile)

Sharma & Mittal (2013) ผู้วิจัยกล่าวว่าการประมวลผลแบบคลาวด์เป็นผลมาจากความก้าวหน้าทางเทคโนโลยีที่มีอยู่ในปัจจุบัน โดยเป็นการผสมผสานของเทคโนโลยีการคำนวณแบบอัตโนมัติ แบบจำลองของผู้ให้บริการ-ผู้ใช้บริการ การคำนวณแบบกริด เมนเฟรมคอมพิวเตอร์ ยูทิลิตี้-คอมพิวเตอร์แบบเพียร์ทูเพียร์ และเกมบนคลาวด์ เทคโนโลยีการประมวลผลแบบคลาวด์ได้ให้คุณประโยชน์ทั้งในระดับผู้ใช้หรือระดับองค์กร แต่ยังมีประเด็นด้านความปลอดภัยในการใช้การประมวลผลแบบคลาวด์ ผู้วิจัยได้เน้นไปที่การเปรียบเทียบเทคนิคของการพิสูจน์ตัวจริงเพื่อใช้ในการตรวจสอบการระบุตัวตนของผู้ใช้บริการกับผู้ให้บริการคลาวด์ ผลการวิจัยสรุปได้ว่าการเทคนิคการพิสูจน์ตัวจริงเพื่อใช้กับการประมวลผลแบบคลาวด์นั้นมี 3 วิธีหลักคือ 1) การพิสูจน์ตัวจริงโดยใช้เคอร์เบอร์รอส (Kerberos) 2) การพิสูจน์ตัวจริงโดยใช้ศูนย์รวมคีย์แบบกระจาย (Key Distribution Center) และ 3) การพิสูจน์ตัวจริงโดยใช้ โครงสร้างพื้นฐานคีย์แบบสาธารณะ (Public Key Infrastructure)

มหาวิทยาลัยรังสิต Rangsit University

Peer et al. (2013) ผู้วิจัยให้ความเห็นว่าปริมาณข้อมูลด้านชีวมิติจากองค์กรต่าง ๆ จะมีปริมาณเพิ่มขึ้นเป็นอย่างมาก ทำให้องค์กรต่าง ๆ ต้องมีการจัดเตรียมพื้นที่เพื่อใช้ในการจัดเก็บข้อมูล รวมทั้งสมรรถนะการประมวลผลที่ต้องเพิ่มขึ้นเช่นกัน แนวทางการประยุกต์ใช้การประมวลผลแบบคลาวด์ที่สามารถช่วยแก้ปัญหาทั้งด้านการขยายตัวของหน่วยจัดเก็บข้อมูลและสมรรถนะการประมวลผลที่เพิ่มขึ้นอย่างพลวัต อย่างไรก็ตามการประยุกต์ใช้การประมวลผลแบบคลาวด์ก็มีสิ่งที่ต้องคำนึงถึงเช่น ปัญหาและอุปสรรคจากการเปลี่ยนเทคโนโลยี มาตรฐานของประมวลผลแบบคลาวด์รวมถึงชีวมิติ และวิธีแก้ปัญหาที่มีอยู่ในปัจจุบัน ผู้วิจัยได้นำการพิสูจน์ตัวจริงโดยใช้ชีวมิติในการใช้บริการประมวลผลแบบคลาวด์ไปปฏิบัติจริงกับระบบการจัดการการเรียนการสอนด้วยแอปพลิเคชัน Moodle

Shakil et al. (2020) บรรยายว่าข้อมูลต่าง ๆ ของผู้ป่วยมีความสำคัญสูงมากจึงมีความจำเป็นอย่างมากที่จะต้องมีการจัดการข้อมูลให้ความปลอดภัยระดับสูงสุด ทั้งด้านการจัดเก็บ การเข้าถึง และการบริหารจัดการ นักวิจัยได้เสนอการพิสูจน์ตัวจริงเชิงพฤติกรรมโดยใช้ลายเซ็นของผู้ป่วยแต่ละรายโดยระบบการพิสูจน์ตัวจริงนี้จะทำงานอยู่บนระบบการประมวลผลแบบคลาวด์

Errattahia et al. (2018) ได้ทบทวนการตรวจหาข้อผิดพลาดและวิธีการแก้ไขระบบการรู้จำเสียงแบบอัตโนมัติ (Automatic Voice Recognition - ASR) โดยนักวิจัยให้ความสำคัญกับการแก้ไขข้อผิดพลาดระบบการรู้จำเสียงแบบอัตโนมัติ เพื่อทำให้ระบบมีประสิทธิภาพ ใช้งานได้และทนทานต่อการใช้งานในสภาพแวดล้อมต่าง ๆ เพิ่มมากขึ้น

Bah & Ming (2020) เสนอวิธีการใหม่ในการแก้ไขความเที่ยงตรงของระบบจดจำใบหน้าโดยผสานขั้นตอนวิธีโลคอลไบนารีแพลตเทิน (Local Binary Pattern) เข้ากับเทคนิคการประมวลผลภาพบางอย่าง ตัวอย่างเช่น การเปรียบเทียบความแตกต่างของแสง ความสว่าง หรือการปรับฮิสโตแกรม เทคนิคเหล่านี้สามารถช่วยให้ระบบรู้จำใบหน้ามีความแม่นยำ ความน่าเชื่อถือได้และความแข็งแกร่งเพิ่มมากยิ่งขึ้น

Mason et al. (2020) รายงานว่าเทคโนโลยีชีวมิติเติบโตอย่างรวดเร็วในอุตสาหกรรมด้านการดูแลสุขภาพ พวกเขาเสนอแนวทางใหม่ที่ใช้การผสมผสานชีวมิติบริเวณรอบดวงตาร่วมกับหมายเลขดัชนีจากระบบสารสนเทศของผู้ป่วยในระบบข้อมูลด้านการดูแลสุขภาพเพื่อใช้ในการแยกแยะผู้ป่วยแต่ละราย

มหาวิทยาลัยรังสิต Rangsit University

Naidu & Babu (2018) นำเสนอระบบการรู้จำชีวมิติหลายรูปแบบ ตัวอย่างเช่น ใบหน้า นิ้ว และเสียงเพื่อใช้ในการระบุตัวตน ระบบที่นำเสนอนี้มีความปลอดภัย และความถูกต้องแม่นยำที่ดีกว่าเมื่อเปรียบเทียบกับการระบุตัวตนโดยใช้ชีวมิติแบบเดี่ยวที่มีอยู่ ความถูกต้องและความแม่นยำของระบบนี้ได้มาจากการนำคะแนนความแม่นยำของการรู้จำจากชีวมิติหลายรูปแบบที่ใช้งานมารวมกัน (Score Level Fusion)

Choudhury et al. (2021) เสนอกรอบการทำงานสำหรับการผสานชีวมิติที่มีการจัดระดับอันดับที่ปรับเปลี่ยนได้ การจัดอันดับได้รับการปรับใช้โดยใช้เทคนิคแอนท์โคโลนีออปติไมส์เซชัน (Ant Colony Optimization) เพื่อให้เกิดประสิทธิภาพสูงสุด งานวิจัยนี้มีการปรับใช้ชีวมิติหลายรูปแบบโดยใช้การดึงคุณสมบัติของแผ่นเล็บจาก นิ้วชี้ นิ้วกลาง และนิ้วนางมารวมกัน การสกัดคุณสมบัติของแผ่นเล็บทั้งสามนี้ใช้ขั้นตอนวิธี AlexNet, ResNet-18 และ DenseNet-201

Fei et al. (2021) นำเสนอการรู้จำชีวมิติโดยใช้คุณสมบัติต่าง ๆ จากมือโดยใช้หลายอินสแตนซ์ร่วมกัน นักวิจัยปรับใช้ข้อมูลเบื้องต้นจากภาพชีวมิติหลายอินสแตนซ์ คุณลักษณะที่คัดแยกออกมาของชีวมิติ และแสดงการทำงานร่วมกันของคุณลักษณะชีวมิติแบบหลายอินสแตนซ์และการรวมกันคุณลักษณะที่คัดแยกออกมาของชีวมิติแบบหลายอินสแตนซ์

Sarier (2021) เสนอซึ่งเป็นการพิสูจน์ตัวจริงโดยใช้ชีวมิติแบบหลายวิธีบนเทคโนโลยีมือถือ (Multimodal Biometrics Authentication - Mobile Edge Computing หรือ MBA-MEC) เป็นรูปแบบใหม่ที่ใช้โปรโตคอลความปลอดภัย Privacy Preserving Biometric Authentication (PPBA) เพื่อต่อต้านผู้บุกรุก การจับคู่เพื่อยืนยันตัวตนของ MBA-MEC จะดำเนินการในรูปแบบที่มีการเข้ารหัส จากนั้นคะแนนการจับคู่ของชีวมิติแบบหลายวิธีจำนำมารวมขั้นสุดท้ายโดยจะมีการเข้ารหัสเพื่อให้เกิดความปลอดภัยจากผู้บุกรุก

Kumari & Thangaraj (2020) เสนอเทคนิคการเลือกคุณสมบัติอย่างรวดเร็วสำหรับชีวมิติแบบหลายวิธี บนเฟรมเวิร์กระบบคลาวด์ ชีวมิติแบบหลายวิธีประกอบด้วยการรู้จำภาพใบหน้าและการรู้จำลายนิ้วมือ เทคนิคการเลือกคุณลักษณะที่นำเสนอนี้ใช้เทคนิคแอนท์โคโลนีออปติไมส์เซชัน (Ant Colony Optimization) ส่วนกระบวนการแยกคุณลักษณะและการจัดประเภทใช้เทคนิคพาร์ติเคิลสวอร์มออปติไมส์เซชัน (Particle Swarm Optimization)

มหาวิทยาลัยรังสิต Rangsit University

Chang et al. (2021) เสนอเฟรมเวิร์กแบบรวมข้อมูลชีวมิติแบบหลายรูปแบบชื่อ S-BIOFUSE ซึ่งเป็นรวมกันของฟัสซีคอมมิตเมนต์ (Fuzzy Commitment) และฟัสซีโวล์ท (Fuzzy Vault) เทคนิคทั้งสองนี้ถูกนำมาใช้เพื่อสร้างรูปแบบการรักษารูปแบบการเข้ารหัสจากข้อมูลชีวมิติทั้งหมดเพื่อเพิ่มความปลอดภัยของข้อมูลชีวมิติ เฟรมเวิร์กที่นำเสนอนี้ทำให้ผู้ที่จะเข้ามาโจมตีหรือขโมยข้อมูลทำได้ยากมากขึ้นเนื่องจากต้องเลียนแบบข้อมูลชีวมิติทั้งหมดที่เป็นข้อมูลต้นฉบับ

Vijay & Indumathi (2021) เสนอชีวมิติแบบหลายรูปแบบประกอบด้วยชีวมิติสามแบบ ได้แก่ ม่านตา (Iris) ลักษณะใบหู (Ear) และ โครงร่างเส้นเลือดของนิ้ว (Finger Vein) ซึ่งคุณสมบัติต่าง ๆ ถูกดึงออกมาโดยใช้วิธีการ BiComp Masking จากนั้นคะแนนการรู้จำจะถูกคำนวณโดยใช้ตัวจัดหมวดหมู่ชื่อ multi-SVNN ของชีวมิติทั้งสามลักษณะ

Kausar (2021) กล่าวถึงการประยุกต์ใช้ชีวมิติเพื่อปกป้องข้อมูลด้านสุขภาพที่เป็นข้อมูลที่สำคัญส่วนบุคคลของผู้ป่วย ผู้วิจัยนำเสนอระบบเข้ารหัสลับที่ยกเลิกได้โดยใช้ม่านตาบนบัตรสมาร์ตการ์ด (Iris-based Cancelable Crypto System) ข้อมูลที่สำคัญส่วนบุคคลของผู้ป่วยจะถูกเข้ารหัสคีย์แบบสมมาตรและถูกจัดเก็บในรูปแบบที่เข้ารหัสบนสมาร์ทการ์ดเพื่อให้เกิดความปลอดภัยของข้อมูลส่วนบุคคล

Piciucco et al. (2021) เสนอการผสมผสานการรู้จำชีวมิติและอุปกรณ์สวมใส่เพื่อป้องกันการใช้งานอุปกรณ์เหล่านี้โดยไม่ได้รับอนุญาต โดยเป็นการรวมขั้นตอนวิธี EDA และ BVP Spectrograms เข้ากับ MobileNetv2 ผลการศึกษาพบว่าการรู้จำชีวมิตินำมาประยุกต์ใช้รวมเข้ากับอุปกรณ์สวมใส่เพื่อเป็นการพิสูจน์ตัวจริงผู้ใช้ที่ได้รับอนุญาต

Bisogni et al. (2021) เสนอระบบชีวมิติที่มุ่งเน้นความปลอดภัยเพื่อนำมาประยุกต์ใช้กับการอนุญาตและลงชื่อในการทำธุรกรรมบล็อกเชน ระบบชีวมิติที่นำเสนอนี้ใช้การรู้จำภาพใบหน้าและมีการเข้ารหัสโดยใช้ CNN จากนั้นนำไปรวมกับ RSA Key ผลการศึกษาพบว่าการรวมชีวมิติ การเข้ารหัสโดยใช้ CNN และการรวมกับ RSA Key ช่วยให้เกิดความมั่นใจในยืนยันตัวตนเพื่อทำธุรกรรมบล็อกเชนและเป็นการรักษาความเป็นส่วนตัวของผู้ใช้อีกด้วย

BrundhaElci et al. (2019) เสนอการประยุกต์ระบบการรู้จำภาพใบหน้าเพื่อใช้กับกล้องวงจรปิดเพื่อการการรู้จำอาชญากรและการติดตามบุคคลได้อย่างรวดเร็วเพื่อลดอัตราการเกิด

มหาวิทยาลัยรังสิต Rangsit University

อาชญากรรมงานวิจัยนี้ใช้ขั้นตอนวิธีโครงข่ายประสาทเทียมเชิงลึกในการตรวจหาและรู้จำอาชญากรและการติดตามบุคคล

Cherifi, Omar, & Amroun (2021) เสนอระบบการยืนยันตัวแบบทันทีอย่างต่อเนื่อง โดยบันทึกกิจกรรมต่าง ๆ ของผู้ใช้โดยใช้เซนเซอร์ที่อยู่ในสมาร์ตโฟน ตัวอย่างเช่น ไจโรสโคป (Gyroscope) หรือมาตรความเร่ง (Accelerometer) เพื่อรวบรวมข้อมูลตำแหน่งหรือพิกัดของผู้ใช้ กระบวนการโดยรวมของระบบการยืนยันตัวแบบทันทีอย่างต่อเนื่องประกอบด้วย การบันทึกข้อมูลกิจกรรมของผู้ใช้ การคัดแยกคุณลักษณะที่สำคัญ การเรียนรู้ของเครื่องโดยใช้ HMM Model และการพิสูจน์ตัวจริงของผู้ใช้

Falmari & Brindha (2021) เสนอแนวทางใหม่ในการเข้ารหัสให้กับข้อมูลชีวมิติซึ่งเพิ่มความปลอดภัยให้กับระบบการพิสูจน์ตัวจริงให้มากขึ้น ในระบบเครื่องบริการ (Server) และลูกข่าย ข้อมูลชีวมิติอาจถูกจัดเก็บไว้บนเครื่องบริการ (Server) ผ่านระบบเครือข่ายที่อาจอยู่ห่างไหลกัน ดังนั้นข้อมูลชีวิมิติอาจถูกขโมยระหว่างการส่งหรือส่งต่อบนเครือข่ายได้ วิธีการที่นำเสนอนี้จะมีการเข้ารหัสข้อมูลชีวมิติ ตัวอย่างเช่น ภาพของม่านตา ภาพใบหน้า หรือภาพลายนิ้วมือ โดยใช้ขั้นตอนวิธีแฮชขนาด 256 บิต ก่อนการส่งข้อมูลชีวมิติไปยังเครือข่าย กุญแจการเข้ารหัสถูกสร้างขึ้นจากภาพชีวมิติต้นฉบับ ดังนั้นจึงเป็นเรื่องยากที่จะถอดรหัสกุญแจที่เข้ารหัสโดยไม่มีภาพชีวมิติต้นฉบับ

Yang et al. (2021) นำเสนอแนวทางชื่อ Feature-adaptive Random Projection-based โดยโปรเจคชัน (Projection) ในที่นี้หมายถึงเมทริกซ์ที่สืบทอดมาจากคุณลักษณะภายในที่มาจากเมทริกซ์พื้นฐาน เมทริกซ์โปรเจคชันหลังจากที่ถูกใช้งานแล้วจะถูกเอาออกจากระบบเพื่อป้องกันการถูกนำข้อมูลในเมทริกซ์ไปใช้อย่างอื่น

Saeed (2021) เสนอแนวทางใหม่ที่ผสมผสานคุณลักษณะของ Soft Biometric กับคุณลักษณะใบหน้าแบบทั่วไป คุณลักษณะ Soft Biometric ถูกใช้เพื่อสร้างแบบจำลองไมโครเอ็กซ์เพรสชัน (Micro-expression) ส่วนลักษณะของใบหน้าทั่วไปถูกใช้เพื่อสร้างแบบจำลองโครงสร้างใบหน้า ผลการศึกษาพบว่าแนวทางที่นำเสนอนี้สามารถเพิ่มอัตราการรู้จำภาพใบหน้าประมาณร้อยละ 5

มหาวิทยาลัยรังสิต Rangsit University

Stylios et al. (2021) เสนอเทคนิคการพิสูจน์ตัวจริงด้วยชีวมิติเชิงพฤติกรรมแบบต่อเนื่องโดยใช้โทรศัพท์มือถือ (Continuous Behavioral Biometrics Authentication Technique Using Mobile Phones) บทความนี้มีการวิเคราะห์วิธีการรวบรวมและการแยกคุณลักษณะ บทความนี้ยังแสดงให้เห็นจุดอ่อนของโมเดลการเรียนรู้ของเครื่อง ช่วยให้เตรียมการป้องกันและมีมาตรการป้องกันการโจมตีจากผู้ไม่ประสงค์ดีและมาตรการป้องกันที่เกี่ยวข้อง

Behera et al. (2021) นำเสนอแนวคิดใหม่ของการพิสูจน์ตัวจริงบนอุปกรณ์ชีวมิติที่เชื่อมต่อกับอินเทอร์เน็ต (Internet of Biometrics Things - IoBT) ซึ่งเป็นระบบตรวจสอบชีวมิติบนระบบการประมวลผลแบบคลาวด์ ระบบที่นำเสนอจะติดตามการเคลื่อนไหวของบุคคลในกล้องวงจรปิดหลายตัว ซึ่งช่วยลดความซับซ้อนของการพิสูจน์ตัวจริงซ้ำ ๆ ในกล้องวงจรปิดหลายตัวในสถานการณ์เมืองอัจฉริยะที่พบว่าอินเทอร์เน็ตของสรรพสิ่ง (IoT) ถูกใช้อย่างแพร่หลายมากขึ้นโดยเฉพาะกล้องวงจรปิดอัจฉริยะซึ่งมีการรับส่งข้อมูลผ่านเครือข่ายจำนวนมาก

Ajish & AnilKumar (2021) นำเสนอระบบการลงคะแนนเลือกตั้งโดยใช้การพิสูจน์ตัวจริงแบบชีวมิติซึ่งทำงานบนแอปพลิเคชันมือถือที่มีการเข้ารหัสข้อมูลเพื่อเพิ่มความปลอดภัยของข้อมูลของผู้มีสิทธิเลือกตั้ง แอปพลิเคชันบนมือถือจะประมวลผลข้อมูลภาพที่ผ่านการเข้ารหัสโดยการคัดแยกคุณลักษณะสำคัญและจัดเก็บในรูปแบบของเทมเพลตชีวมิติ แล้วทำการส่งเทมเพลตชีวมิติที่ถูกเข้ารหัสส่งบนเครือข่ายของผู้ให้บริการมือถือไปยังเครื่องบริการ (Server) เพื่อทำการประมวลผลในขั้นตอนถัดไป เพื่อเพิ่มความปลอดภัยระหว่างการส่งข้อมูลบนเครือข่ายมือถือกระบวนการเข้ารหัสข้อมูลใช้ขั้นตอนวิธี Wavelet-based AES ซึ่งผลการศึกษาพบว่ามีสมรรถนะและให้ผลการทำงานดีกว่าการเข้ารหัสข้อมูลวิธีการอื่น

Kumar, Joshi, & Singh (2021) นำเสนอการเข้ารหัสสองชั้นเพื่อความปลอดภัยของเทมเพลตชีวมิติ ขั้นที่หนึ่งข้อมูลจะถูกแบ่งเป็นส่วนย่อย ๆ เพื่อนำมาเป็นตัวแทนของเทมเพลตชีวมิติโดยใช้เทคนิคเวปเล็ตไม่ต่อเนื่องแบบสองมิติ (Two Dimensional Discrete Wavelet) และขั้นตอนที่สองเป็นกระบวนการแทนที่และการเปลี่ยนแปลงจะใช้เทคนิค Three Dimensional Lorenz-Chaotic System โดยทั้งสองขั้นตอนมีการเข้ารหัสข้อมูล ส่วนกระบวนการถอดรหัสจะทำการกระบวนการแบบย้อนลำดับ ผลการศึกษาพบว่าวิธีการที่นำเสนอสามารถเพิ่มความปลอดภัยอย่างเข้มแข็งจากผู้โจมตี

มหาวิทยาลัยรังสิต Rangsit University

Jia et al. (2021) นำเสนองานวิจัยแบบสำรวจที่เกี่ยวข้องกับการพิสูจน์ตัวจริงด้วยชีวมิติโดยใช้โครงสร้างเส้นเลือดที่หลังมือ รายงานผลการศึกษาอธิบายกระบวนการที่เกี่ยวข้องกับการพิสูจน์ตัวจริงด้วยชีวมิติโดยใช้โครงสร้างเส้นเลือดที่หลังมือ ประกอบด้วย การเก็บข้อมูล การออกแบบโครงสร้างฐานข้อมูล กระบวนการก่อนการประมวลผล ขั้นตอนวิธีการคัดแยกคุณลักษณะสำคัญ ขั้นตอนวิธีการจับคู่ และการรวมคะแนนหาผลสรุป นอกจากนี้ผู้วิจัยได้บรรยายแง่มุมต่างของเทคโนโลยีการพิสูจน์ตัวจริงด้วยชีวมิติโดยใช้โครงสร้างเส้นเลือดที่หลังมือในอนาคต

Lee & Jeong (2021) นำเสนอระบบ BDAS ซึ่งเป็นระบบยืนยันตัวตนด้วยชีวมิติแบบใหม่ที่ประยุกต์ใช้ร่วมกับเทคโนโลยีบล็อกเชน ระบบ BDAS มีกลไกการแยกออกจากศูนย์กลาง (Decentralized) และการกระจาย (Distributed) ตามแนวคิดของเทคโนโลยีบล็อกเชนและกลไกที่ใช้การตรวจสอบเพื่อใช้สำหรับการพิสูจน์ตัวจริงด้วยชีวมิติ ผู้วิจัยได้นำเสนอผลการประเมินระบบ BDAS พบว่ามีความน่าเชื่อถือได้และมีความปลอดภัย ในการพิสูจน์ตัวจริงด้วยชีวมิติเมื่อเปรียบเทียบกับกับแนวทางอื่น ๆ

Srivastva, Singh, & Singh (2021) นำเสนอระบบการรู้จำชีวมิติโดยใช้ข้อมูลคลื่นไฟฟ้าของหัวใจซึ่งแสดงถึงกิจกรรมทางไฟฟ้าของหัวใจโดยใช้อุปกรณ์อิเล็กโทรดที่วางอยู่บนผิวหนังของมนุษย์ ผู้วิจัยเสนอโมเดลชื่อ Plexnet ซึ่งเป็นการรวมโมเดลอื่น 4 ชนิดที่ผ่านการปรับแต่งแล้ว โดยผลลัพธ์ที่ได้จากโมเดลทั้ง 4 ชนิดจะนำมารวมกันเพื่อให้ได้เป็นผลลัพธ์ของโมเดลที่นำเสนอ ผลการทดสอบโมเดลที่นำเสนอกับกลุ่มข้อมูลพบว่ามีคะแนนความถูกต้องสูงสุดที่ร้อยละ 99.66 และมีความแข็งแกร่งต่อการใช้งาน

Cui, Wang, & Li (2021) ศึกษาการรู้จำชีวมิติโดยใช้ข้อมูลคลื่นไฟฟ้าของหัวใจซึ่งผู้วิจัยกล่าวว่าวิธีนี้เป็นเรื่องยากมากที่จะปลอมชีวมิตินี้ได้ ผู้วิจัยได้สร้างกลุ่มข้อมูลขึ้นมาเองทั้งจากขณะออกกำลังและขณะพักผ่อนเพื่อให้ได้กลุ่มข้อมูลที่มีการกระจายตัว ผู้วิจัยประเมินผลแนวคิดนี้โดยใช้ขั้นตอนวิธีหลายแบบกับกลุ่มข้อมูลที่สร้างขึ้นมา ผลการศึกษาพบว่าแนวคิดที่นำเสนอนี้ให้ผลลัพธ์เป็นน่าพอใจในสถานการณ์ที่อาจจะแตกต่างกันตามสภาพแวดล้อม

Marquez et al. (2021) นำเสนองานวิจัยระบบแจ้งเตือนการเป็นสัดที่สามารถช่วยให้เกษตรกรตรวจพบการเป็นสัดของวัวได้ เป็นการศึกษาการใช้ชีวมิติเชิงพฤติกรรมร่วมกับการถ่ายภาพความร้อนด้วยอินฟราเรดเพื่อติดตามการเป็นสัดของโคนมในฟาร์ม โดยมีปัญหาการ

มหาวิทยาลัยรังสิต Rangsit University

วิจัยคืออัตราการเป็นสัดของสัตว์ที่เลี้ยงในฟาร์มต่ำ ซึ่งสะท้อนถึงระยะเวลาการคลอดที่นานขึ้น กำไรทางเศรษฐกิจลดลง การมีอายุยืนยาวของสัตว์ที่เลี้ยงในฟาร์มที่ลดลง การใช้ภาพถ่ายความร้อนด้วยอินฟราเรดใช้เพื่อรวบรวมอุณหภูมิผิวหนังของโคนม จากนั้นระบบจะวิเคราะห์ตัวบ่งชี้การตกไข่โดยการหดตัวของรูขุมขนที่เห็นได้เด่นชัด

Liu et al. (2021) ศึกษาการพิสูจน์ตัวจริงโดยใช้ชีวมิติสำหรับอุปกรณ์สวมใส่ เนื่องจากปัจจุบันอุปกรณ์สวมใส่ได้ถูกนำมาใช้กันอย่างแพร่หลายในชีวิตประจำวันเพิ่มมากขึ้น ผู้วิจัยได้ทบทวนวรรณกรรมที่เกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้ชีวมิติขั้นสูงสำหรับอุปกรณ์สวมใส่ ผู้วิจัยจำแนกชีวมิติออกเป็นสองประเภทตามที่ใช้กันทั่วไป ได้แก่ ชีวมิติทางสรีระวิทยาและชีวมิติเชิงพฤติกรรม โดยมีเป้าหมายเพื่อที่จะจัดทำแนวทางสำหรับการวิจัยในอนาคตที่เกี่ยวข้องกับการศึกษานี้

Kute, Vyas, & Anuse (2021) เสนอแนวทางการใช้ลายนิ้วมือเพื่อระบุภาพใบหน้าของบุคคลโดยเฉพาะในการสอบสวนคดีอาญา โดยทั่วไปแล้วทั้งการจดจำใบหน้าและการจดจำลายนิ้วมือมักจะใช้ในการตรวจสอบทางนิติเวช แนวทางนี้ใช้ Bregman Divergence Regularization ในการสอนให้ระบบรู้จำชีวมิติด้วยลายนิ้วมือ จากนั้นจะถ่ายโอนการเรียนรู้นี้ไปยังการการเรียนรู้ชีวมิติด้วยใบหน้า ผลการศึกษาพบว่าการถ่ายโอนการเรียนรู้นี้สามารถช่วยเพิ่มสมรรถนะในการระบุตัวผู้ต้องสงสัยได้อย่างถูกต้อง

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 3

ระเบียบวิธีการวิจัย

เนื้อหาในบทนี้ผู้วิจัยนำเสนอและบรรยาย กรอบงานที่นำเสนอ (Proposed Framework) การออกแบบและพัฒนาระบบ และระเบียบวิธีวิจัย ประกอบด้วย ประชากรและกลุ่มตัวอย่าง การเก็บรวบรวมข้อมูล เครื่องมือที่ใช้ในการวิจัย และการวิเคราะห์ข้อมูล

3.1 กรอบงานที่นำเสนอ (Proposed Framework)

การศึกษานี้เป็นการศึกษาการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ โดยใช้กระบวนการวิจัยเชิงพัฒนา และเป็นการวิจัยเชิงทดลอง โดยมีภาพรวมของระบบดังรูปที่ 3.1 ระบบโดยรวมแบ่งได้เป็น 3 ระดับชั้นคือ ระดับแอปพลิเคชันบนเครื่องคอมพิวเตอร์ของผู้ใช้ ระดับแอปพลิเคชันของระบบการพิสูจน์ตัวจริง และระดับฐานข้อมูล

ระดับแอปพลิเคชัน (Client Layer) บนเครื่องคอมพิวเตอร์ของผู้ใช้ จะมีการติดตั้งแอปพลิเคชันไว้ที่ฝั่งผู้ใช้เพื่อให้ผู้สามารถป้อนข้อมูลส่วนบุคคลได้แก่ ชื่อบัญชีผู้ใช้ รหัสโดยใช้อีเมล ภาพใบหน้าและข้อมูลเสียงพูด แล้วนำเข้าสู่ระบบ และแสดงผลลัพธ์จากการพิสูจน์ตัวจริง

ระดับแอปพลิเคชันของระบบการพิสูจน์ตัวจริง (Application Layer) เป็นส่วนของแอปพลิเคชันที่ติดตั้งไว้ที่เครื่องให้บริการ (Server) บนการประมวลผลแบบคลาวด์ ทำหน้าที่คัดกรอง ตรวจสอบข้อมูลเบื้องต้นก่อน การกรองคุณลักษณะที่ต้องการ หรือการสร้างแบบจำลอง แล้วจัดเก็บไว้ในระบบฐานข้อมูล เพื่อใช้ในการเปรียบเทียบของการพิสูจน์ตัวจริง

ระดับฐานข้อมูล (Database Layer) ทำหน้าที่บริการจัดการข้อมูลชีวมิติทั้งการเพิ่ม การลบ การแก้ไข หรือการสืบค้นข้อมูล เป็นต้น โดยข้อมูลจะถูกเข้ารหัสเพื่อเพิ่มความปลอดภัยในการเข้าถึงหรือเข้าใช้ข้อมูล โดยทำงานบนการประมวลผลแบบคลาวด์

การพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ โดยใช้เครื่องคอมพิวเตอร์สามารถแบ่งเป็น 3 เฟสดังรูปที่ 3.2

รูปที่ 3.1 ภาพรวมกรอบงานที่นำเสนอ

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.2 เฟสของการพิสูจน์ตัวจริงโดยใช้ชีวมิติ

รูปที่ 3.3 เฟสการลงทะเบียนข้อมูล (Registration Phase)

มหาวิทยาลัยรังสิต Rangsit University

1) เฟสการลงทะเบียนข้อมูล (Registration Phase)

ขั้นตอนนี้เป็นขั้นตอนในการเก็บรวบรวมข้อมูลของผู้ใช้ผ่านกระบวนการลงทะเบียน ผู้ใช้จะป้อนข้อมูลพื้นฐานส่วนบุคคลและข้อมูลชีวมิติ ข้อมูลชีวมิติทั้งสองแบบคือภาพใบหน้าและข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท ดังแสดงในรูปที่ 3.3

1.1) ขั้นที่ 1 การรับข้อมูล (Capturing) ผู้ใช้ที่ต้องการลงทะเบียนทำการป้อนข้อมูลส่วนบุคคล ได้แก่ ชื่อบัญชีผู้ใช้ รหัสโดยใช้ อีเมล และข้อมูลชีวมิติได้แก่ภาพใบหน้าและข้อมูลเสียงโดยใช้เว็บแอปพลิเคชันที่ได้พัฒนาขึ้นบนอุปกรณ์ต่าง ๆ ที่มีโปรแกรมเว็บเบราเซอร์

1.2) ขั้นที่ 2 การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) ข้อมูลที่ชีวมิติที่รับเข้ามาจำเป็นต้องมีการแยกคุณลักษณะเด่นที่ต้องการไว้ ส่วนข้อมูลใดที่ไม่จำเป็นก็จะทำการนำออกไป ตัวอย่างเช่น ภาพหน้าคน ก็จะทำการตัดเฉพาะส่วนที่เป็นใบหน้าเท่านั้นที่จะมีผลต่อการพิสูจน์ตัวจริง ส่วนผมหรือส่วนอื่น ๆ ก็จะถูกตัดออกไป ข้อมูลชีวมิติทั้งสองแบบคือภาพใบหน้าและข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท

การวิจัยนี้ใช้เทคนิค Haar-cascade ในการตรวจหาภาพใบหน้าของคน เทคนิคนี้ใช้วิธีการฮิสโตแกรมเพื่อเปรียบเทียบหาความหนาแน่นของจุดบนภาพใบหน้า ตัวอย่างเช่น ใช้ในการเส้นขอบบนใบหน้า การหาส่วนของมุมบนใบหน้า หรือการหาส่วนที่แบนราบบนใบหน้า การตรวจหาภาพใบหน้าของคนจะให้ผลลัพธ์ได้ไม่ดีนักหากภาพใบหน้าคนที่รับเข้ามานั้นอยู่ในสภาพแวดล้อมที่มีแสงสว่างน้อย ดังนั้นภาพใบหน้าที่รับเข้ามานั้นมีความจำเป็นต้องใช้เทคนิคฮิสโตแกรมในการปรับความสว่างและความคมชัดของภาพใบหน้าต้นฉบับทั้งในขั้นตอนการลงทะเบียนและขั้นตอนการรู้จำด้วยเทคนิคฮิสโตแกรมนี้สามารถช่วยปรับปรุงการตรวจหาภาพใบหน้าของคนให้มีประสิทธิภาพดีขึ้นและยังช่วยลดเวลาในการประมวลผลลงด้วย

การพัฒนาการวิจัยนี้มีการกำหนดค่าการทำงานของขั้นตอนวิธี Harr-cascade โดยใช้ไลบรารีของ Opencv โดยมีรูปแบบการกำหนดค่าการทำงานดังนี้

```
cv2.CascadeClassifier.detectMultiScale(image[, scaleFactor[, minNeighbors[, flags[, minSize[,
maxSize]]]]])
```

พารามิเตอร์ที่ใช้ในการกำหนดค่าการทำงานมีดังนี้

1) image: เป็นพารามิเตอร์ที่ใช้กำหนดเมตริกซ์ของภาพที่จะนำมาตรวจหาใบหน้าคนในภาพ มีชนิดของไฟล์เป็น CV_8U

2) scaleFactor: เป็นพารามิเตอร์ที่ใช้กำหนดอัตราการลดขนาดของภาพ ตัวอย่างเช่น scaleFactor มีค่าเท่ากับ 1.02 จะเป็นการลดขนาดของภาพลงร้อยละ 2 ซึ่งเป็นค่าที่ไม่สูงมากเพื่อเพิ่มโอกาสของโมเดลในการตรวจหาใบหน้าในภาพแต่ก็จะไม่ได้ลดเวลาในการประมวลผลมากนัก

มหาวิทยาลัยรังสิต Rangsit University

หากกำหนดค่า scaleFactor ไว้สูงเพื่อเป็นการลดขนาดของภาพมากจะส่งผลให้โอกาสของโมเดลในการตรวจหาใบหน้าในภาพลดลง แต่ก็จะช่วยลดเวลาในการประมวลผลได้

3) minNeighbors: เป็นพารามิเตอร์ที่ใช้กำหนดจำนวนจุดภาพที่อยู่รอบ ๆ เพื่อใช้เปรียบเทียบกับจุดภาพกึ่งกลาง พารามิเตอร์นี้มีผลต่อคุณภาพของใบหน้าที่ตรวจหา หากกำหนดค่าไว้สูงส่งผลให้โอกาศการรตรวจหาใบหน้าจากภาพลดลง แต่จะได้คุณภาพของภาพใบหน้าที่สูงขึ้น

4) flags: เป็นพารามิเตอร์ที่ใช้กำหนดเพื่อรองรับการทำ Cascade แบบเก่า แต่การ Cascade แบบใหม่ได้ใช้พารามิเตอร์นี้

5) minSize: เป็นพารามิเตอร์ที่ใช้กำหนดขนาดขั้นต่ำของวัตถุที่ตรวจหา วัตถุที่มีขนาดเล็กกว่าที่กำหนดจะถูกละเว้น

6) maxSize: เป็นพารามิเตอร์ที่ใช้กำหนดขนาดขั้นสูงสุดของวัตถุที่ตรวจหา วัตถุที่มีขนาดใหญ่กว่าที่กำหนดจะถูกละเว้น

การเตรียมข้อมูลภาพใบหน้าก่อนการประมวลผล (Face Preprocessing) ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การตรวจหาบริเวณดวงตาซึ่งมักเป็นบริเวณที่มีสีเข้มกว่าบริเวณอื่นและจะมีการปรับขนาด (Scaling) การหมุนภาพ (Rotating) และการแปลงภาพ (Translating) นอกจากนี้จะทำการตัดส่วนของภาพให้เหลือเฉพาะบริเวณใบหน้าเท่านั้น ส่วนประกอบอื่นเช่น หน้าผาก คาง ใบหู และภาพพื้นหลังอื่น ๆ ออก ขั้นที่ 2 การใช้เทคนิคฮิสโตแกรมในการเพิ่มคุณภาพของภาพต้นฉบับ โดยการจัดวางตำแหน่งภาพ การปรับความสว่างและความคมชัดให้ด้านซ้ายและด้านขวาของภาพใบหน้า ขั้นที่ 3 การทำเครื่องหมายรูปวงรีเพื่อเป็นการเน้นภาพใบหน้า และจะกำจัดผมและพื้นหลังบางส่วนออกจากภาพใบหน้า ผลลัพธ์ที่ได้คือเฉพาะในรูปภาพใบหน้าเท่านั้น

การเตรียมข้อมูลเสียงก่อนการประมวลผล (Voice Preprocessing) เป็นกระบวนการย่อยของกระบวนการการคัดแยกคุณลักษณะเด่น โดยจะมีการปรับความสมดุลความถี่ของเสียงที่รับมาจากอุปกรณ์ไมโครโฟนให้อยู่ในระดับสัญญาณเสียงที่หูของมนุษย์สามารถรับรู้ได้อย่างเหมาะสม

1.3) การคัดแยกคุณลักษณะเด่น (Feature Extraction) เป็นนำผลลัพธ์ที่ได้จากขั้นตอนก่อนหน้านี้ทั้งส่วนของข้อมูลชีวมิติภาพใบหน้ามาทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองเฉพาะส่วนของตำแหน่ง หรือขนาดของอวัยวะ ตัวอย่างเช่น ตา จมูก หรือปาก การวิจัยนี้ใช้ขั้นตอนวิธี Local Binary Pattern Histogram (LBPH) ส่วนข้อมูลชีวมิติเสียงจะมา

มหาวิทยาลัยรังสิต Rangsit University

ทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองคือเวกเตอร์ของเสียง MFCC ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การคัดแยกคุณลักษณะเด่นของข้อมูลเสียง (MFCC Extraction) โดยใช้ขั้นตอนวิธี MFCC จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติ ขั้นที่ 2 การคำนวณค่าเดลตา (Delta) จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติเช่นกัน ดังนั้นเมื่อรวมกันทั้งเวกเตอร์ของเสียงจาก MFCC กับเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติจากเดลตา (Delta) จะได้เวกเตอร์ของเสียงที่มีคุณลักษณะจำนวน 40 มิติ ขั้นที่ 3 ข้อมูลชีวมิติเสียงจะถูกคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์คือ เทมเพลตของชีวมิติเสียง

1.4) การจัดเก็บลงในฐานข้อมูล (Storing in Database) เป็นการนำเทมเพลตหรือแบบจำลองไปจัดเก็บไว้ในฐานข้อมูลซึ่งอยู่บนระบบการประมวลผลแบบคลาวด์ เพื่อนำไปใช้ในขั้นตอนถัดไป

2) เฟสการเรียนรู้ของเครื่อง (Training Phase)

เป็นขั้นตอนที่นำเอาข้อมูลที่ได้จากการแยกคุณลักษณะเด่นที่ต้องการ (Feature Extraction) ของแต่ละบุคคลมาเป็นข้อมูลเพื่อสอนให้คอมพิวเตอร์เรียนรู้ด้วยตนเองว่าเค้าโครงภาพใบหน้าของแต่ละคนมีคุณลักษณะอย่างไร ตัวอย่างเช่น ความเข้มของสีของส่วนประกอบต่าง ๆ บนใบหน้า เป็นต้น รวมทั้งคุณลักษณะเด่นของเสียงของแต่ละบุคคลด้วยเช่นกัน สำหรับการเรียนรู้ภาพใบหน้า (Facial Training) จะเป็นการนำเอาคุณลักษณะเด่นของภาพใบหน้าที่ได้มาจากเฟสที่ 1 มาสอนให้คอมพิวเตอร์เรียนรู้แล้วทำการสร้างเป็นโมเดล สำหรับการเรียนรู้เสียง (Voice Training) การวิจัยนี้ใช้ขั้นตอนวิธี แบบจำลองส่วนผสมเกาส์เซียน (Gaussian Mixture Model) ซึ่งผลลัพธ์จากขั้นตอนการเรียนรู้ของเครื่องคอมพิวเตอร์นี้จะได้แบบจำลองหรือโมเดลสำหรับการเรียนรู้ของเครื่องคอมพิวเตอร์ ดังรูปที่ 3.4

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 3.4 เฟสการเรียนรู้ของเครื่อง (Training Phase)

3) เฟสการพิสูจน์ตัวจริง (Authentication Phase)

กระบวนการรู้จำเป็นกระบวนการที่สามารถใช้เพื่อยืนยันตัวตนหรือการตรวจสอบตัวบุคคลโดยการใช้ข้อมูลชีวมิติ ดังรูปที่ 3.5 คุณลักษณะเด่นของใบหน้าหรือเสียงเปรียบเทียบกับคุณลักษณะเด่นของใบหน้าหรือเสียงที่จัดเก็บไว้ในฐานข้อมูล สำหรับกระบวนการรู้จำภาพใบหน้าการวิจัยนี้ใช้ เทคนิค LBPH (Local Binary Pattern Histogram) สำหรับการรู้จำเสียงการวิจัยนี้ใช้การแจกแจงความน่าจะเป็นแบบผสมตามขั้นตอนวิธี MFCC ผลคะแนนที่ได้จากการเปรียบเทียบของชีวมิติทั้งสองแบบจะนำคะแนนมารวมกันเพื่อใช้กำหนดว่าการพิสูจน์ตัวจริงผ่านหรือไม่โดยผู้วิจัยกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่ร้อยละ 60 เนื่องจากผลการทดลองเชิงประจักษ์จากการวิจัยนี้พบว่า การใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันในการพิสูจน์ตัวจริงเพื่อเข้าใช้การบริการประมวลผลแบบคลาวด์มีค่าอยู่ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบในการพิสูจน์ตัวจริงโดยใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันเพื่อใช้บริการบนการประมวลผลแบบคลาวด์ได้ในอัตราร้อยละ 60

รูปที่ 3.5 เฟสการพิสูจน์ตัวจริง (Authentication Phase)

3.2 การออกแบบและพัฒนาระบบ

งานวิจัยนี้มีการออกแบบระบบโดยใช้เครื่องมือการออกแบบ ตัวอย่างเช่น แผนภาพการใช้งานผู้ใช้ (Use Case Diagram) แผนภาพแสดงความสัมพันธ์ของเอนทิตี้ (E-R diagram) พจนานุกรมข้อมูล (Data Dictionary) และแผนภาพการทำงาน (Flow Diagram) พิจารณาแผนภาพการใช้งานผู้ใช้ (Use Case Diagram) ดังรูปที่3.6 ประกอบด้วยผู้ใช้ที่เกี่ยวข้องกับระบบจำนวน 3 กลุ่มได้แก่ ผู้เรียน อาจารย์ และผู้ดูแลระบบ ผู้เรียนในระบบนี้สามารถการกระทำได้แก่ การลงทะเบียนเรียน การแก้ไขวิชาที่ลงทะเบียน การแสดงวิชาที่ลงทะเบียนเรียน การลงรายวิชาที่เปิดให้ลงทะเบียนเรียน การแสดงรายวิชาที่เปิดให้สอบออนไลน์ การล็อกอินเข้าสู่ระบบเพื่อเข้าสอบออนไลน์ ส่วนการกระทำของอาจารย์ ประกอบด้วย การแสดงรายวิชาที่เปิดให้ลงทะเบียน การแสดงรายวิชาที่เปิดให้สอบออนไลน์ การล็อกอินเข้าสู่ระบบเพื่อเข้าสอบออนไลน์ และส่วนการกระทำของผู้ดูแลระบบประกอบด้วย การสร้าง/การแก้ไข/การแสดงรายวิชาที่เปิดให้ลงทะเบียน การสร้าง การแก้ไข หรือการแสดงรายวิชาที่เปิดให้สอบออนไลน์ และการกำหนดอาจารย์ในการสอบออนไลน์

รูปที่ 3.6 แผนภาพการใช้งานผู้ใช้ (Use Case Diagram)

รูปที่ 3.7 แผนภาพแสดงความสัมพันธ์ของเอนทิตี้ (E-R Diagram)

พิจารณาแผนภาพแสดงความสัมพันธ์ของเอนทิตี้ (E-R Diagram) ดังรูปที่3.7 ประกอบด้วยเอนทิตีจำนวน 8 เอนทิตี้ ได้แก่ ผู้เรียน (Students) อาจารย์ (Instructors) ผู้ดูแลระบบ (Administrators) วิชาเรียน (Courses) วิชาเรียน_ผู้เรียน (Courses_Students) การสอบ (Examinations) และการสอบของผู้เรียน (Exam_Students) แต่ละเอนทิตีมีความสัมพันธ์กันดังภาพ ตัวอย่างเช่น ผู้เรียนหลายคนสามารถลงทะเบียนวิชาเดิมได้หากเป็นคนละภาคการศึกษาหรือคนละปีการศึกษา และวิชาหนึ่งวิชาสามารถมีผู้เรียนได้มากกว่าหนึ่งคนได้ ดังนั้นเอนทิตีวิชาเรียนและผู้เรียนจึงมีความพันธ์แบบ หลายต่อหลาย (Many-to-many) ผู้เรียนหลายคนสามารถลงทะเบียนเพื่อสอบออนไลน์วิชาเดิมได้หากเป็นคนละภาคการศึกษาหรือคนละปีการศึกษา และการสอบออนไลน์สามารถหนึ่งวิชาสามารถมีผู้เรียนได้มากกว่าหนึ่งคนได้ ดังนั้นเอนทิตีการสอบออนไลน์และผู้เรียนจึงมีความพันธ์แบบ หลายต่อหลาย (Many-to-many) เอนทิตีทั้งหมดจะผ่านกระบวนการทำให้อยู่ในรูปแบบปกติ (Normalization Form)

พจนานุกรมข้อมูล (Data Dictionary)

หลังจากทำการพัฒนาแผนภาพแสดงความสัมพันธ์ของเอนทิตี้ (E-R Diagram) แล้วขั้นตอนต่อไปจะนำผลที่ได้มาพัฒนาต่อเป็นพจนานุกรมข้อมูล (Data Dictionary) เพื่อจะได้นำไปสู่การสร้างตารางข้อมูลในฐานข้อมูลเพื่อนำมาใช้งานกับระบบการจัดการฐานข้อมูล (Database Management System) พจนานุกรมข้อมูลของการวิจัยนี้แสดงในตารางที่ 3.1 ถึง 3.8 มีรายละเอียดดังนี้

ตารางที่ 3.1 ตารางข้อมูลผู้เรียน (Students)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Stu_No	Number	10	Primary Key	เลขลำดับข้อมูลผู้เรียน
Students_Id	Number	10	Alternate Key	เลขรหัสผู้เรียน
Fname	Varchar	50		ชื่อผู้เรียน
Lname	Varchar	50		นามสกุลผู้เรียน
Email	Varchar	50		อีเมลผู้เรียน
Password	Varchar	50		รหัสผ่าน
Telephone	Varchar	10		เบอร์โทรศัพท์
Status	Number	1		สถานะผู้เรียน 0=ปิด 1=ปกติ 2=ลบ
Voice	Varchar	255		ไฟล์เสียงผู้เรียน
Pic1	Varchar	255		ไฟล์รูปที่ 1 ของผู้เรียน
Pic2	Varchar	255		ไฟล์รูปที่ 2 ของผู้เรียน
Pic3	Varchar	255		ไฟล์รูปที่ 3 ของผู้เรียน
Pic4	Varchar	255		ไฟล์รูปที่ 4 ของผู้เรียน
Pic5	Varchar	255		ไฟล์รูปที่ 5 ของผู้เรียน
Pic6	Varchar	255		ไฟล์รูปที่ 6 ของผู้เรียน
Pic7	Varchar	255		ไฟล์รูปที่ 7 ของผู้เรียน
Pic8	Varchar	255		ไฟล์รูปที่ 8 ของผู้เรียน
Pic9	Varchar	255		ไฟล์รูปที่ 9 ของผู้เรียน

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.1 ตารางข้อมูลผู้เรียน (Students) (ต่อ)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Pic10	Varchar	255		ไฟล์รูปที่ 10 ของผู้เรียน
Pic11	Varchar	255		ไฟล์รูปที่ 11 ของผู้เรียน
Pic12	Varchar	255		ไฟล์รูปที่ 12 ของผู้เรียน
Pic13	Varchar	255		ไฟล์รูปที่ 13 ของผู้เรียน
Pic14	Varchar	255		ไฟล์รูปที่ 14 ของผู้เรียน
Pic15	Varchar	255		ไฟล์รูปที่ 15 ของผู้เรียน
Pic16	Varchar	255		ไฟล์รูปที่ 16 ของผู้เรียน
Pic17	Varchar	255		ไฟล์รูปที่ 17 ของผู้เรียน
Pic18	Varchar	255		ไฟล์รูปที่ 18 ของผู้เรียน
Pic19	Varchar	255		ไฟล์รูปที่ 19 ของผู้เรียน
Pic20	Varchar	255		ไฟล์รูปที่ 20 ของผู้เรียน

ตารางที่ 3.2 ตารางข้อมูลอาจารย์ (Instructors)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Instr_No	Number	10	Primary Key	เลขลำดับข้อมูลอาจารย์
Instructors_Id	Number	10	Alternate Key	เลขรหัสอาจารย์
Fname	Varchar	50		ชื่ออาจารย์
Lname	Varchar	50		นามสกุลอาจารย์
Email	Varchar	50		อีเมลอาจารย์
Password	Varchar	50		รหัสผ่าน
Telephone	Varchar	10		เบอร์โทรศัพท์
Status	Number	1		สถานะอาจารย์ 0=ปิด 1=ปกติ 2=ลบ
Voice	Varchar	255		ไฟล์เสียงอาจารย์
Pic1	Varchar	255		ไฟล์รูปที่ 1 ของอาจารย์
Pic2	Varchar	255		ไฟล์รูปที่ 2 ของอาจารย์
Pic3	Varchar	255		ไฟล์รูปที่ 3 ของอาจารย์

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.2 ตารางข้อมูลอาจารย์ (Instructors) (ต่อ)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Pic4	Varchar	255		ไฟล์รูปที่ 4 ของอาจารย์
Pic5	Varchar	255		ไฟล์รูปที่ 5 ของอาจารย์
Pic6	Varchar	255		ไฟล์รูปที่ 6 ของอาจารย์
Pic7	Varchar	255		ไฟล์รูปที่ 7 ของอาจารย์
Pic8	Varchar	255		ไฟล์รูปที่ 8 ของอาจารย์
Pic9	Varchar	255		ไฟล์รูปที่ 9 ของอาจารย์
Pic10	Varchar	255		ไฟล์รูปที่ 10 ของอาจารย์
Pic11	Varchar	255		ไฟล์รูปที่ 11 ของอาจารย์
Pic12	Varchar	255		ไฟล์รูปที่ 12 ของอาจารย์
Pic13	Varchar	255		ไฟล์รูปที่ 13 ของอาจารย์
Pic14	Varchar	255		ไฟล์รูปที่ 14 ของอาจารย์
Pic15	Varchar	255		ไฟล์รูปที่ 15 ของอาจารย์
Pic16	Varchar	255		ไฟล์รูปที่ 16 ของอาจารย์
Pic17	Varchar	255		ไฟล์รูปที่ 17 ของอาจารย์
Pic18	Varchar	255		ไฟล์รูปที่ 18 ของอาจารย์
Pic19	Varchar	255		ไฟล์รูปที่ 19 ของอาจารย์
Pic20	Varchar	255		ไฟล์รูปที่ 20 ของอาจารย์

ตารางที่ 3.3 ตารางข้อมูลผู้ดูแลระบบ (Administrators)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Admin_ID	Number	10	Primary Key	เลขลำดับข้อมูลผู้ดูแลระบบ
Administrators_Id	Number	10	Alternate Key	เลขรหัสผู้ดูแลระบบ
Fname	Varchar	50		ชื่อผู้ดูแลระบบ
Lname	Varchar	50		นามสกุลผู้ดูแลระบบ
Email	Varchar	50		อีเมลผู้ดูแลระบบ
Password	Varchar	50		รหัสผ่าน
Telephone	Varchar	10		เบอร์โทรศัพท์

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.3 ตารางข้อมูลผู้ดูแลระบบ (Administrators) (ต่อ)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Status	Number	1		สถานะผู้ดูแลระบบ 0=ปิด 1=ปกติ 2=ลบ
Voice	Varchar	255		ไฟล์เสียงผู้ดูแลระบบ
Pic1	Varchar	255		ไฟล์รูปที่ 1 ของผู้ดูแลระบบ
Pic2	Varchar	255		ไฟล์รูปที่ 2 ของผู้ดูแลระบบ
Pic3	Varchar	255		ไฟล์รูปที่ 3 ของผู้ดูแลระบบ
Pic4	Varchar	255		ไฟล์รูปที่ 4 ของผู้ดูแลระบบ
Pic5	Varchar	255		ไฟล์รูปที่ 5 ของผู้ดูแลระบบ
Pic6	Varchar	255		ไฟล์รูปที่ 6 ของผู้ดูแลระบบ
Pic7	Varchar	255		ไฟล์รูปที่ 7 ของผู้ดูแลระบบ
Pic8	Varchar	255		ไฟล์รูปที่ 8 ของผู้ดูแลระบบ
Pic9	Varchar	255		ไฟล์รูปที่ 9 ของผู้ดูแลระบบ
Pic10	Varchar	255		ไฟล์รูปที่ 10 ของผู้ดูแลระบบ
Pic11	Varchar	255		ไฟล์รูปที่ 11 ของผู้ดูแลระบบ
Pic12	Varchar	255		ไฟล์รูปที่ 12 ของผู้ดูแลระบบ
Pic13	Varchar	255		ไฟล์รูปที่ 13 ของผู้ดูแลระบบ
Pic14	Varchar	255		ไฟล์รูปที่ 14 ของผู้ดูแลระบบ
Pic15	Varchar	255		ไฟล์รูปที่ 15 ของผู้ดูแลระบบ
Pic16	Varchar	255		ไฟล์รูปที่ 16 ของผู้ดูแลระบบ
Pic17	Varchar	255		ไฟล์รูปที่ 17 ของผู้ดูแลระบบ
Pic18	Varchar	255		ไฟล์รูปที่ 18 ของผู้ดูแลระบบ
Pic19	Varchar	255		ไฟล์รูปที่ 19 ของผู้ดูแลระบบ
Pic20	Varchar	255		ไฟล์รูปที่ 20 ของผู้ดูแลระบบ

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.4 ตารางข้อมูลวิชา (Courses)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Courses_No	Number	10	Primary Key	เลขลำดับข้อมูลวิชา
Courses_Id	Number	10	Alternate Key	เลขรหัสวิชา
Name	Varchar	100		ชื่อวิชา
Semester	Number	50		ภาคการศึกษา
Year	Number	4		ปีการศึกษา
Instructors_ID	Number	10	FK (Instructors)	รหัสอาจารย์
Status	Number	1		สถานะวิชา 0=ปิด 1= ปกติ 2=ลบ

ตารางที่ 3.5 ตารางข้อมูลวิชาที่ผู้เรียนลงทะเบียน (Courses_Students)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Cour_Stu_Id	Number	10	Primary Key	เลขลำดับข้อมูลวิชาที่ผู้เรียนลงทะเบียน
Courses_Id	Number	10	FK (Courses)	เลขรหัสวิชา
Students_Id	Varchar	100	FK (Students)	เลขรหัสผู้เรียน
Status	Number	1	0..9	สถานะวิชาที่ผู้เรียนลงทะเบียน 0=ปิด 1=ปกติ 2=ลบ

ตารางที่ 3.6 ตารางข้อมูลการสอบ (Examinations)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Exam_No	Number	10	Primary Key	เลขลำดับการสอบ
Examinations_Id	Number	10	Alternate Key	เลขรหัสการสอบ
StartDateTime	DateTime	8		วัน-เวลาที่เริ่มสอบ
EndDateTime	DateTime	8		วัน-เวลาที่สิ้นสุดการสอบ
Courses_Id	Number	10	FK (Courses)	รหัสวิชา
Exam_Link	Varchar	255		ลิงค์การสอบ

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.6 ตารางข้อมูลการสอบ (Examinations) (ต่อ)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Status	Number	1	0..9	สถานะการสอบ 0=ปิด 1=ปกติ 2=ลบ

ตารางที่ 3.7 ตารางข้อมูลการสอบของผู้เรียน (Exam_Students)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
ExamStu_No	Number	10	Primary Key	เลขลำดับการสอบของผู้เรียน
Exam_Id	Number	10	Alternate Key	เลขรหัสการสอบ
Students_Id	Number	10	FK (Students)	เลขรหัสผู้เรียน
Courses_Id	Number	10	FK (Courses)	เลขรหัสวิชา
EntryDateTime	DateTime	8		วัน-เวลาที่เข้าสอบ
Exam_Score	Number	4		คะแนนสอบ
Status	Number	1	0..9	สถานะการสอบ 0=ปิด 1=ปกติ 2=ลบ

ตารางที่ 3.8 ตารางข้อมูลการเข้าสู่ระบบ (Authen_Log)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Log_No	Number	10	Primary Key	เลขลำดับข้อมูลการสอบของผู้เรียน
Log_Id	Number	10	Alternate Key	เลขรหัสการเข้าสู่ระบบ
Log_DateTime	DateTime	10		วันเวลาการเข้าสู่ระบบ
Student_ID	Number	10	FK (Students)	เลขรหัสผู้เรียน
Face_Score	Number	10,5		คะแนนการตรวจสอบจากใบหน้า
Face_Time	Number	10		เวลาที่ใช้การตรวจสอบจากใบหน้า
Voice_Score	Number	10,5		คะแนนการตรวจสอบจากเสียง

มหาวิทยาลัยรังสิต Rangsit University

ตารางที่ 3.8 ตารางข้อมูลการเข้าสู่ระบบ (Authen_Log) (ต่อ)

ชื่อฟิลด์	ชนิดข้อมูล	ความยาว	ข้อกำหนด	คำอธิบาย
Voice_Time	Number	10		เวลาที่ใช้การตรวจสอบจากเสียง
Total_Time	Number	11		เวลารวมที่ใช้การตรวจสอบ
Fusion_Score	Number	10,5		คะแนนรวมการตรวจสอบ
FS_Result	Number	1		จำนวนครั้งการตรวจสอบ
Password_Result	Number	10		จำนวนครั้งการใช้รหัสผ่าน
Status	Number	1	0..9	สถานะการสอบ 0=ปิด 1=ปกติ 2=ลบ

รูปที่ 3.8 แผนภาพการทำงานของระบบ (Flow Diagram)

มหาวิทยาลัยรังสิต Rangsit University

แผนภาพการทำงานของระบบ (Flow Diagram) ในส่วนของผู้เรียน ดังรูปที่ 3.8 แสดงให้เห็นลำดับขั้นตอนการทำงานของผู้เรียน เริ่มจากผู้เรียนใช้อุปกรณ์ได้แก่ ไอโฟน แอนดรอยด์ สมาร์ตโฟน คอมพิวเตอร์ส่วนบุคคล หรือโน้ตบุ๊ก คอมพิวเตอร์ในการล็อกอินเพื่อยืนยันตัวตนเข้าใช้งานระบบการสอบออนไลน์ ผู้เรียนสามารถใช้ถ่ายภาพใบหน้าตนเองเพื่อเป็นการพิสูจน์ตัวจริง โดยใช้กล้องถ่ายภาพของอุปกรณ์ที่มีอยู่ในอุปกรณ์ จากนั้นผู้เรียนสามารถใช้ไมโครโฟนเพื่อป้อนข้อมูลเสียงของตนเองเพื่อเป็นการพิสูจน์ตัวจริง เมื่อผู้ใช้กดปุ่ม Login ระบบจะทำการนำไฟล์ภาพใบหน้าและเสียงของผู้เรียนไปเก็บไว้ที่เครื่องคอมพิวเตอร์แม่ข่าย จากนั้นโมดูลที่ทำหน้าที่พิสูจน์ตัวจริงของผู้ที่เข้าใช้งานระบบจะนำข้อมูลเข้าสู่กระบวนการพิสูจน์ตัวจริง

3.3 ประชากรและกลุ่มตัวอย่าง

การวิจัยนี้เป็นการวิจัยเชิงทดลองที่ต้องให้บุคคลที่เป็นกลุ่มเป้าหมายเข้ามาใช้งาน ทดสอบและทดลองระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ โดยใช้เครื่องคอมพิวเตอร์ ประชากรการวิจัยนี้คือนักศึกษาภาควิชาวิทยาการคอมพิวเตอร์ และภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศและนวัตกรรม มหาวิทยาลัยกรุงเทพ มีอายุระหว่าง 16- 25 ปี ที่ลงทะเบียนเรียนในภาคการศึกษาที่ 1 ปีการศึกษา 2563 มีจำนวน 291 คน โดยนักศึกษาที่เป็นกลุ่มประชากรการศึกษามีพื้นฐานการใช้งานโปรแกรมและคอมพิวเตอร์ประเภทต่าง ๆ ได้เป็นอย่างดี

สุวิมล ว่องวาณิช และนงลักษณ์ วิรัชชัย (2546) กล่าวถึงขนาดของกลุ่มตัวอย่างมีความสำคัญอย่างมากในการวิจัยเมื่อกลุ่มตัวอย่างมีความเหมาะสมข้อมูลที่ได้จากกลุ่มตัวอย่างมีมากพอก็จะทำให้ผลงานวิจัยนั้นมีคุณค่า ขนาดของกลุ่มตัวอย่างเท่าไรจึงจะเหมาะสมกับการวิจัยขึ้นอยู่กับการวิจัยว่าจะยอมให้เกิดความคลาดเคลื่อนมากน้อยเพียงใด จึงจะยอมรับได้ การหาขนาดตัวอย่างสามารถคำนวณได้จากสูตรในกรณีที่ต้องการประมาณค่าเฉลี่ยของประชากร และในกรณีที่ประมาณค่าสัดส่วนของประชากร และการใช้ตารางการสุ่มตัวอย่างของ Yamane การหาขนาดของกลุ่มตัวอย่างอาจทำได้ 2 ลักษณะ คือ 1) การใช้ตารางหาขนาดตัวอย่างในรูปร้อยละ และ 2) การกำหนดขนาดตัวอย่างตามวัตถุประสงค์การวิจัย การวิจัยนี้เป็นการวิจัยเชิงทดลอง ผู้วิจัยได้กำหนดขนาดของตัวอย่างตามวัตถุประสงค์การวิจัยไว้ อย่างน้อยคือกลุ่มละ 20 คน

ผู้วิจัยใช้การคัดเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) ซึ่งสอดคล้องกับวัตถุประสงค์การวิจัยโดยกลุ่มตัวอย่างคือนักศึกษาที่ลงทะเบียนเรียนวิชา CS320: โครงสร้างและสถาปัตยกรรมคอมพิวเตอร์ ในภาคการศึกษาที่ 1 ปีการศึกษา 2563 จำนวน 152 คน แต่มีผู้ที่เข้าร่วมการวิจัยจำนวน 80 คน โดยนักศึกษาที่เป็นกลุ่มตัวอย่างนี้ส่วนใหญ่เป็นนักศึกษาชั้นปีที่ 2 ซึ่งมีพื้นฐานการใช้งานโปรแกรมและคอมพิวเตอร์ประเภทต่าง ๆ ได้เป็นอย่างดี เนื่องจากช่วงระยะเวลานี้อยู่ในช่วงสถานการณ์การแพร่ระบาดของโรคโควิด-19 ทำให้การเรียนการสอนต้องทำรูปแบบการเรียนออนไลน์ และบางช่วงมีการจัดการเรียนการสอนแบบผสมผสาน (Blended Learning) ทำให้เกิดความไม่สะดวกในการสื่อสารและจัดเก็บข้อมูลจากกลุ่มตัวอย่างด้วยวิธีการเก็บข้อมูลจากผู้เรียนในห้องเรียน นอกจากนี้การวิจัยนี้มีการจัดเก็บข้อมูลชีวมิติได้แก่ ข้อมูลภาพใบหน้าและข้อมูลเสียงของกลุ่มตัวอย่างซึ่งเป็นข้อมูลส่วนบุคคล จึงต้องได้รับการยินยอมจากกลุ่มตัวอย่างที่มีความประสงค์ในการให้ข้อมูลการวิจัย

3.4 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัยเป็นสิ่งที่มีความสำคัญและมีบทบาทอย่างมากในการวิจัย การเลือกใช้เครื่องมือขึ้นอยู่หลายปัจจัย ตัวอย่างเช่น สถานการณ์และลักษณะพฤติกรรมที่ต้องการจะวัด เครื่องมือที่ใช้ในการวิจัยจะต้องสอดคล้องกับวัตถุประสงค์การวิจัย จากการศึกษาพบว่าเครื่องมือวิจัยที่นิยมใช้ในการเก็บรวบรวมข้อมูลมี 5 ประเภท ได้แก่ แบบทดสอบ แบบสังเกต แบบสัมภาษณ์ แบบสอบถาม และแบบประเมินการปฏิบัติ เครื่องมือแต่ละประเภทจะมีคุณลักษณะที่สำคัญและความสามารถในการเก็บรวบรวมข้อมูลได้แตกต่างกันออกไป เพื่อให้ผู้วิจัยสามารถเลือกใช้เครื่องมือได้เหมาะสมกับวัตถุประสงค์การวิจัย การวิจัยนี้ใช้เครื่องการวิจัยคือการประเมินการปฏิบัติงานหรือการทดลอง โดยผู้วิจัยได้พัฒนาระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ โดยใช้อุปกรณ์โมไบล์หรือเครื่องคอมพิวเตอร์ ที่พัฒนานี้ใช้เทคโนโลยีเว็บแอปพลิเคชันที่ทำงานอยู่บนการประมวลผลแบบคลาวด์ ช่วยให้กลุ่มตัวอย่างสามารถเข้าถึงและเข้าใช้งานเพื่อทดสอบระบบได้จากที่ใดก็ได้และสามารถใช้บนอุปกรณ์ได้หลายชนิดที่มีโปรแกรมเว็บเบราเซอร์ แล้วให้กลุ่มตัวอย่างทำการทดลองใช้งานระบบ

3.5 การเก็บรวบรวมข้อมูล

ผู้วิจัยได้ทำการอธิบาย ชี้แจง และสอบถามกลุ่มตัวอย่างในการยินยอมที่จะเข้าร่วมการวิจัยในครั้งนี้ผ่านทางโปรแกรมซูม (Zoom) แบบออนไลน์เนื่องจากช่วงระยะเวลานี้อยู่ในช่วงสถานการณ์การแพร่ระบาดของโรคโควิด-19 ทำให้การเรียนการสอนต้องทำรูปแบบการเรียนออนไลน์ โดยผู้วิจัยซึ่งเป็นผู้สอนวิชา CS320: โครงสร้างและสถาปัตยกรรมคอมพิวเตอร์ ภาคการศึกษาที่ 1 ปีการศึกษา 2563 มีผู้ที่เข้าร่วมการวิจัยจำนวน 80 คน โดยผู้วิจัยได้พัฒนาระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้อุปกรณ์โมไบล์หรือเครื่องคอมพิวเตอร์แล้วให้กลุ่มตัวอย่างทำการทดลองใช้งานระบบ เนื่องจากระบบที่พัฒนานี้ใช้เทคโนโลยีเว็บแอปพลิเคชันที่ทำงานอยู่บนการประมวลผลแบบคลาวด์ ช่วยให้กลุ่มตัวอย่างสามารถเข้าถึงและเข้าใช้งานเพื่อทดสอบระบบได้จากที่ใดก็ได้และสามารถใช้บนอุปกรณ์ได้หลายชนิดที่มีโปรแกรมเว็บเบราเซอร์ ข้อมูลที่จะได้จากการทดสอบระบบจะถูกจัดเก็บไว้ในระบบการจัดการฐานข้อมูลบนการประมวลผลแบบคลาวด์ จากนั้นผู้วิจัยจะนำผลการเก็บรวบข้อมูลมาใช้ในกระบวนการวิเคราะห์ข้อมูลต่อไป

3.6 การวิเคราะห์ข้อมูล

ผู้วิจัยได้ออกแบบการวิเคราะห์ข้อมูล (Analysis Design) ซึ่งเป็นกระบวนการในการเลือกแบบการวิเคราะห์ให้เหมาะสมกับข้อมูลที่เก็บรวบรวมมาได้อันจะนำไปสู่การตอบคำถามตามวัตถุประสงค์และสมมติฐานการวิจัย แบบการวิเคราะห์ข้อมูลสามารถแบ่งตามประเภทของข้อมูล คือ การวิเคราะห์ข้อมูลเชิงคุณภาพ (Qualitative Data Analysis) และการวิเคราะห์สำหรับข้อมูลเชิงปริมาณ (Quantitative Data Analysis)

การทดสอบไคสแควร์ (Chi-Square Test) เป็นสถิติแบบนอนพาราเมตริก (Nonpara -metric Statistics) ซึ่งเป็นสถิติที่ไม่คำนึงถึงลักษณะการแจกแจงของประชากร เป็นวิธีการทดสอบเพื่อเปรียบเทียบข้อมูลที่อยู่ในรูปของความถี่หรือในรูปของสัดส่วน ซึ่งข้อมูลที่ศึกษาไม่สามารถวัดค่าออกมาเป็นตัวเลขที่แน่นอน แต่สามารถจำแนกออกเป็นหมวดหมู่ได้ ตัวอย่างเช่น มากที่สุด มาก ปานกลาง น้อย หรือน้อยที่สุด เป็นต้น ซึ่งเป็นข้อมูลที่เกิดจากการเก็บรวบรวมจากตัวแปรที่เกี่ยวข้องแล้วจำแนกออกมาเป็นความถี่หรือสัดส่วน ถ้าหากต้องการศึกษาว่าการแจกแจงความถี่ของข้อมูลที่ได้จากตัวแปรหนึ่งเป็นไปลักษณะใด หรือถ้าหากต้องการเปรียบเทียบตัวแปร 2

กลุ่มหรือมากกว่า 2 กลุ่มว่ามีความสัมพันธ์กันหรือไม่ การทดสอบไคสแควร์เป็นสถิติหนึ่งที่เหมาะสมกับลักษณะของการศึกษาข้างต้น โดยสรุปการทดสอบไคสแควร์เป็นวิธีการทางสถิติหนึ่งที่นิยมใช้ในการเปรียบเทียบหรือทดสอบข้อมูลที่เป็นความถี่หรือข้อมูลที่อยู่ในรูปของสัดส่วน โดยเฉพาะการใช้วิเคราะห์ข้อมูลจากการแบบสอบถามแบบมาตราส่วน การวิจัยนี้ใช้การทดสอบไคสแควร์ เพื่อทดสอบสมติฐานว่าระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลที่นำเสนอมีความสัมพันธ์หรือเกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้โมไบล์หรือเครื่องคอมพิวเตอร์ในการเข้าสอบออนไลน์ของผู้เรียนในระดับอุดมศึกษาหรือไม่

นอกจากนี้ผู้วิจัยประเมินผลระเบียบวิธีที่นำเสนอด้วยการใช้ข้อมูลเก็บรวบรวมไว้ในตารางคอนฟิวชันเมทริกซ์ (Confusion Matrix) โดยใช้สถิติพรรณนาซึ่งเป็นสถิติที่เกี่ยวข้องกับการวิเคราะห์และการบรรยายถึงลักษณะของข้อมูลที่เก็บรวบรวมมา เช่น การแจกแจงข้อมูล การนำเสนอข้อมูล การหาค่ากลาง การวัดการกระจาย เป็นต้น ค่าของข้อมูลตารางคอนฟิวชันเมทริกซ์ประกอบด้วย ค่าคะแนนความถูกต้อง คะแนนความแม่นยำ คะแนนรีคอล หรือค่าเอฟวัน ใช้เพื่อวิเคราะห์ประเมินผลความถูกต้อง ความแม่นยำ และความคลาดเคลื่อนของผลการทำนายจากโมเดลของเรียนรู้ของเครื่อง (Machine Learning) ที่ถูกใช้ในการรู้จำของระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลโดยใช้การรู้จำภาพใบหน้าและเสียง ตารางคอนฟิวชันเมทริกซ์ประกอบด้วยจำนวนครั้งของผลการทำนายทั้งที่ระบบทำนายถูกและทำนายไม่ถูก รวมทั้งจำนวนครั้งของค่าความจริงของการเป็นสมาชิกหรือไม่เป็นสมาชิกของข้อมูลผู้ที่นำมาทดสอบ ตารางคอนฟิวชันเมทริกซ์นี้ใช้สำหรับการวิเคราะห์เชิงคาดการณ์ซึ่งเป็นสถิติที่สามารถใช้เพื่อสกัดข้อมูลจากข้อมูลและคาดการณ์แนวโน้มและรูปแบบของพฤติกรรม การวิเคราะห์เชิงคาดการณ์ประกอบด้วยขั้นตอนวิธีของการเรียนรู้เชิงลึก การสร้างแบบจำลองข้อมูล และการทำเหมืองข้อมูล การวิจัยนี้มีการประเมินผลด้านต่าง ๆ ดังนี้ (Tharwat, 2018; Chicco & Jurman, 2020; Piryonesi & ElDiraby, 2020; Chicco et al., 2021).

1) คะแนนความถูกต้อง (Accuracy Score) เป็นการวัดทางสถิติที่คำนวณจากอัตราส่วนของผลการพยากรณ์ว่าถูกต้องเทียบกับจำนวนครั้งของการทดสอบทั้งหมด สมการที่ (3-1) ใช้ในการคำนวณหาคะแนนความถูกต้อง

$$\text{Accuracy} = \frac{\sum\left(\text{True}_{\text{positive}}\right) + \sum\left(\text{True}_{\text{negative}}\right)}{\sum\left(\text{Total_population}\right)} \tag{3-1}$$

2) คะแนนความแม่นยำ (Precision) คะแนนความแม่นยำนี้สามารถแสดงได้ 2 มิติคือ ด้านที่เป็นบวก (Positive) และด้านที่เป็นลบ (Negative) คะแนนความแม่นยำด้านบวกแสดงถึงการพยากรณ์ที่ถูกต้องว่าผู้ใช้เป็นสมาชิกที่ได้ลงทะเบียนไว้จริงจากจำนวนการพยากรณ์ที่ถูกต้องทั้งหมด ส่วนคะแนนความแม่นยำด้านลบแสดงถึงอัตราส่วนของจำนวนครั้งที่ระบบพยากรณ์ถูกต้องว่าผู้ที่พิสูจน์ตัวจริงเป็นผู้ที่ไม่เป็นสมาชิกของระบบ และความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบกับจำนวนครั้งทั้งหมดของการพยากรณ์ถูกต้องและไม่ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบ สมการที่ (3-2) ใช้ในการคำนวณคะแนนความแม่นยำด้านบวก (Precision_Positive) สมการที่ (3-3) ใช้ในการคำนวณคะแนนความแม่นยำด้านลบ (Precision_Negative)

$$\text{Precision_Positive} = \frac{(\text{True}_{\text{positive}})}{(\text{True}_{\text{positive}} + \text{False}_{\text{positive}})} \tag{3-2}$$

$$\text{Precision_Negative} = \frac{(\text{True}_{\text{negative}})}{(\text{True}_{\text{negative}} + \text{False}_{\text{negative}})} \tag{3-3}$$

3) คะแนนรีคอลด้านบวก (Recall_Positive) แสดงถึงอัตราส่วนของจำนวนครั้งที่ระบบพยากรณ์ว่าผู้ที่พิสูจน์ตัวจริงเป็นผู้ที่เป็นสมาชิกของระบบและความจริงคือผู้พิสูจน์ตัวจริงนั้นเป็นสมาชิกของระบบจริงเทียบกับจำนวนครั้งของการพยากรณ์ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นเป็นสมาชิกของระบบจริงรวมกับจำนวนครั้งของการพยากรณ์ไม่ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบ สมการที่ (3-4) ใช้ในการคำนวณคะแนนความแม่นยำด้านบวก (Precision_Positive) คะแนนรีคอลด้านลบ (Recall_Negative) แสดงถึงอัตราส่วนของจำนวนครั้งที่ระบบพยากรณ์ว่าผู้ที่พิสูจน์ตัวจริงเป็นผู้ที่ไม่เป็นสมาชิกของระบบและความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบเทียบกับจำนวนครั้งของการพยากรณ์ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบจริงรวมกับจำนวนครั้งของการพยากรณ์ไม่ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นเป็นสมาชิกของระบบ สมการที่ (3-5) ใช้ในการคำนวณคะแนนความแม่นยำด้านลบ (Precision_Negative)

$$\text{Recall_Positive} = \frac{(\text{True}_{\text{positive}})}{(\text{True}_{\text{positive}} + \text{False}_{\text{negative}})} \tag{3-4}$$

มหาวิทยาลัยรังสิต Rangsit University

$$\text{Recall_Negative} = \frac{\left(\text{True}_{\text{negative}}\right)}{\left(\text{True}_{\text{negative}} + \text{False}_{\text{positive}}\right)} \tag{3-5}$$

4. คะแนนเอฟวัน (F1 Score) หรือเรียกว่าค่าเฉลี่ยฮาร์โมนิก เป็นค่าที่แสดงถึงสมรรถนะการทำงานของระบบโดยเป็นการคำนวณการหาค่าเฉลี่ยของค่าคะแนนความแม่นยำ (Precision) และค่าคะแนนรีคอล (Recall) สมการที่ (3-6) ใช้ในการคำนวณคะแนนเอฟวัน

$$\text{F1 Score} = \frac{2PR}{(P+R)} \tag{3-6}$$

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 4

ผลการวิจัย

เนื้อหาในบทนี้กล่าวถึง ผลการพัฒนาระบบ ผลการวิจัยการวิเคราะห์ข้อมูลจากตารางคอนฟิวชันเมทริกซ์ (Confusion Matrix) และการใช้ค่าทางสถิติไคสแควร์ (Pearson's Chi Square Statistic) เพื่อวิเคราะห์สมมติฐานวิจัย ค่าทางสถิติไคสแควร์สามารถใช้วิเคราะห์ข้อมูลเชิงปริมาณหรือค่าของข้อมูลอยู่ในมาตรวัดแบบนามบัญญัติและเรียงลำดับ (เป็นข้อมูลเชิงคุณภาพ) ค่าของข้อมูลสามารถแบ่งได้เป็น k กลุ่ม

4.1 ผลการพัฒนาระบบ

สถาปัตยกรรมทางด้านฮาร์ดแวร์และการเชื่อมโยงระบบเครือข่ายของระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติโดยใช้การรู้จำภาพใบหน้าและเสียงบนดอกเกอร์คอนเทนเนอร์ (Docker Container) ดังแสดงในรูปที่ 4.1 บนเครื่องเสมือนที่ทำงานบนระบบการประมวลผลแบบคลาวด์ โดยผู้วิจัยได้ทำการเช่าและใช้บริการเครื่องแม่ข่ายจากบริษัทผู้บริการ โดยเครื่องบริการ (Server) นี้ตั้งอยู่เลขที่ 159 ถ.กรุงศรีใน ต.ในเมือง อ.เมือง จ.สุรินทร์ โดยเครื่องบริการ (Server) มีการติดตั้งระบบปฏิบัติการพร้อมกับเครื่องมือนการบริหารและจัดการเครื่องเสมือนคือ Proxmox Virtual-Environment เวอร์ชัน 6.4-6

มหาวิทยาลัยรังสิต Rangsit University

Proxmox Virtual-Environment 6.4-6 เป็นแพลตฟอร์มการจัดการเครื่องบริการ (Server) แบบโอเพนซอร์ส (Opensource) ที่มีความสามารถในการจัดการกับการจำลองเสมือนได้เป็นอย่างดี Proxmox ใช้ KVM เป็นไฮเปอร์ไวเซอร์ และใช้ Linux (LXC) เป็นเครื่องมือจัดการกับคอนเทนเนอร์ที่เก็บข้อมูลที่เป็นข้อกำหนดของซอฟต์แวร์และฟังก์ชันต่าง ๆ ไว้บนแพลตฟอร์มเดียว Proxmox มีส่วนประสานกับผู้ใช้แบบเว็บแอปพลิเคชันช่วยให้ผู้ดูแลระบบสามารถจัดการเครื่องเสมือนและคอนเทนเนอร์ได้สะดวกมากขึ้น นอกจากนี้มีความสามารถในการสร้างเครื่องเสมือนแบบคลัสเตอร์เพื่อเพิ่มความสามารถในการประมวลผลหรือการทนทานต่อการบกพร่อง (Fault Tolerance) รวมถึงมีเครื่องมือที่ใช้ในการกู้คืนระบบที่อาจเกิดความเสียหายได้เป็นอย่างดี ผู้ดูแลระบบสามารถใช้ Proxmox ในการปรับเพิ่มหรือลดสมรรถนะการประมวลผล พื้นที่จัดเก็บข้อมูล และองค์ประกอบ

ส่วนต่าง ๆ ได้แบบพลวัตตามความต้องการที่มีการเปลี่ยนแปลงได้ ช่วยทำให้มั่นใจได้ว่าระบบเครื่องบริการ (Server) จะปรับให้เข้ากับการเติบโตในอนาคตได้อย่างเป็นพลวัต ดังแสดงในรูปที่ 4.2 จะเห็นว่าระบบคลาวด์ของผู้วิจัยมีการสร้างเครื่องเสมือนไว้จำนวน 13 เครื่อง แต่มีการเปิดเครื่องเสมือนขึ้นมาทำงานจำนวน 8 เครื่อง โดยที่ระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้อุปกรณ์โมไบล์หรือสมาร์ตโฟนจะติดตั้งและทำงานอยู่บนเครื่องเสมือนหมายเลข 3003 ผู้ดูแลระบบสามารถดูและจัดการระบบได้โดยใช้การแสดงผลที่อยู่ด้านขวามือของจอภาพ

เครื่องเสมือนหมายเลข 3003 ที่มีการติดตั้งระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้อุปกรณ์โมไบล์หรือเครื่องคอมพิวเตอร์มีการใช้เทคโนโลยีดอกเกอร์คอนเทนเนอร์ เพื่อใช้ในการติดตั้งโปรแกรมต่าง ๆ แยกออกเป็นส่วน ๆ เป็นการสร้างสภาพแวดล้อมด้านการพัฒนาและการเรียกใช้โปรแกรมต่าง ๆ เพื่อไม่ให้เกิดผลกระทบต่อกัน แต่ละดอกเกอร์คอนเทนเนอร์จะทำงานมีสภาพแวดล้อมที่แตกต่างกัน เครื่องเสมือนหมายเลข 3003 จะมีการสร้างดอกเกอร์คอนเทนเนอร์ที่มีการติดตั้งเครื่องมือและโปรแกรมต่าง ๆ สำหรับใช้พัฒนาและใช้งานระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้อุปกรณ์โมไบล์หรือเครื่องคอมพิวเตอร์ ตัวอย่างเช่น Python 3.x ระบบการจัดการฐานข้อมูล Sqlite3 เฟรมเวิร์ค Djanco เป็นต้น

รูปที่ 4.1 สถาปัตยกรรมดอกเกอร์คอนเทนเนอร์ (Docker Container)

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 4.2 หน้าจอ Proxmox Virtual-Environment 6.4-6

ระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงพัฒนาระบบโดยใช้เทคโนโลยีเว็บที่สามารถทำงานได้หลายแพลตฟอร์มทั้งคอมพิวเตอร์ส่วนบุคคล โน้ตบุ๊ก หรืออุปกรณ์สมาร์ตโฟน เป็นต้น รูปที่ 4.3 แสดงถึงหน้าโฮมเพจของระบบเพื่อให้ผู้เรียนเข้ามาใช้งานระบบโดยการล็อกอินเพื่อพิสูจน์ตัวจริงเพื่อเข้าใช้งานระบบ หากเป็นผู้ใช้รายใหม่จะมีลิงค์ Sign up เพื่อให้ผู้ที่ยังไม่เคยลงทะเบียนไว้สามารถลงทะเบียนก่อนการเข้าใช้งานระบบ โดยผู้ที่ลงทะเบียนใหม่ต้องกรอกข้อมูลพื้นฐานส่วนตัว ได้แก่ ชื่อหรืออีเมลผู้ใช้งาน และต้องป้อนข้อมูลชีวมิติได้แก่ ภาพใบหน้าจำนวน 20 ภาพและบันทึกเสียง ดังแสดงในรูปที่ 4.4 และ 4.5 เมื่อผู้ใช้งานป้อนข้อมูลเสร็จเรียบร้อยแล้ว ระบบจะทำการอัพโหลดข้อมูลและไฟล์ข้อมูลชีวมิติไปยังเครื่องบริการ (Server) ของระบบนี้ซึ่งทำงานอยู่บนระบบการประมวลผลแบบคลาวด์ โดยไฟล์ข้อมูลชีวมิติจะถูกแยกเก็บไว้ในโฟลเดอร์ที่กำหนดไว้เพื่อนำไปใช้ในการสอนระบบให้เรียนรู้ต่อไปด้วย

การเตรียมข้อมูลก่อนการประมวลผล (Preprocessing) ข้อมูลที่ชีวมิติที่รับเข้ามาจำเป็นต้องมีการแยกคุณลักษณะเด่นที่ต้องการไว้ ส่วนข้อมูลใดที่ไม่จำเป็นก็จะทำการนำออกไป ตัวอย่างเช่น ภาพหน้าคน ก็จะทำการตัดเฉพาะส่วนที่เป็นใบหน้าเท่านั้นที่จะมีผลต่อการพิสูจน์ตัวจริง ส่วนเส้นผมหรือส่วนอื่น ๆ ก็จะถูกตัดออกไป ข้อมูลชีวมิติทั้งสองแบบคือภาพใบหน้าและข้อมูลเสียงจะมีกระบวนการในการคัดแยกคุณลักษณะเด่นที่แตกต่างกันเนื่องจากเป็นข้อมูลคนละประเภท

การเตรียมข้อมูลภาพใบหน้าก่อนการประมวลผล (Face Preprocessing) ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การตรวจหาบริเวณดวงตาซึ่งมักเป็นบริเวณที่มีสีเข้มกว่าบริเวณอื่นโดยใช้ขั้นตอนวิธี Haar-cascade และจะมีการปรับขนาด (Scaling) การหมุนภาพ (Rotating) และการแปลงภาพ (Translating) นอกจากนี้จะทำการตัดส่วนของภาพให้เหลือเฉพาะบริเวณใบหน้าเท่านั้นส่วนประกอบอื่นเช่น หน้าผาก คาง ใบหู และภาพพื้นหลังอื่น ๆ ออก ขั้นที่ 2 การใช้เทคนิคฮิสโตแกรม (Histogram of Oriented Gradients) ในการเพิ่มคุณภาพของภาพต้นฉบับโดยการจัดวางตำแหน่งภาพ การปรับความสว่างและความคมชัดให้ด้านซ้ายและด้านขวาของภาพใบหน้า ขั้นที่ 3 การทำเครื่องหมายรูปวงรีเพื่อเป็นการเน้นภาพใบหน้า และจะกำจัดผมและพื้นหลังบางส่วนออกจากภาพใบหน้า ผลลัพธ์ที่ได้คือเฉพาะในรูปภาพใบหน้าเท่านั้น การเตรียมข้อมูลเสียงก่อนการประมวลผล (Voice Preprocessing) เป็นกระบวนการย่อยของกระบวนการการคัดแยกคุณลักษณะเด่น โดยจะมีการปรับความสมดุลความถี่ของเสียงที่รับมาจากอุปกรณ์ไมโครโฟนให้อยู่ในระดับสัญญาณเสียงที่หูของมนุษย์สามารถรับรู้ได้อย่างเหมาะสม

การคัดแยกคุณลักษณะเด่น (Feature Extraction) เป็นนำผลลัพธ์ที่ได้จากขั้นตอนก่อนหน้านี้ทั้งส่วนของข้อมูลชีวมิติภาพใบหน้ามาทำคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองเฉพาะส่วนของตำแหน่ง หรือขนาดของอวัยวะ เช่น ตา จมูก หรือปาก การวิจัยนี้ใช้ขั้นตอนวิธี LBPH (Local Binary Pattern Histogram) ส่วนข้อมูลชีวมิติเสียงจะมาทำการคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์เป็นเทมเพลตหรือแบบจำลองคือเวกเตอร์ของเสียง MFCC ประกอบด้วยขั้นตอนย่อย 3 ขั้นตอน ได้แก่ ขั้นที่ 1 การคัดแยกคุณลักษณะเด่นของข้อมูลเสียง (MFCC Extraction) โดยใช้ขั้นตอนวิธี MFCC จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติ ขั้นที่ 2 การคำนวณค่าเดลตา (Delta) จะทำการสร้างเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติเช่นกัน ดังนั้นเมื่อรวมกันทั้งเวกเตอร์ของเสียงจาก MFCC กับเวกเตอร์ของเสียงที่มีคุณลักษณะ 20 มิติจาก Delta จะได้เวกเตอร์ของเสียงที่มีคุณลักษณะจำนวน 40 มิติ ขั้นที่ 3 ข้อมูลชีวมิติเสียงจะถูกคัดแยกคุณลักษณะที่สำคัญและจะได้ผลลัพธ์คือ เทมเพลตของชีวมิติเสียง

การจัดเก็บลงในฐานข้อมูล (Storing in Database) เป็นการนำเทมเพลตหรือแบบจำลองไปจัดเก็บไว้ในฐานข้อมูลซึ่งอยู่บนระบบการประมวลผลแบบคลาวด์ เพื่อนำไปใช้ในขั้นตอนถัดไป

มหาวิทยาลัยรังสิต Rangsit University

เฟสการเรียนรู้ของเครื่อง (Training Phase) เป็นขั้นตอนที่นำเอาข้อมูลที่ได้จากการแยกคุณลักษณะเด่นที่ต้องการ (Feature Extraction) ของแต่ละบุคคลมาเป็นข้อมูลเพื่อสอนให้คอมพิวเตอร์เรียนรู้ด้วยตนเองว่าลักษณะของโครงสร้างรูปภาพใบหน้าของแต่ละคนมีคุณลักษณะอย่างไร เช่นระยะห่างของตำแหน่งต่าง ๆ ของอวัยวะบนใบหน้า หรือตำแหน่งของอวัยวะต่าง ๆ บนในหน้า เป็นต้น รวมทั้งคุณลักษณะเด่นของเสียงของแต่ละบุคคลด้วยเช่นกัน สำหรับการเรียนรู้ภาพใบหน้า (Facial Training) จะเป็นการนำเอาคุณลักษณะเด่นของภาพใบหน้าที่ได้มาจากเฟสที่ 1 มาสอนให้คอมพิวเตอร์เรียนรู้แล้วทำการสร้างเป็นโมเดล สำหรับการเรียนรู้เสียง (Voice Training) การวิจัยนี้ใช้ขั้นตอนวิธีแบบจำลองส่วนผสมเกาส์เซียน (Gaussian Mixture Model) ซึ่งผลลัพธ์จากขั้นตอนการเรียนรู้ของเครื่องคอมพิวเตอร์นี้จะได้แบบจำลองหรือโมเดลสำหรับการเรียนรู้ของเครื่องคอมพิวเตอร์

รูปที่ 4.3 หน้าจอโฮมเพจของระบบการพิสูจน์ตัวจริงด้วยชีวมิติ

รูปที่ 4.4 หน้าจอแสดงขั้นตอนการป้อนข้อมูลของกระบวนการลงทะเบียน (Registration Process)

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 4.5 หน้าจอแสดงการถ่ายภาพใบหน้าของผู้เรียนในขั้นตอนการลงทะเบียน (Facial Registration)

รูปที่ 4.6 หน้าจอแสดงปุ่มล็อกอินเมื่อผู้ใช้ลงทะเบียนเรียบร้อยแล้ว

รูปที่ 4.7 หน้าจอแสดงผลการพิสูจน์ตัวจริงเพื่อล็อกอินเข้าสู่ระบบ

มหาวิทยาลัยรังสิต Rangsit University

ช่วงเฟสการพิสูจน์ตัวจริง (Recognition Phase) เมื่อผู้ใช้ป้อนข้อมูลชีวมิติทั้งข้อมูลเสียงและข้อมูลภาพใบหน้าเข้าสู่ระบบ ดังรูปที่ 4.6 ระบบจะทำการเปรียบเทียบเทมเพลตข้อมูลชีวมิติที่รับเข้ามากับเทมเพลตชีวมิติที่ระบบได้ทำการเรียนรู้มาแล้ว ผลการเปรียบเทียบของชีวมิติจะออกมาในรูปแบบค่าของคะแนนการพยากรณ์ (Confident Score) เป็นตัวเลขร้อยละของความใกล้เคียงกัน แล้วนำผลคะแนนของการเปรียบเทียบชีวมิติทั้งสองแบบมาหาค่าผลรวมสุดท้ายของการเปรียบเทียบ (Fusion Score) หากค่าผลรวมสุดท้ายมีค่ามากกว่าขอบเขตขั้นต่ำที่กำหนดไว้คือร้อยละ 60 ระบบจะถือว่าการพิสูจน์ตัวจริงของผู้เข้าสอบถูกต้องและจะอนุญาตให้เข้าสอบออนไลน์ได้ ดังรูปที่ 4.7 แต่หากค่าผลรวมสุดท้ายมีค่าน้อยกว่าขอบเขตขั้นต่ำที่กำหนดไว้คือร้อยละ 60 ระบบจะถือว่าการพิสูจน์ตัวจริงของผู้เข้าสอบไม่ถูกต้องและจะไม่อนุญาตให้เข้าสอบออนไลน์ได้ อย่างไรตามเนื่องจากการป้อนข้อมูลชีวมิติภายใต้สภาพแวดล้อมที่แตกต่างกัน ตัวอย่างเช่น สภาพแสงน้อยหรือมากเกินไป มุมกล้อง ระยะห่างของกล้อง ความคมชัดหรือความคลาดเคลื่อนของเซนเซอร์ รวมถึงอาจมีเสียงรบกวนการป้อนข้อมูลเสียงได้เช่นกัน ซึ่งอาจส่งผลให้ผลการรู้จำมีความคลาดเคลื่อนได้ ระบบนี้จึงได้มีการออกแบบให้รองรับเงื่อนไขความแตกต่างของสภาพแวดล้อมที่อาจแตกต่างกันโดยยังคงรองรับการพิสูจน์ตัวจริงด้วยการใช้รหัสผ่านเพื่อเข้าสู่ระบบ

รูปที่ 4.8 หน้าจอแสดงการจัดการวิชา (Course Management)

มหาวิทยาลัยรังสิต Rangsit University

Exam name	Course	Start Date	End Date	Link Exam	Status	
test	test112 - test	2021-04-26T11:30	2021-04-28T11:30	tt	close	VIEW
poring	te001 - qwerty	2021-04-27T21:11	2021-04-29T21:11	https://forms.gle/rNWXwSv8yhqvS3rTA	close	VIEW
tuyyui	test02 - asdf	2021-04-30T13:38	2021-05-01T13:38	https://forms.gle/rNWXwSv8yhqvS3rTA	close	VIEW
ret	test02 - asdf	2021-05-01T13:42	2021-05-02T13:42	https://forms.gle/rNWXwSv8yhqvS3rTA	close	VIEW
rw	test112 - test	2021-04-28T13:43	2021-05-01T13:43	https://forms.gle/rNWXwSv8yhqvS3rTA	close	VIEW
Pre Test2	CO301 - Pre-Cooperative Education (LECT)	2021-05-12T20:29	2021-05-29T20:29	https://forms.gle/rNWXwSv8yhqvS3rTA	open	VIEW
Mid Test	CO301 - Pre-Cooperative Education (LECT)	2021-06-05T21:11	2021-06-26T21:11	d	close	VIEW

รูปที่ 4.9 หน้าจอแสดงการจัดการการสอบออนไลน์ (Examination Management)

ระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลโดยใช้การรู้จำภาพใบหน้าและเสียงมีผู้ใช้งานที่เกี่ยวข้องจำนวน 3 กลุ่มประกอบด้วย ผู้เรียน อาจารย์ และผู้ดูแลระบบ ผู้ดูแลระบบทำหน้าที่บริหารจัดการและดูแลระบบนี้ ผู้ดูแลระบบสามารถเพิ่ม แก้ไข ลบ หรือค้นหาข้อมูลต่าง ๆ ในระบบได้ถือได้ว่ามีสิทธิการใช้งานมากที่สุดเพื่อให้ระบบสามารถทำงานได้อย่างเรียบร้อย อาจารย์สามารถจัดการเพิ่ม ลบแก้ไข หรือค้นหาข้อมูลส่วนตัวได้และสามารถจัดการรายวิชาที่รับผิดชอบ จัดการสอบออนไลน์ที่รับผิดชอบ และการสร้างรายงานผลการสอบออนไลน์ได้ ดังรูปที่ 4.8 และ 4.9 และผู้เรียนสามารถจัดการข้อมูลส่วนตัว เช่น การแก้ไขได้ และสามารถจัดการข้อมูลการลงทะเบียนวิชา และการสอบออนไลน์ของตนเองได้

4.2 การวิเคราะห์ค่าสถิติไคสแควร์ (Pearson's Chi Square Statistic)

การศึกษานี้มีการวิเคราะห์ข้อมูลจากตารางคอนฟิวชันเมทริกซ์ (Confusion Matrix) โดยใช้ค่าทางสถิติไคสแควร์ (Pearson's Chi Square Statistic) เพื่อวิเคราะห์สมมติฐานวิจัย ค่าสถิติไคสแควร์สามารถใช้วิเคราะห์ข้อมูลเชิงปริมาณหรือค่าของข้อมูลอยู่ในมาตรวัดแบบนามบัญญัติและเรียงลำดับ (เป็นข้อมูลเชิงคุณภาพ) ค่าของข้อมูลสามารถแบ่งได้เป็น k กลุ่ม โดยแต่ละกลุ่มจะมีการแจงนับความถี่ ค่าทางสถิติไคสแควร์เป็นสถิติแบบไม่ใช้พารามิเตอร์ สถิติไคสแควร์ใช้ในการทดสอบความเป็นอิสระของตัวแปรสองตัวและใช้ในการทดสอบสมมติฐานการวิจัยที่เกี่ยวข้องกับตัวแปรสองกลุ่ม การทดสอบนี้สามารถใช้เพื่อสรุปความเป็นอิสระของประชากรสองกลุ่ม

การทดสอบสถิติไคสแควร์ครั้งนี้เป็นการทดสอบสมมติฐานที่เกี่ยวข้องกับตัวแปรจำนวน 2 ตัว เพื่อสรุปลักษณะของประชากร 2 ลักษณะว่ามีความเป็นอิสระหรือเกี่ยวข้องกันอยู่ โดยจะมีค่าความถี่ที่เกี่ยวข้องในการทดสอบ 2 ชนิด คือ

1) ความถี่สังเกต (Observed Frequency) คือ ความถี่ที่ได้จากตัวอยางที่ถูกสุ่มเพื่อเก็บข้อมูล นิยมใช้สัญลักษณ์ ด้วย Oij

2) ความถี่คาดหวัง (Expected Frequency) คือ ความถี่ที่ได้จากการคำนวณภายใต้ทฤษฎีความเป็นอิสระกันของตัวแปร 2 ตัว นิยมใช้สัญลักษณ์ด้วย Eij

การทดสอบสถิติไคสแควร์ จะนำค่าความถี่ที่สังเกต (Observed frequency) มาเปรียบเทียบกับความถี่ที่คาดหวัง (Expected frequency) ถ้าค่าของความถี่ทั้งสองนี้ใกล้เคียงกัน ซึ่งสามารถสรุปได้ว่าตัวอย่างทั้งสองกลุ่มนี้ไม่เกี่ยวข้องกัน (Independent) ถ้าค่าของความถี่ทั้งสองนี้แตกต่างกันอย่างมาก ซึ่งสามารถสรุปได้ว่าตัวอย่างทั้งสองกลุ่มนี้เกี่ยวข้องกัน (Dependent)

ตารางที่ 4.1 ตารางคอนฟิวชันเมทริกซ์ (Confusion Matrix) สำหรับการทดสอบสถิติไคสแควร์

	N=80	Nonmember /Negative (0)	Member /Positive (1)	Total
Actual	Nonmember /Negative (0)	8 (4.25)	9 (12.75)	17
	Member /Positive (1)	12 (15.75)	51 (47.25)	63
	Total	20	60	80

ขั้นที่ 1 การกำหนดสมมติฐาน (Hypothesis)

สมมติฐาน H0: ระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลที่นำเสนอไม่เกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้โมไบล์หรือเครื่องคอมพิวเตอร์ในการเข้าสอบออนไลน์ของผู้เรียนในระดับอุดมศึกษาสมมติฐาน H1: ระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลที่นำเสนอเกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้โมไบล์หรือเครื่องคอมพิวเตอร์ในการเข้าสอบออนไลน์ของผู้เรียนในระดับอุดมศึกษา

มหาวิทยาลัยรังสิต Rangsit University

ขั้นที่ 2 กำหนดระดับนัยสำคัญทางสถิติ (Significant Level) = 0.05

เป็นโอกาสที่จะเกิดความผิดพลาดในการทดสอบสมมติฐาน โดยมักจะกำหนดค่าเป็นร้อยละ งานวิจัยนี้กำหนดนัยสำคัญทางสถิติไว้ที่ 0.05 หรือ ร้อยละ 5

ขั้นที่ 3 การคำนวณค่าสถิติเพียร์สันไคสแควร์เพื่อใช้ทดสอบสมมติฐาน (Pearson's Chi-Square Test) ดังสมการที่ (4-1)

$$X^n = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{(O_{ij} - E_{ij})^2}{E_{ij}} \qquad (4\text{-}1)$$

จากสมการที่ (4-1) จะได้ค่าสถิติเพียร์สันไคสแควร์เท่ากับ 5.602241 อย่างไรก็ตาม ค่าองศาอิสระของการทดสอบ (df) มีค่าเท่ากับ 1 ให้คำนวณไคสแควร์ ด้วยสูตรของ Yate's Correction ดังสมการที่ (4-2)

$$\text{Chi-square test} = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{(|Oij\text{-}Eij|\text{-}0.5)^2}{Eij} \qquad (4\text{-}2)$$

จากสูตรข้างต้นจะได้ค่าสถิติเพียร์สันไคสแควร์เท่ากับ 4.465842

ขั้นที่ 4 สร้างบริเวณวิกฤต (Create Critical Region)

การสร้างบริเวณวิกฤต รูปที่ 4.10 สามารถทำได้โดยอาศัยตารางสถิติไคสแควร์ (Chi-square Distribution Table) โดยใช้ระดับนัยสำคัญและองศาอิสระ (df) ของการทดสอบ คือ df = (r-1)(c-1) และมีระดับนัยสำคัญเท่ากับ 0.05 จะได้ค่าสถิติไคสแควร์จากตาราง $X^2_{(\alpha,\,(r-1)(c-1))} = X^2_{(0.05,\,(1)(1))}$ มีค่าเท่ากับ 3.841 ดังนั้นบริเวณวิกฤตคือบริเวณที่มีค่ามากกว่า 3.841

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 4.10 กราฟแสดงพื้นที่บริเวณวิกฤต

นอกจากนี้จากการคำนวณพบว่าค่าความน่าจะเป็น P-value มีค่าเท่ากับ 0.03841

ขั้นที่ 5 การสรุปผล

จากข้อมูลข้างต้นพบว่าค่าสถิติเพียร์สันไคสแควร์ที่ได้จากตารางสถิติมีค่าเท่ากับ 3.841 และค่าสถิติเพียร์สันไคสแควร์ที่ได้จากการคำนวณเท่ากับ 4.465842 ซึ่งค่ามากกว่าค่าสถิติเพียร์สันไคสแควร์ที่ได้จากตารางสถิติทำให้ตกอยู่ในบริเวณวิกฤต ซึ่งทำให้ปฏิเสธสมมติฐาน H0 ที่ระดับนัยสำคัญ 0.05 สรุปได้ว่าสมมติฐานการวิจัยนี้ถูกต้อง หรือระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลที่นำเสนอเกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้โมไบล์หรือเครื่องคอมพิวเตอร์ในการเข้าสอบออนไลน์ของผู้เรียนในระดับอุดมศึกษา

นอกจากนี้ยังสามารถสรุปได้จากค่าความน่าจะเป็น P-value มีค่าเท่ากับ 0.03841 ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญที่ 0.05 ทำให้ตกอยู่ในบริเวณวิกฤต ซึ่งทำให้ปฏิเสธสมมติฐาน H0 ที่ระดับนัยสำคัญ 0.05 สรุปได้ว่าสมมติฐานการวิจัยนี้ถูกต้อง หรือระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลที่นำเสนอเกี่ยวข้องกับการพิสูจน์ตัวจริงโดยใช้โมไบล์หรือเครื่องคอมพิวเตอร์ในการเข้าสอบออนไลน์ของผู้เรียนในระดับอุดมศึกษาได้เช่นกัน

มหาวิทยาลัยรังสิต Rangsit University

4.3 ผลการวิจัย

ผู้วิจัยให้ผู้เรียนจำนวน 80 คนลงทะเบียนบนระบบที่พัฒนา ผู้เรียนแต่ละคนจะมีการป้อนข้อมูลพื้นฐานส่วนบุคคลและข้อมูลชีวมิติซึ่งประกอบด้วยข้อมูลเสียงและข้อมูลภาพใบหน้าจำนวน 20 รูปในขั้นตอนการลงทะเบียน ข้อมูลทั้งหมดจะถูกบันทึกไว้บนระบบการคำนวณแบบคลาวด์ ผู้วิจัยทำการประเมินผลระบบเป็นจำนวน 80 ครั้ง โดยแบ่งออกเป็น 2 ส่วนคือผู้ที่ลงทะเบียนกับระบบไว้แล้วจำนวน 63 คนคิดเป็นจำนวน 63 ครั้ง และผู้ที่ไม่ได้ลงทะเบียนกับระบบไว้จำนวน 17 คนคิดเป็นจำนวน 17 ครั้ง อย่างไรก็ตามในการใช้งานจริงระบบมีการเสนอทางเลือกในการใช้รหัสผ่านด้วยเช่นกันเนื่องจากอาจเกิดปัญหาจากสภาพแวดล้อมหรือปัญหาทางด้านอุปกรณ์ที่ผู้ใช้งานแต่คนใช้งานซึ่งอาจมีความแตกต่างกัน

งานวิจัยนี้เน้นการศึกษาการประเมินผลระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ ผลการทดสอบแสดงดังตารางที่ 4.2 คือตารางคอนฟิวชันเมทริกซ์ และแสดงแผนภาพในรูปที่ 4.11 มีรายละเอียดดังนี้

1) True Positive หมายถึงผลการพยากรณ์ถูกต้องว่าเป็นผู้ที่เคยลงทะเบียนไว้แล้วและความจริงคือเป็นผู้ที่เคยลงทะเบียนไว้แล้วจริง มีค่าเท่ากับ 49 ครั้ง

2) True Negative หมายถึงผลการพยากรณ์ถูกต้องว่าเป็นผู้ที่ไม่เคยลงทะเบียนไว้และความจริงคือเป็นผู้ที่ไม่เคยลงทะเบียนไว้ มีค่าเท่ากับ 8 ครั้ง

3) False Positive หมายถึงผลการพยากรณ์ไม่ถูกต้องว่าเป็นผู้ที่เคยลงทะเบียนไว้แต่ความจริงคือเป็นผู้ที่ไม่เคยลงทะเบียนไว้ มีค่าเท่ากับ 9 ครั้ง

4) False Negative หมายถึงผลการพยากรณ์ไม่ถูกต้องว่าเป็นผู้ที่ไม่เคยลงทะเบียนไว้แต่ความจริงคือเป็นผู้ที่เคยลงทะเบียนไว้ มีค่าเท่ากับ 12 ครั้ง

ตารางที่ 4.2 ตารางคอนฟิวชันเมทริกซ์ (Confusion Matrix)

	N=80	Nonmember /Negative (0)	Member /Positive (1)	Support
Actual	Nonmember /Negative (0)	8	9	17
	Member /Positive (1)	12	51	63

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 4.11 กราฟแสดงค่าจากตารางคอนฟิวชันเมทริกซ์

ตารางที่ 4.3 ตารางแสดงค่าสถิติจากการทดลอง

Accuracy Score	0.712500			
	Precision	Recall	F1 Score	Support
Nonmember	0.363636	0.470588	0.410256	17
Member	0.844828	0.777778	0.809917	63

รูปที่ 4.12 กราฟแสดงค่าสถิติจากการทดลอง

มหาวิทยาลัยรังสิต Rangsit University

ผลลัพธ์ที่ปรากฏในตารางที่ 4.3 ตารางแสดงค่าสถิติจากการทดลอง และรูปที่ 4.12 แสดงกราฟสถิติจากการทดลอง ผลการวิจัยสามารถวิเคราะห์ผลการทดลองได้หลายค่า ตัวอย่างเช่น ค่าคะแนนความถูกต้อง คะแนนความแม่นยำ คะแนนรีคอล หรือค่าเอฟวัน จากการประเมินผลการทดลองพบว่า ค่าคะแนนความถูกต้อง (Accuracy Score) มีค่าเท่ากับ 0.712500 คิดเป็นร้อยละ 71.2500 ซึ่งแสดงให้เห็นถึงอัตราส่วนของจำนวนครั้งจากการพยากรณ์ว่าถูกต้องเป็นจำนวน 57 ครั้ง เทียบกับจำนวนครั้งของการทดสอบทั้งหมด 80 ครั้ง ค่าคะแนนความถูกต้องจัดอยู่ในระดับปานกลาง ปัจจัยที่ส่งผลกระทบต่อการทดลองที่หลายประเด็น ตัวอย่างเช่นสภาพแวดล้อมที่มีความแตกต่างกันและอาจอยู่ในสภาวะที่ไม่เหมาะสมของผู้ใช้แต่ละคนและอาจมีส่งผลกระทบต่อคุณภาพของข้อมูลชีวมิติที่นำเข้าสู่ระบบ

ส่วนของคะแนนความแม่นยำ (Precision) เป็นค่าที่แสดงถึงความแม่นยำจากการพยากรณ์ของระบบ คะแนนความแม่นยำนี้สามารถแสดงได้ 2 มิติคือ ด้านที่เป็นบวก (Positive) และด้านที่เป็นลบ (Negative) คะแนนความแม่นยำด้านบวก มีค่าเท่ากับ 0.844828 คิดเป็นร้อยละ 84.4828 แสดงถึงการพยากรณ์ที่ถูกต้องว่าผู้ใช้เป็นสมาชิกที่ได้ลงทะเบียนไว้จริง จำนวน 49 ครั้ง จากจำนวนการพยากรณ์ที่ถูกต้องทั้งหมดจำนวน 58 ส่วนคะแนนความแม่นยำด้านลบ มีค่าเท่ากับ 0.363636 คิดเป็นร้อยละ 36.3636 แสดงถึงอัตราส่วนของจำนวนครั้งที่ระบบพยากรณ์ถูกต้องว่าผู้ที่พิสูจน์ตัวจริงเป็นผู้ที่ไม่เป็นสมาชิกของระบบ และความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบจำนวน 8 ครั้ง กับจำนวนครั้งทั้งหมดของการพยากรณ์ถูกต้องและไม่ถูกต้อง และความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบ จำนวน 22 ครั้ง

คะแนนรีคอลด้านบวก (Recall_Positive) มีค่าเท่ากับ 0.777778 คิดเป็นร้อยละ 77.7778 แสดงถึงอัตราส่วนของจำนวนครั้งที่ระบบพยากรณ์ว่าผู้ที่พิสูจน์ตัวจริงเป็นผู้ที่เป็นสมาชิกของระบบและความจริงคือผู้พิสูจน์ตัวจริงนั้นเป็นสมาชิกของระบบจริง จำนวน 49 ครั้ง เทียบกับจำนวนครั้งของการพยากรณ์ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นเป็นสมาชิกของระบบจริงรวมกับจำนวนครั้งของการพยากรณ์ไม่ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบจำนวน 63 ครั้งคะแนนรีคอลด้านลบ (Recall_Nagative) มีค่าเท่ากับ 0. 470588 คิดเป็นร้อยละ 47.0588แสดงถึงอัตราส่วนของจำนวนครั้งที่ระบบพยากรณ์ว่าผู้ที่พิสูจน์ตัวจริงเป็นผู้ที่เป็นสมาชิกของระบบ และความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบ จำนวน 8 ครั้ง เทียบกับจำนวนครั้งของการพยากรณ์ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นไม่เป็นสมาชิกของระบบ

มหาวิทยาลัยรังสิต Rangsit University

รวมกับจำนวนครั้งของการพยากรณ์ไม่ถูกต้องและความจริงคือผู้พิสูจน์ตัวจริงนั้นเป็นสมาชิกของระบบ จำนวน 17 ครั้ง

ค่าคะแนนเอฟวัน (F1 Score) หรือเรียกว่าค่าเฉลี่ยฮาร์โมนิก เป็นค่าที่แสดงถึงสมรรถนะการทำงานของระบบโดยเป็นการคำนวณการหาค่าเฉลี่ยของค่าคะแนนความแม่นยำ (Precision) และค่าคะแนนรีคอล (Recall) ค่าคะแนนเอฟวันมีสองค่าได้แก่ ค่าด้านบวก (F1_Score_Positive) และ ค่าด้านลบ (F1_Score_Negative) จากการทดลองพบว่าค่าคะแนนเอฟวันด้านบวกเท่ากับ 0.809917 คิดเป็นร้อยละ 80.9917 ส่วนค่าคะแนนเอฟวันด้านลบเท่ากับ 0.410256 คิดเป็นร้อยละ 41.0256 หากค่าคะแนนเอฟวันมีค่าสูงแสดงถึงโมเดลของระบบมีสมรรถนะที่สูง ในทางตรงข้ามหากค่าคะแนนเอฟวันมีค่าต่ำแสดงถึงโมเดลของระบบมีสมรรถนะที่ต่ำเช่นกัน

ตารางที่ 4.4 ตารางแสดงค่าสถิติจากการทดลองชีวมิติแบบมัลติโมดัล

	Accuracy	F-Test	Chi-square	df	P-value
Face	0.9650	0.9375	5.3333	1	0.0209
Voice	0.8437	0.75	8.5714	1	0.0034
Face+Voice	0.8740	0.7875	4.3905	1	0.0361

ตารางที่ 4.4 แสดงค่าสถิติจากการทดลองการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง ผลการศึกษาพบว่าการพิสูจน์ตัวจริงโดยใช้ชีวมิติด้วยการรู้จำใบหน้าเพียงอย่างเดียวจะได้ค่าความถูกต้อง (Accuracy) ที่ร้อยละ 96.50 ค่าของค่าคะแนนเอฟวัน (F1 Score) หรือค่าเฉลี่ยฮาร์โมนิกที่ร้อยละ 93.75 ค่าของ Chi-square เท่ากับ 5.3333 ค่าขององศาอิสระ (df) เท่ากับ 1 และค่า P-value เท่ากับ 0.0209 ผลการศึกษาพบว่าการพิสูจน์ตัวจริงโดยใช้ชีวมิติการรู้จำเสียงเพียงอย่างเดียวจะได้ค่าความถูกต้อง (Accuracy) ที่ร้อยละ 84.37 ค่าของค่าคะแนนเอฟวัน (F1 Score) หรือค่าเฉลี่ยฮาร์โมนิกที่ร้อยละ 75 ค่าของ Chi-square เท่ากับ 8.5714 ค่าขององศาอิสระ (df) เท่ากับ 1 และค่า P-value เท่ากับ 0.0034 และผลการศึกษาพบว่าการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงจะได้ค่าความถูกต้อง (Accuracy) ที่ร้อยละ 87.40 ค่าของค่าคะแนนเอฟวัน (F1 Score) หรือค่าเฉลี่ยฮาร์โมนิกที่ร้อยละ 78.75 ค่าของ Chi-square เท่ากับ 4.3905 ค่าขององศาอิสระ (df) เท่ากับ 1 และค่า P-value เท่ากับ 0.0361

มหาวิทยาลัยรังสิต Rangsit University

รูปที่ 4.13 กราฟแสดงค่าสถิติจากการทดลองชีวมิติแบบมัลติโมดัล

ผลการศึกษาเชิงประจักษ์จากข้อมูลกลุ่มตัวอย่างพบว่าข้อมูลของผู้ทดสอบแต่ละบุคคลมีหน่วยเป็นร้อยละ ดังรูปที่ 4.13 พบว่าอัตราการผิดพลาดของการรู้จำลดลง (Fake Detection) ด้วยการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง มีค่าน้อยกว่าการพิสูจน์ตัวจริงชีวมิติแบบเดี่ยวด้วยการรู้จำใบหน้าเพียงอย่างเดียว และมีค่ามากกว่าอัตราการที่บุคคลจะถูกพยากรณ์ว่าเป็นตัวปลอมด้วยการการพิสูจน์ตัวจริงชีวมิติแบบเดี่ยวด้วยการรู้จำเสียงเพียงชนิดเดียว นอกจากนี้ยังผลการศึกษาเชิงประจักษ์พบว่าอัตราการพิสูจน์ตัวจริงด้วยการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง ควรกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่ร้อยละ 60 เนื่องจากผลการทดลองเชิงประจักษ์จากการวิจัยนี้พบว่า การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง เพื่อเข้าใช้การบริการประมวลผลแบบคลาวด์มีค่าอยู่ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบในการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง เพื่อใช้การบริการประมวลผลแบบคลาวด์ได้ในอัตราร้อยละ 60

รูปที่ 4.14 กราฟแสดงค่าสถิติจำนวนภาพใบหน้า ความยาวเสียงและเวลาประมวลผล

ผลการศึกษาเชิงประจักษ์จากข้อมูลกลุ่มตัวอย่างพบว่าข้อมูลของผู้ทดสอบแต่ละบุคคล ดังรูปที่ 4.14 พบว่าระยะเวลาของเสียงที่ควรบันทึกเพื่อใช้ในการพิสูจน์ตัวจริงได้อย่างเหมาะสมทั้งด้านเวลาที่ใช้ในการประมวลผลควรมีระยะเวลาของเสียงที่บันทึกระหว่าง 2 ถึง 4 วินาที เนื่องจากหากระยะเวลาของเสียงที่บันทึกมากกว่า 4 วินาทีจะทำให้ใช้เวลาในการประมวลผลนานและใช้พื้นที่ในการจัดเก็บข้อมูลไฟล์เสียงที่เพิ่มขึ้นโดยไม่เพิ่มอัตราการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง นอกจากนี้ยังพบว่าจำนวนภาพใบหน้าที่เหมาะสมต่อการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงควรอยู่ที่ 4 ภาพ เนื่องจากหากเพิ่มจำนวนภาพใบหน้ามากกว่า 4 ภาพจะทำให้ใช้เวลาในการประมวลผลนานและใช้พื้นที่ในการจัดเก็บข้อมูลไฟล์ข้อมูลรูปที่เพิ่มขึ้นโดยไม่เพิ่มอัตราการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียง

มหาวิทยาลัยรังสิต Rangsit University

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

ผู้วิจัยได้ดำเนินการตามกรอบของกระบวนการวิจัยอย่างเป็นระบบ ผู้วิจัยสรุปผลการวิจัยดังนี้

1) มีการออกแบบโครงร่างกรอบแนวคิดระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

2) มีการนำเสนอกระบวนการออกแบบระบบโครงร่างกรอบแนวคิดเพื่อนำมาพัฒนาระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

3) มีการนำเสนอการออกแบบระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์

4) มีการพัฒนาระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ต้นแบบจากโครงร่างกรอบแนวคิด โดยใช้เทคโนโลยีเว็บที่สามารถทำงานได้หลายแพลตฟอร์มผ่านโปรแกรมเว็บเบราเซอร์

5) มีการประเมินผลระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ต้นแบบจากผู้ใช้ โดยมีกลุ่มตัวอย่างจำนวน 80 คน แบ่งเป็นกลุ่มที่มีการลงทะเบียนเพื่อใช้งานระบบจำนวน 63 คน คิดเป็นร้อยละ 79 และกลุ่มที่ไม่ได้ลงทะเบียนกับระบบไว้จำนวน 17 คน คิดเป็นร้อยละ 21

ผลจากการวิจัยครั้งนี้สามารถตอบคำถามการวิจัยที่ได้ตั้งไว้ดังนี้

คำถามข้อที่ 1 ระบบการพิสูจน์ตัวจริงเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์โดยใช้ชีวมิติที่ใช้ใบหน้าเพียงอย่างเดียวให้มีอัตราการผิดพลาดลดลงได้อย่างไร

คำตอบข้อที่ 1 ผลจากการวิจัยเชิงประจักษ์พบว่าการพัฒนาระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ ช่วยให้

อัตราการพยากรณ์การรู้จำที่ผิดพลาด (Fake Detection) ที่ลดลงอย่างมีนัยสำคัญและสามารถเพิ่มความเข้มแข็งให้กับการพิสูจน์ตัวจริง เมื่อเทียบกับการพิสูจน์ตัวจริงโดยใช้ชีวมิติภาพใบหน้าเพียงชนิดเดียว ผลการวิจัยพบว่าสอดคล้องกับผลการศึกษาของ Rotika (2008), Jain et al. (2011) ว่าการพิสูจน์ตัวจริงยังไม่มีวิธีการที่สมบูรณ์ที่สุดจึงควรใช้การพิสูจน์ตัวจริงหลาย ๆ แบบผสมผสานกันโดยใช้จุดเด่นของแต่ละวิธีเพื่อให้ได้การพิสูจน์ตัวจริงที่มีความปลอดภัยมากขึ้นกว่าการใช้วิธีการพิสูจน์ตัวจริงเพียงวิธีใดวิธีหนึ่งเพียงแบบเดียว

คำถามข้อที่ 2 ชีวมิติที่จะนำมาใช้เพื่อการพิสูจน์ตัวจริงเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ร่วมกับระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติที่ใช้ใบหน้ามีคุณลักษณะอย่างไร

คำตอบข้อที่ 2 ผลจากการวิจัยเชิงประจักษ์พบว่าชีวมิติที่จะนำมาใช้เพื่อการพิสูจน์ตัวจริงเพื่อเข้าใช้บริการประมวลผลแบบคลาวด์ร่วมกับระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติที่ใช้ใบหน้าคือชีวมิติเสียง (Voice) ซึ่งมีคุณลักษณะคือมีความยาวเสียงประมาณ 2-4 วินาที และใช้ภาพใบหน้าจำนวน 4 ภาพ ช่วยให้ลดเวลาการประมวลผล ลดพื้นที่จัดเก็บข้อมูลชีวมิติ และให้ผลการพิสูจน์ตัวจริงอย่างเหมาะสม สอดคล้องกับผลการศึกษาของ Rao & Manjunath (2017)

คำถามข้อที่ 3 ชีวมิติที่จะนำมาใช้เพื่อการพิสูจน์ตัวจริงร่วมกับระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติที่ใช้ใบหน้า (Fusion Biometric) ควรกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่เท่าไร

คำตอบข้อที่ 3 ผลจากการศึกษาเชิงประจักษ์พบว่าการใช้ชีวมิติเสียงและภาพใบหน้าในการพิสูจน์ตัวจริง (Voice and Facial Biometrics) ควรกำหนดค่าคะแนนความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ไว้ที่ร้อยละ 60 เนื่องจากผลการทดลองเชิงประจักษ์จากการวิจัยนี้พบว่า การใช้ชีวมิติภาพใบหน้าและเสียงร่วมกันในการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์มีค่าอยู่ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ได้ในอัตราร้อยละ 60 โดยบริบทการวิจัยครั้งนี้อยู่ในบริบทของการพิสูจน์ตัวจริงของนักศึกษากลุ่มตัวอย่างในการเข้าสอบออนไลน์วิชา CS320: โครงสร้างและสถาปัตยกรรมคอมพิวเตอร์ ภาคการศึกษาที่ 1 ปีการศึกษา 2563

มหาวิทยาลัยรังสิต Rangsit University

การวิจัยนี้มีการตั้งสมมติฐานไว้ และผลการวิจัยเชิงประจักษ์สามารถนำมาใช้เพื่อตอบสมมติฐานได้ดังนี้

สมมติฐาน H0: ไม่มีชีวมิติอื่นที่ใช้ร่วมกับชีวมิติที่ใช้ภาพใบหน้าที่ช่วยให้มีอัตราการผิดพลาดของการรู้จำลดลง

สมมติฐาน H1: มีชีวมิติอื่นที่ใช้ร่วมกับชีวมิติที่ใช้ภาพใบหน้าที่ช่วยให้มีอัตราการผิดพลาดของการรู้จำลดลง

ผลการศึกษาเชิงประจักษ์พบว่ามีชีวมิติอื่นที่ใช้ร่วมกับชีวมิติภาพใบหน้าที่ช่วยให้มีอัตราการผิดพลาดของการรู้จำ (Fake Detection) ที่ลดลงอย่างมีนัยสำคัญคือการชีวมิติเสียง (Voice Biometric) ร่วมกับการใช้ชีวมิติภาพใบหน้า จึงปฏิเสธสมมติฐาน H0 และยอมรับสมมติฐาน H1

สมมติฐาน H2: ไม่มีคุณลักษณะของชีวมิติอื่นที่จะนำมาใช้ร่วมกับชีวมิติที่ใช้ใบหน้าเพื่อใช้ในการพิสูจน์ตัวจริงในการเข้าใช้บริการประมวลผลแบบคลาวด์

สมมติฐาน H3: มีคุณลักษณะของชีวมิติอื่นที่จะนำมาใช้ร่วมกับชีวมิติที่ใช้ใบหน้าเพื่อใช้ในการพิสูจน์ตัวจริงในการเข้าใช้บริการประมวลผลแบบคลาวด์

ผลการศึกษาเชิงประจักษ์พบว่ามีชีวมิติอื่นที่ใช้ร่วมกับชีวมิติภาพใบหน้าคือการชีวมิติเสียง (Voice Biometric) ร่วมกับการใช้ชีวมิติภาพใบหน้า โดยมีคุณลักษณะที่มีความยาวเสียงประมาณ 2-4 วินาที และใช้ภาพใบหน้าจำนวน 4 ภาพ ช่วยให้ลดเวลาการประมวลผล ลดพื้นที่จัดเก็บข้อมูลชีวมิติ และให้ผลการพิสูจน์ตัวจริงอย่างเหมาะสม จึงปฏิเสธสมมติฐาน H2 และยอมรับสมมติฐาน H3

สมมติฐาน H4: ไม่สามารถหาค่าความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ของระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติอื่นร่วมกับชีวมิติที่ใช้ใบหน้าได้

สมมติฐาน H5: สามารถหาค่าความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ของระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติอื่นร่วมกับชีวมิติที่ใช้ใบหน้าได้

มหาวิทยาลัยรังสิต Rangsit University

ผลการศึกษาเชิงประจักษ์พบว่าสามารถหาค่าความเชื่อมั่นขั้นต่ำที่ยอมรับได้ (Minimum Acceptable Threshold) ของระบบการพิสูจน์ตัวจริงโดยใช้ชีวมิติเสียงร่วมกับชีวมิติที่ใช้ภาพใบหน้าไว้ที่ร้อยละ 60 ซึ่งเป็นค่าที่แสดงถึงความเชื่อมั่นของผู้ใช้ระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ได้ จึงปฏิเสธสมมติฐาน H4 และยอมรับสมมติฐาน H5

ปัจจุบันระบบสารสนเทศเพื่อยืนยันตัวจริงมักใช้ชื่อบัญชีผู้ใช้และรหัสผ่านเนื่องจากเป็นวิธีการที่ง่ายไม่ซับซ้อนสำหรับทั้งผู้ใช้บริการและผู้ให้บริการ อย่างไรก็ตามวิธีการนี้มีประเด็นที่ต้องพิจารณาหลายด้านโดยเฉพาะอย่างยิ่งปัญหาของการถูกโจรกรรมข้อมูลชื่อบัญชีผู้ใช้และรหัสผ่านซึ่งอาจเกิดขึ้นได้จากทั้งฝั่งผู้ใช้บริการหรือผู้ให้บริการซึ่งปัจจุบันพบว่ามีการโจรกรรมข้อมูลโดยใช้เครือข่ายอินเทอร์เน็ตบ่อยมากขึ้นและในบางกรณีมีความเสียหายในวงกว้างจำนวนมหาศาลจึงต้องมีวิธีการในการป้องกันการเข้าโจรกรรมหรือการเข้ารหัสข้อมูลชื่อบัญชีผู้ใช้และรหัสผ่านอย่างแข็งแกร่งและซับซ้อน

ผู้วิจัยนำเสนอกรอบแนวคิดในระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์แทนการใช้ชื่อบัญชีผู้ใช้และรหัสผ่านซึ่งเป็นเทคนิคที่ใช้ลักษณะทางกายภาพหรือพฤติกรรมการแสดงออกของผู้ใช้แต่ละบุคคลที่มีความเป็นปัจเจกบุคคลทั้งนี้การประยุกต์ใช้งานขึ้นอยู่กับบริบทของแต่ละหน่วยงาน จากการศึกษามีการคาดการณ์ว่าในอีกไม่กี่ปีข้างหน้าจะมีสารสนเทศด้านชีวมิติเพื่อใช้ในการตรวจสอบจะมีจำนวนหลายร้อยจนถึงหลายพันล้านข้อมูลบุคคลจึงจำเป็นต้องมีการพิจารณาถึงเทคโนโลยีที่จำเป็นต้องนำมาใช้ในการจัดการกับข้อมูลจำนวนมหาศาลอีกทั้งต้องการสมรรถนะการประมวลผลของคอมพิวเตอร์เพิ่มขึ้นอย่างมากด้วย ผู้วิจัยพบว่ากรอบแนวคิดในการประยุกต์ใช้การพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ที่นำเสนอมีประโยชน์หลายด้าน ตัวอย่างเช่น ความปลอดภัย ความพร้อมใช้งาน และความยืดหยุ่น ผู้วิจัยได้ประยุกต์ใช้กรอบแนวคิดนี้กับระบบการพิสูจน์ตัวจริงในการเข้าสอบออนไลน์ในช่วงสถานการณ์การแพร่ระบาดของโรคโควิด-19 ในประเทศไทย จากการประยุกต์ใช้งานพบว่าการนำระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์มาใช้แทนการเข้าสอบในห้องเรียนได้

มหาวิทยาลัยรังสิต Rangsit University

5.2 ข้อเสนอแนะ

จากผลการศึกษาพบว่างานวิจัยนี้ยังมีประเด็นที่ต้องพิจารณาและได้รับการศึกษาเพิ่มเติม โดยเฉพาะการป้องกันการเข้าถึงข้อมูล (Accessing to Data) การเข้ารหัสข้อมูล (Encrypted Data) ที่ได้มีการจัดเก็บไว้ระบบฐานข้อมูล และการเข้ารหัสข้อมูลระหว่างที่มีการส่งข้อมูลผ่านระบบเครือข่าย (Secure Socket Layer) เป็นต้น การปลอมแปลงข้อมูลชีวมิติต่าง ๆ ที่มีความซับซ้อนเพิ่มมากขึ้น นอกจากนี้ประเด็นของการนำไปประยุกต์ใช้งานในบริบทต่าง ๆ ต้องใช้งานด้วยความระมัดระวังทั้งนี้เนื่องการจัดเก็บหรือการใช้ชีวมิติซึ่งถือว่าเป็นข้อมูลส่วนบุคล

ประเด็นการป้องกันการเข้าถึงข้อมูลชีวมิติและข้อมูลส่วนบุคคลของผู้ใช้งานระบบการพิสูจน์ตัวจริงแบบมัลติโมดัลชีวมิติด้วยการรู้จำใบหน้าและเสียงเพื่อการบริการประมวลผลแบบคลาวด์ ผู้ให้บริการระบบการประมวลผลแบบคลาวด์ ได้มีการป้องกันส่วนของไฟร์วอลล์ (Firewall) เพื่อเป็นการป้องกันการโจมตีเข้าสู่ระบบสารสนเทศทั้งหมดผ่านเครือข่าย นอกจากนี้ผู้วิจัยได้มีการใช้โปรแกรม OpenVPN ในการป้องกันการเข้าถึงระบบสารสนเทศของผู้วิจัยบนระบบคลาวด์ โดยจะมีการใช้ Public Key และ Private Key ในการเข้ารหัสและถอดรหัสข้อมูล (การเข้ารหัสของ openVPN)

ประเด็นของข้อมูลด้านชีวมิติและข้อมูลส่วนบุคคลของผู้ใช้งานในปัจจุบันนี้ยังไม่ได้มีการเข้ารหัสข้อมูล (Encrypted Data) ที่ได้มีการจัดเก็บไว้ระบบฐานข้อมูล ดังนั้นหากผู้โจมตีสามารถเข้าถึงข้อมูลในฐานข้อมูลได้ก็สามารถนำข้อมูลที่ยังไม่ผ่านการเข้ารหัสนี้ไปใช้งานหรือดำเนินการอย่างอื่นได้ แนวทางการป้องกันและแก้ไขอาจทำได้โดยใช้ระบบการจัดการฐานข้อมูลที่มีคุณสมบัติในการเข้ารหัสข้อมูลทั้งในระดับฐานข้อมูล ระดับตารางข้อมูล หรือระดับคอลัมน์ของข้อมูล ตัวอย่างเช่น ระบบฐานข้อมูลออราเคิล เวอร์ชัน 18c ขึ้นไปจะมีคุณสมบัติในการเข้ารหัสฐานข้อมูลโดยใช้รูปแบบ Public Key และ Private Key ในการเข้ารหัสและถอดรหัสข้อมูล

ประเด็นของระบบการเข้ารหัสข้อมูลระหว่างที่มีการส่งข้อมูลผ่านระบบเครือข่าย (Secure Socket Layer) ปัจจุบันยังไม่ได้มีการเข้ารหัสข้อมูลระหว่างที่มีการส่งข้อมูลผ่านระบบเครือข่าย ทำให้หากมีการส่งข้อมูลชีวมิติผ่านระบบเครือข่ายผู้ไม่ประสงค์ดีอาจมีการดักจับหรือขโมยข้อมูลไปใช้งานหรือดำเนินการอย่างอื่นได้ อย่างไรก็ตามการเพิ่มคุณสมบัติการเข้ารหัสข้อมูลระหว่างที่มีการส่งข้อมูลผ่านระบบเครือข่าย (Secure Socket Layer) สามารถเพิ่มได้โดยอาจจะใช้บริการของผู้

มหาวิทยาลัยรังสิต Rangsit University

ให้บริการประมวลผลแบบคลาวด์ โดยมีค่าบริการเพิ่มเติม หรือผู้วิจัยอาจใช้ดำเนินการเองได้ทั้งแบบที่ต้องมีการเสียค่าบริการจากผู้ให้บริการ SSL หรืออาจใช้ SSL แบบที่ไม่เสียค่าบริการ ทั้งนี้ขึ้นกับบริบทในการนำระบบไปใช้งานว่ามีระดับความต้องการในระดับใด

ประเด็นของการพิสูจน์ตัวจริงโดยใช้ชีวมิติหลายแบบ ปัจจุบันระบบการพิสูจน์ตัวจริงที่ปรับตัวได้โดยชีวิมิติหลายแบบในการเข้าใช้บริการบนการประมวลผลแบบคลาวด์ นี้ใช้ชีวมิติ 2 แบบคือ การรู้จำภาพใบหน้าบุคคลซึ่งเป็นชีวมิติแบบกายภาพ และการรู้จำเสียงซึ่งเป็นชีวมิติแบบพฤติกรรม อย่างไรก็ตามผู้ที่จะไปประยุกต์ใช้งานต้องการความปลอดภัยหรือความเข้มแข็งของระบบการพิสูจน์ตัวจริงก็สามารถเพิ่มรูปแบบการพิสูจน์ตัวจริงต่าง ๆ เพิ่มเติมได้อีก ตัวอย่างเช่น การเพิ่มการพิสูจน์ตัวจริงด้วยชีวมิติโครงสร้างของเส้นเลือดบริเวณมือ การเพิ่มการพิสูจน์ตัวจริงด้วยชีวมิติลายนิ้วมือ การเพิ่มการพิสูจน์ตัวจริงด้วยชีวมิติม่านตา หรือการเพิ่มการพิสูจน์ตัวจริงด้วยชีวมิติลายมือ เป็นต้น อย่างไรก็ตามในประเด็นนี้มีความขึ้นตรงกับชนิดของเซนเซอร์และคุณภาพของเซนเซอร์ที่จะนำมาใช้ในการอ่านค่าของชีวมิติของผู้ใช้งาน รวมถึงปัจจัยสภาพแวดล้อมของผู้ใช้งานแต่ละบุคล ตัวอย่างเช่น มุมองศา ระยะห่าง ความสว่างของการถ่ายภาพ ส่วนปัจจัยสภาพแวดล้อมของการบันทึกเสียงเช่น เสียงรบกวนของสภาพแวดล้อมต่าง ๆ เป็นต้น

ประเด็นการปลอมแปลงข้อมูลชีวมิติ ปัจจุบันระบบการพิสูจน์ตัวจริงที่ปรับตัวได้โดยชีวิมิติหลายแบบในการเข้าใช้บริการบนการประมวลผลแบบคลาวด์ นี้ยังไม่ได้เพิ่มส่วนของการป้องกันการปลอมแปลงหรือการเลียนแบบข้อมูลชีวมิติ ตัวอย่างเช่น อาจมีการใช้ภาพนิ่งของบุคคลอื่นมาใช้แทนภาพใบหน้าของตนเองเพื่อให้ผ่านการพิสูจน์ตัวจริงและสามารถเข้าใช้งานระบบสารสนเทศได้ แนวทางการป้องกันการปลอมแปลงภาพใบหน้าจากการศึกษาพบว่ามีหลายแนวทางขึ้นกับบริบทที่จะนำไปใช้งาน ตัวอย่างเช่น ให้ผู้ใช้กระพริบตา หรือให้หน้าหันไปทางซ้ายหรือไปทางขวาตามที่กำหนดก่อนการบันทึกภาพใบหน้าเพื่อเป็นการยืนยันได้ว่าเป็นมนุษย์จริงไม่ใช่การนำภาพนิ่งใบหน้าของผู้อื่นมาใช้งาน ส่วนการปลอมแปลงเสียงของบุคคลอื่นนั้นอาจทำได้โดยการบันทึกเสียง เลียนแบบเสียงของผู้อื่น จากการทบทวนวรรณกรรมพบว่าอาจให้ระบบสุ่มข้อความเพื่อให้ผู้ใช้งานออกเสียงพูดตามข้อความที่ระบบสุ่มมาให้

ประเด็นของการนำไปประยุกต์ใช้งานในบริบทต่าง ๆ ต้องใช้งานด้วยความระมัดระวังทั้งนี้เนื่องการจัดจัดเก็บหรือการใช้ชีวมิติซึ่งถือว่าเป็นข้อมูลส่วนบุคคล (Data Privacy) ซึ่งต้องได้รับความยินยอมจากผู้ใช้รวมถึงประเด็นด้านกฎหมายที่รองรับของแต่ละประเทศที่อาจมีความแตกต่าง

กัน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (PDPA ย่อมาจาก Personal Data Protection Act) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลถูกประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 จะมีบทบาทในการคุ้มครองและให้สิทธิต่อข้อมูลส่วนบุคคล รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคลในการจัดเก็บข้อมูลส่วนบุคคล รวบรวมข้อมูลส่วนบุคคล ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษของ PDPA สำหรับผู้ที่ไม่ปฏิบัติตามนั้นมีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองด้วย

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม

โครงการบริการคลาวด์ภาครัฐ. (2558). สืบค้น 2 กรกฎาคม 2558, จาก https://www.ega.or.th/th/content/890/273.

สุวิมล ว่องวาณิช และนงลักษณ์ วิรัชชัย. (2546). *แนวทางการให้คำปรึกษาวิทยานิพนธ์*. กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

Ahn, H., Chang, H., Jang, C., & Choi, E. (2011). User Authentication Platform using Provisioning in Cloud Computing Environment. *Advanced Communication and Networking, 199*, 132-138. doi: 10.1007/978-3-642-23312-8_16.

Ajish S., & AnilKumar, K. S. (2021). Secure mobile internet voting system using biometric authentication and wavelet based AES. *Journal of Information Security and Applications, 61*. doi: 10.1016/j.jisa.2021.102908.

Arslan, A., & Yildiz, O. (2018). Automated Auscultative Diagnosis System for Evaluation of Phonocardiogram Signals Associated with Heart Murmur Diseases. *Gazi University Journal of Science, 31*(1), 112-124.

Atmakuri, S. M. (2015). *A Study of Authentication Techniques for mobile cloud computing* (Master's Thesis). Retrieved from https://tamuk.contentdm.oclc.org/

Bah, S. M., & Ming, F. (2020). An improved face recognition algorithm and its application in attendance management system. *Array, 5*, 1-7. doi: 10.1016/j.array.2019.100014.

Balfanz, D., Chow, R., Eisen, O., Jakobsson, M., Kirsch, S., Matsumoto, S., Molina, J., & Oorschot, P. V. (2012). The future of authentication, *IEEE Security & Privacy*, *10*(1), 22-27. doi: 10.1109/MSP.2012.24.

Behera, N. K. S., Behera, T. K., Nappi, M., Bakshi, S., & Saa, P. K. (2021). Futuristic person re-identification over internet of biometrics things (IoBT): Technical potential versus practical reality. *Pattern Recognition Letters*, *151*, 163–171. doi: 10.1016/j.patrec.2021.08.007.

Bisogni, C., Iovane, G., Landi, R. E., & Nappi, M. (2021). ECB2 :A novel encryption scheme using face biometrics for signing blockchain transactions. *Journal of Information Security and Applications, 59*. doi: 10.1016/j.jisa.2021.102814.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

BrundhaElci, J., Punith, R., Gowda, S. C., Shivaprasad, B. M, & Buvaneshwaran, V. S. (2019). Criminal Recognition and Tracking System. *International Research Journal of Computer Science (IRJCS), 6*(6), 118-125. doi: 10.26562/IRJCS.2019.JNCS10095.

Chang, D., Garg, S., Ghosh, M., & Hasan, M. (2021). BIOFUSE: A framework for multi-biometric fusion on biocryptosystem level. *Information Sciences, 546*, 481–511. doi: 10.1016/j.ins.2020.08.065.

Chang, H., & Choi, E. (2011). User Authentication in Cloud Computing. In: Kim, Th., Adeli, H., Robles, R.J., Balitanas, M. (eds) Ubiquitous Computing and Multimedia Applications. UCMA 2011. *Communications in Computer and Information Science, 151*, 338–342. Springer, Berlin, Heidelberg. doi: 10.1007/978-3-642-20998-7_42.

Cherifi, F., Omar, M., & Amroun, K. (2021). An efficient biometric-based continuous authentication scheme with HMM prehensile movements modeling. *Journal of Information Security and Applications, 57*. doi: 10.1016/j.jisa.2020.102739.

Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics, 21*(6). doi: 10.1186/s12864-019-6413-7.

Chicco, D., Toetsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining, 14*(13). doi: 10.1186/s13040-021-00244-z 1-22.

Choudhury, S. H., Kumar, A., & Laskar, S. H. (2021). Adaptive Management of Multimodal Biometrics—A Deep Learning. *Applied Soft Computing, 106*. doi: /10.1016/j.asoc.2021.107344.

Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E., & Song, Z. (2010). Authentication in the Clouds: A Framework and its Application to Mobile Users. *Proceedings of the 2nd ACM Cloud Computing Security Workshop*, CCSW 2010, Chicago, IL, USA.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Cui, W., Wang, Z., & Li. Y. (2021). ECG-based biometric recognition under exercise and rest situations. *Biomedical Engineering Advances, 2*. doi: 10.1016/j.bea.2021.100008.

Czeskis, A., Dietz, M., Kohno, T., Wallach, D., & Balfanz, D. (2012). Strengthening user authentication through opportunistic cryptographic identity assertions. *ACM Conference on Computer and Communications Security*, 404-414. doi: 10.1145/2382196.2382240.

Dalal, N., & Triggs, B. (2005). Histograms of oriented gradients for human detection. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2005, 1*, 886-893. doi: 10.1109/CVPR.2005.177.

Damato, A. (2007). *Cloud Computing*. Retrieved June 15, 2020, from https://en.wikipedia.org/wiki/Biometrics.

Déniz-Suárez, O., García, G.B., Salido, J., & Torre, F.D. (2011). Face recognition using Histograms of Oriented Gradients. *Pattern Recognit. Lett., 32*, 1598-1603. doi: 10.1016/j.patrec.2011.01.004.

Douglas, H., & Gehrmann, C. (2019). Secure Virtualization and Multicore Platforms State-of-the-Art report. Swedish Institute of Computer Science.

Errattahia, S., Hannania, A. E., & Ouahmane, H. (2018). Automatic Speech Recognition Errors Detection and Correction: A Review. *Procedia Computer Science, 128*, 32-37. doi: 10.1016/j.procs.2018.03.005.

Everest Group. (2014). *Enterprise Cloud Adoption Survey 2014: Summary of Results*. Everest Global, Inc.

Falmari, V. R., & Brindha, M. (2021). Privacy preserving biometric authentication using Chaos on remote untrusted server. *Measurement, 177*. doi: 10.1016/j.measurement.2021.109257.

Fei, L., Zhang, B., Tian, C., Teng, S., & Wen, J. (2021). Jointly learning multi-instance hand-based biometric descriptor. *Information Sciences, 562*, 1-12. doi: 10.1016/j.ins.2021.01.086.

Gartner (2013). Forecast: Public Cloud Services, *Worldwide*, 2011-2017, 4Q13 Update.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Heitmeyer, R. (2000). Biometric Identification Promises Fast and Secure Processing of Airline Passengers, *ICAO Journal, 55*(9), 10-11, 27-28.

Jain, A. K. Hong, L., Pankanti, S. & Bolle, R. (1997). An identity-authentication system using fingerprints, *Proceedings of the IEEE*, *85*(9), 1365-1388. doi: 10.1109/5.628674.

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer. doi 10.1007/978-0-387-77326-1.

Jia, W., Xia, W., Zhang, B., Zhao, Y., Fei, L., Kang, W., Huang, D., & Guo, G. (2021). A survey on dorsal hand vein biometrics. *Pattern Recognition, 120*. doi: 10.1016/j.patcog.2021.108122.

Johannsson, B., Kashyap, S., & Manjappa, R. (2016). *OpenCV (Open Source Computer Vision Library). Delft University of Technology*. Retrieved June 20, 2021, from https://delftswa.gitbooks.io/desosa2016/content/opencv/Chapter.html.

Johnston, S. (2009). *Cloud Computing*. Retrieved June 13, 2020, from https://en.wikipedia.org/wiki/File:Cloud_computing.svg.

Kausar, F. (2021). Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal, 22*(4), 447-453. doi: 10.1016/j.eij.2021.01.004.

Kazemi, V., & Sullivan, J. (2011). Face Alignment with Part-Based Modeling. BMVC 2011 - *Proceedings of the British Machine Vision Conference* 2011, 27.1-27.10. doi: 10.5244/C.25.27.

King, D. E. (2009). Dlib-ml: A Machine Learning Toolkit. *Journal of Machine Learning Research*, 10, 1755–1758. doi: 10.1145/1577069.1755843.

King, D. (2014). *dlib C++ Library: Dlib 18.6 released: Make your own object detector!* Retrieved May 12, 2020, from https://blog.dlib.net/2014/02/dlib-186-released-make-your-own-object.html.

Kohlwaey, E., Sussman, A., Trost, J., & Maurer, A. (2011). Leveraging the Cloud for Big Data Biometric: Meeting the performance requirements of the Next Generation Biometric Systems*, Proceeding of the IEEE World Congress on Services*, 597-601. doi: 10.1109/SERVICES.2011.95.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Kumar, D., Joshi, A.B., & Singh, S. (2021). A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system. *Results in Optics, 5*. doi: 10.1016/j.rio.2021.100146.

Kumari, P., & Thangaraj, P. (2020). A fast feature selection technique in multi modal biometrics using cloud framework. *Microprocessors and Microsystems, 79*(2). doi: 10.1016/j.micpro.2020.103277.

Kute, R., Vyas, V., & Anuse, A. (2021). Transfer learning for face recognition using fingerprint biometrics. *Journal of King Saud University - Engineering Sciences*. doi: 10.1016/j.jksues.2021.07.011.

Lee, M. J., Teoh, A.B.J., Uhl, A., Liang, S., & Jina, Z. (2021). A Tokenless Cancellable Scheme for Multimodal Biometric Systems. *Computers & Security, 108*(C). doi: 10.1016/j.cose.2021.102350.

Lee, Y. K., & Jeong, J. (2021). Securing biometric authentication system using blockchain. *ICT Express, 7*(3), 322–326. doi: 10.1016/j.icte.2021.08.003.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, M. & Leaf, D. (2011), *NIST Cloud Computing Reference Architecture.* Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. doi:10.6028/NIST.SP.500-292. Retrieved June 20, 2020, from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909505.

Liu, S., Shao, W., Li, T., Xu, W., & Song, L. (2021). Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing, 125*. doi: 10.1016/j.dsp.2021.103120.

Magre,S. B., Janse,P. V., & Deshmukh, R. R. (2014). A Review on Feature Extraction and Noise Reduction Technique. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(2), 352-356.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Marquez, H. J. P., Ambrose, D. J., Schaefera, A. L., Cook, N. J., & Bench, C. J. (2021). Evaluation of infrared thermography combined with behavioral biometrics for estrus detection in naturally cycling dairy cows. *Animal, 15*(7). doi: 10.1016/j.animal.2021.100205.

Mason, J., Dave, R., Chatterjee, P., Allen, I. G., Esterline, A., & Roy, K. (2020). An Investigation of Biometric Authentication in the Healthcare Environment. *Array, 8*. doi: 10.1016/j.array.2020.100042.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. Special Publication 800-145.

Naidu, B. R., & Babu, M. S. P. (2018). Biometric authentication data with three traits using compression technique, HOG, GMM and fusion technique. *Data in Brief, 18*, 1976–1986. doi: 10.1016/j.dib.2018.03.115.

Peer, P., Bule, J., Gros, J. Ž., & Štruc, V. (2013). Building Cloud-based Biometric Services. *Informatica ,37*, 115–122.

Piciucco, E., Lascio, E. D., Maiorana, E., Santini, S., & Campisi, P. (2021). Biometric recognition using wearable devices in real-life settings. *Pattern Recognition Letters, 146*(3), 260–266. doi: 10.1016/j.patrec.2021.03.020.

Piryonesi, S. M., & El-Diraby, T. E. (2020). Data Analytics in Asset Management: Cost-Effective Prediction of the Pavement Condition Index. *Journal of Infrastructure Systems, 26*(1). doi:10.1061/(ASCE)IS.1943-555X.0000512.

Pukdesree, S., & Netinant, P. (2016). Biometric Authentication for Accessing Cloud Computing Services using iPhone. Proceedings of the 12th International Conference on Computing and Information Technology (IC2IT), *Advances in Intelligent Systems and Computing*, *463*, 209-216. doi: 10.1007/978-3-319-40415-8.

Pukdesree, S., & Netinant, P. (2018). Reviewed: The Face Authentication Processes for Accessing Cloud Computing Services using iPhone. *TEM Journal, 7*(3), 475-479. doi: 10.18421/TEM73-01.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Shelly & Raghava, N. S. (2011). Iris recognition on Hadoop: A biometrics system implementation on cloud computing, *2011 IEEE International Conference on Cloud Computing and Intelligence Systems*, 482-485. doi: 10.1109/CCIS.2011.6045114.

Rao, K. S., & Manjunath, K. E. (2017). Speech Recognition Using Articulatory and Excitation Source Features. *Springer Briefs in Electrical and Computer Engineering*. doi: 10.1007/978-3-319-49220-9_1.

Rokita, J., Krzyzak, A., & Suen, C. (2008). Multimodal biometric system based on face and hand images taken by a cell phone. *International Journal of Pattern Recognition and Artificial Intelligence, 22*(3), 411-429. doi: 10.1142/S0218001408006302.

Romo, J. T. (2014). *Towards Seamless and Secure Mobile Authentication* (Master's Thesis, Arizona State University). Retrieved from https://www.proquest.com/openview/0a9b817a0702ced2d5efc08bd44a5911/1?pq-origsite=gscholar&cbl=18750

Rosebrock, A. (2017). *Facial landmarks with dlib, OpenCV, and Python*. Retrieved May 25, 2021, from https://pyimagesearch.com/2017/04/03/facial-landmarks-dlib-opencv-python.

Rukhiran, M., Pukdesree, S., & Netinant, P. (2022). Biometric Cloud Services for Web-Based Examinations: An Empirical Approach. *International Journal of Information Technology and Web Engineering (IJITWE)*, *17*(1), 1-25. doi: 10.4018/IJITWE.299022

Saeed, U. (2021). Facial micro-expressions as a soft biometric for person recognition. *Pattern Recognition Letters, 143*, 95–103. doi: 10.1016/j.patrec.2020.12.021.

Sarier, N. D. (2021). Multimodal Biometric Authentication for Mobile Edge Computing. *Information Sciences*, *573*, 82-99. doi: 10.1016/j.ins.2021.05.036.

Schneier, B. (2009). *Cloud Computing*. Retrieved June 13, 2020, from https://www.schneier.com/blog/archives/2009/06/cloud_computing.html.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University – Computer and Information Sciences, 32*(1), 57–64. doi: 10.1016/j.jksuci.2017.07.001.

Sharma, S., & Mittal, U. (2013). Comparative Analysis of Various Authentication Techniques in Cloud Computing. *International Journal of Innovative Research in Science, Engineering and Technology, 2*, 994-998.

Srivastva, R., Singh, A., & Singh., Y. N. (2021). PlexNet: A fast and robust ECG biometric system for human Recognition. *Information Sciences, 558*, 208–228. doi: 10.1016/j.ins.2021.01.001.

Struc, V., & Zganec-Gros, J. (2012). Developing Face Recognition Technology for KC Class Biometrics service. *Proceedings of the 1th International Conference on Cloud Assisted Services (CLASS)*, 68-75. Bled, Slovenia.

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion, 66*, 76–99. doi: 10.1016/j.inffus.2020.08.021.

Tharwat, A. (2021). Classification assessment methods. *Applied Computing and Informatics, 17*(1), 168-192. doi: 10.1016/j.aci.2018.08.003.

Vallabhu, H., & Satyanrayana, R. V. (2012). Biometric Authentication as a Service on Cloud: Novel Solution. International. *Journal of Soft Computing and Engineering, 2*(4), 163-165.

Vijay, M., & Indumathi, G. (2021). Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications. *Journal of Information Security and Applications, 58*(3). doi: 10.1016/j.jisa.2020.102707.

Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *Computer Vision and Pattern Recognition (CVPR)*, 1, 511-518. doi: 10.1109/CVPR.2001.990517.

มหาวิทยาลัยรังสิต Rangsit University

บรรณานุกรม (ต่อ)

VMWare Cloud Index. (2012). Retrieved July 15, 2016, from http://www.vmware.com/ap/cloudindex.

Yang, W., Wang, S., Shahzad, M., & Zhou, W. (2021). A cancelable biometric authentication system based on feature-adaptive random projection. *Journal of Information Security and Applications, 58*. doi: 10.1016/j.jisa.2020.102704.

Zareen, F. J., & Jabin, S. (2013). A comparative study of the recent trends in biometric signature verification. *2013 Sixth International Conference on Contemporary Computing (IC3)*, 354-358. doi: 10.1109/IC3.2013.6612219.

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก ก

บทความที่ตีพิมพ์เผยแพร่ในวารสารวิชาการ Advances in Intelligent Systems and Computing ฐานข้อมูล Scopus Q3

Conceptual Framework: The Adaptive Biometrics Authentication for Accessing Cloud Computing Services Using iPhone

มหาวิทยาลัยรังสิต Rangsit University

มหาวิทยาลัยรังสิต Rangsit University

Program Committee

A. Agarwal, UoHyd, India
T. Anwar, UTM, Malaysia
S. Auwatanamongkol, NIDA, Thailand
G. Azzopardi, University of Groningen, The Netherlands
T. Bernard, Syscom CReSTIC, France
T. Boehme, TU Ilmenau, Germany
M. Caspar, TU Chemnitz, Germany
N. Ditcharoen, UBU, Thailand
K. Djemame, University of Leeds, UK
T. Eggendorfer, HS Weingarten, Germany
L. Fung, Murdoch University, Australia
M. Ghazali, UTM, Malaysia
W. Halang, FernUni, Germany
C. Haruechaiyasak, NECTEC, Thailand
S. Hengpraprohm, NPRU, Thailand
U. Inyaem, RMUTT, Thailand
M. Kaenampornpan, MSU, Thailand
P. Kirdwichai, KMUTNB, Thailand
A. Kongthon, NECTEC, Thailand
M. Kubek, FU Hagen, Germany
P. Kucharoen, NIDA, Thailand
K. Kyamakya, University of Klagenfurt, Austria
U. Lechner, UniBwM, Germany
A. Mingkhwan, KMUTNB, Thailand
C. Namman, UBU, Thailand
H.H.C. Nguyen, QNU, Vietnam
S. Nitsuwat, KMUTNB
S. Nuanmeesri, RSU, Thailand
P. Palawisut, NPRU, Thailand
J. Phuboonob, MSU, Thailand
N. Porrawatpreyakorn, KMUTNB, Thailand

มหาวิทยาลัยรังสิต Rangsit University

P. Prathombutr, NECTEC, Thailand
S. Puangpronpitag, MSU, Thailand
T. Quan, HCUT, Vietnam
P. Saengsiri, TISTR, Thailand
J. Shen, University of Wollongong, Australia
S. Smanchat, KMUTNB, Thailand
M. Sodanil, KMUTNB, Thailand
S. Sodsee, KMUTNB, Thailand
G. Somprasertsri, MSU, Thailand
T. Srikhacha, TOT, Thailand
W. Sriurai, UBU, Thailand
T. Sucontphunt, NIDA, Thailand
S. Suranauwarat, NIDA, Thailand
D. Thammasiri, NPRU, Thailand
S. Tongngam, NIDA, Thailand
D.H. Tran, HNUE, Vietnam
K. Treeprapin, UBU, Thailand
D. Tutsch, University of Wuppertal, Germany
S. Valuvanathorn, UBU, Thailand
M. Weiser, OSU, USA
N. Wisitpongphan, KMUTNB, Thailand
K. Woraratpanya, KMITL, Thailand
P. Wuttidittachotti, KMUTNB, Thailand

มหาวิทยาลัยรังสิต Rangsit University

Contents

Part I Invited Paper

Cloud Computing: New Paradigms and Challenges 3
Djamshid Tavangarian

Part II User Centric Data Mining and Text Processing

User-Triggered Structural Changes in OSN-Alike Distributed Content Networks 7
Hauke Coltzau and Mario Kubek

Modeling Disease Spread at Global Mass Gatherings: Data Requirements and Challenges 17
Sultanah M. Alshammari and Armin R. Mikler

Concept-Based Sentiment Analysis for Opinion Texts with Multiple-Languages 27
Jantima Polpinij, Natthakit Srikanjanapert and Chetarin Wongsin

Automatic Advisor for Detecting Summarizable Chat Conversations in Online Instant Messages 37
Fajri Koto and Omar Abdillah

Optical Character Recognition for Nepali, English Character and Simple Sketch Using Neural Network 45
Subarna Shakya, Abinash Basnet, Suman Sharma and Amar Bdr Gurung

Segmentation of Overlapping Isan Dhamma Character on Palm Leaf Manuscript's with Neural Network 55
Mahasak Ketcham, Worawut Yimyam and Narumol Chumuang

Comparative Results of Attribute Reduction Techniques for Thai Handwritten Recognition with Support Vector Machines 67
Tanasanee Phienthrakul and Massaya Samnienggam

มหาวิทยาลัยรังสิต Rangsit University

Human Action Invarianceness for Invarianceness Using Integration Moment for Human Action Recognition in Video 79
Nilam Nur Amir Sjarif, Siti Mariyam Shamsuddin, Siti Zaiton Mohd Hashim, Aida Ali and Zanariah Zainudin

Part III Data Mining Algorithms and Their Applications

Parallel Shallow Water Simulations by Finite Volume Method with CUDA 95
Kedsararat Khawyuen, Worasait Suwannik and Montri Maleewong

Intrusion Detection System Based on Cost Based Support Vector Machine 105
Md. Rafiul Hassan

Predicting Quality-Assured Consensual Answers in Community-Based Question Answering Systems 117
Krissada Maleewong

Influence of ERP Employment on Work Skills 129
Suphan Petyim, Bunthit Watanapa, Nipon Charoenkitkarn and Jidapa Archanainant

Electrocardiogram Identification: Use a Simple Set of Features in QRS Complex to Identify Individuals 139
Tuerxunwaili, Rizal Mohd Nor, Abdul Wahab Bin Abdul Rahman, Khairul Azami Sidek and Adamu Abubakar Ibrahim

The Research on Improving Algorithms for Hilltop to Improve Search Quality 149
Peng Lu and Xiao Cong

A Fast Outlier Detection Algorithm for Big Datasets 159
Duong van Hieu and Phayung Meesad

Fast Computing of Microarray Data Using Resilient Distributed Dataset of Apache Spark 171
Ransingh Biswajit Ray, Mukesh Kumar and Santanu Kumar Rath

Heuristic Search Algorithms for Constructing Optimal Latin Hypercube Designs 183
Anamai Na-udom and Jaratsri Rungrattanaubol

A Hybrid Multi-objective Genetic Algorithm with a New Local Search Approach for Solving the Post Enrolment Based Course Timetabling Problem 195
Dome Lohpetch and Sawaphat Jaengchuea

มหาวิทยาลัยรังสิต Rangsit University

Part IV Optimisation of Complex Networks

Conceptual Framework: The Adaptive Biometrics Authentication for Accessing Cloud Computing Services Using iPhone 209
Sorapak Pukdesree and Paniti Netinant

An Insurmountable and Fail-Secure Network Interface 217
Wolfgang A. Halang, Panchalee Sukjit, Maytiyanin Komkhao and Sunantha Sodsee

Finding an Optimal Parameter for Threshold Cryptography 223
Weena Janratchakool, Sirapat Boonkrong and Sucha Smanchat

Effective Linear Transformation Matrices for Block Cipher Based on Bi-regular Matrix 233
The Dung Luong

A High Radix Hierarchical Interconnection Network for Network-on-Chip 245
Mohammed N.M. Ali, M.M. Hafizur Rahman, Rizal Mohd Nor and Tengku Mohd Bin Tengku Sembok

Prioritized Probabilistic Caching Algorithm in Content Centric Networks 255
Warit Sirichotedumrong, Wuttipong Kumwilaisak, Saran Tarnoi and Nattanun Thatphithakkul

KSBS Solution of Power Allocation in Multi-user Multi-relay Networks Using Stackelberg Game 267
Supenporn Somjit, Pattarawit Polpinit and Chatchai Khunboa

Energy-Distance Aware Clustering Scheme (E-DACS) for Wireless Sensor Networks 277
Abdullah Said Alkalbani, Teddy Mantoro and Satyanarayana Degala

Fast Tracking Algorithm for Designed Marker 293
Teera Siriteerakul and Rutchanee Gullayanon

Real-Time Control of Mobile Communication Channels 301
Mario M. Kubek and Herwig Unger

E-Model Parameters Estimation for VoIP with Non-ITU Codec Speech Quality Prediction 309
Tuul Triyason and Prasert Kanthamanon

ICT Implementation and Infrastructure Deployment Approach for Rural Nepal 319
Babu Ram Dawadi and Subarna Shakya

Author Index 333

มหาวิทยาลัยรังสิต Rangsit University

Conceptual Framework: The Adaptive Biometrics Authentication for Accessing Cloud Computing Services Using iPhone

Sorapak Pukdesree and Paniti Netinant

Abstract Presently, cloud computing technology is widely applied in many domains. The trends of cloud computing are forecasted to be worth around 250 billion dollars in 2017. In Thailand, cloud computing situations also correspondence to other countries. The survey report from Forester in 2012, showed that growth rate of utilization of cloud computing trended to increase continuously. Thai government also foresees the importance of cloud computing technology to support digital economy campaign by setting up Government Cloud Service project. However there are some issues which to be concerned when deploy cloud computing especially security on cloud computing. Currently, mobile devices are very more widely used in our society as we have seen the large number of delivered mobile devices in each year. Therefore we proposed adaptive biometric authentication for accessing cloud computing services using iPhone. The adaptive biometric authentication, which has advantages of fast, flexible and more secure, uses sequential authentications instead of multi-modal approaches. The current status of this research is on developing phase.

Keywords Biometric authentication • Cloud computing • iPhone • Security • iOS

S. Pukdesree (✉)
School of Science and Technology, Bangkok University, Bangkok, Thailand
e-mail: sorapuck.p@bu.ac.th

S. Pukdesree • P. Netinant
College of Information and Communication Technology, Rangsit University, Pathum Thani, Thailand
e-mail: netinant1@gmail.com

© Springer International Publishing Switzerland 2016

P. Meesad et al. (eds.), *Recent Advances in Information and Communication Technology 2016*, Advances in Intelligent Systems and Computing 463,
DOI 10.1007/978-3-319-40415-8_20

Rangsit University

1 Introduction

Presently, cloud computing technology is widely applied in many domains. The trends of cloud computing are forecasted to be worth around 250 billion dollars in 2017 [1]. In 2016, one-fourth of typical Software can be accessed as services of cloud computing (SaaS) which would be worth from 18.2 billion dollars to 45.6 billion dollars in 2017. Furthermore, there was a forecast that enterprise businesses will spend more than 10 % of the budgets on cloud computing services [2].

In Thailand, cloud computing situations also correspondence to other countries. The survey report [3] showed that growth rate of utilization of cloud computing trends to increase continuously. Approximately 83 % of survey correspondences have already planned or adapted to use cloud computing technology. The correspondences have agreed that cloud computing will help the organizations to have more potential than competitors. Approximately 68 % of survey correspondences have also agreed that if the organizations would not use cloud computing, the organizations would not work as fast as competitors.

Thai government also foresees the importance of cloud computing technology to support digital economy campaign by setting up Government Cloud Service project named G-Cloud under controlling of Electronic Government Agency [4]. The survey report of IT market in 2013 showed that the growth rate was 15.6 % with worth 293,239 million baht. If we consider in more details, we found that the all of IT budget of Thai government was around 20.2 % with worth 59,818 million baht. Therefore, Thai government would like to reduce and duplicate of overall IT budgets but still has effectiveness to manage IT system for all sectors of government.

Currently, mobile devices are very more widely used in our society. The IDC reported of second quarter of 2015 [5, 6], there were 341.5 million smart phones delivered to end users, which was growth around 13 %. Samsung was the first rank of the market share with 21.4 % and Apple was the second rank with 13.9 %. The report also showed that the growth rate of smart phones trended to increase continuously according to 4G telecommunication network.

There are several information systems available in our diary life which typically use knowledge-based authentication such as password, therefore users have to remember all passwords which are difficult to remember all of those. If users write passwords on papers or save on to smart phones or computers which may be stolen or hacked by hackers. Everyone would get risk when using network or internet including cloud computing. One of the most important issues of cloud computing is security. Therefore researcher would like to propose adaptive biometric authentication for accessing services on cloud computing using smart phones. The proposed adaptive biometric authentication uses sequence authentications instead of multi-modal approaches which has advantages such as fast, flexible and security level. The current status of this research is on developing phase.

มหาวิทยาลัยรังสิต Rangsit University

2 Related Work

Atmakuri [7] had proposed new biometric authentication framework using face authentication which should be better than previous. The main research objective was to study current several biometric authentication techniques. The researcher suggested that selection of biometric authentication technique should consider the available resources within mobile devices. The researcher also compared the proposed framework and other techniques by considering accuracy, cost, long term stability and security level.

Rotika [8] had studied and compared totally 13 biometric authentication techniques, then researcher had assessed all of these techniques by using seven factors proposed by Jain et al. [9] including universality, uniqueness, performance, collectability, permanence, acceptability and circumvention. Furthermore researcher suggested that using only one biometric authentication might not enough for biometric authentication because each biometric authentication has difference either advantages or disadvantages. And also each of biometric sensors may have difference approach to detect the biometric features. Therefore researcher had suggested using more than one biometric authentication which can improve security level. This research used biometric authentication using both face and hand authentications. The results showed that this approach had 99.82 % of accuracy. The researcher used six assessment factors including enrollment, renewal, machine requirements and public perception.

Romo [10] had proposed framework for biometric authentication on mobile devices named physical smart key which composed of five components including RFID manager, encryption layer, policy manager, hardware key and device id. The researcher represented the results of this study with 10 biometric authentication techniques. The researcher had assessed these techniques by using 3 factors including usability, deploy ability and security. The results of this research showed that the proposed framework had highest score with 84 points. However the researcher also mention about the proposed framework that if user had loss the physical smart key or the mobile devices was stolen, therefore the devices can also be accessed by other people.

Ahn et al. [11] had suggested that authentication was very importance for accessing cloud computing. They also had suggested that there still have problems for users to enter identity repetitiously for accessing cloud computing that are waste time and inconvenience for users. Therefore researchers had proposed framework which used concept of provisioning in cloud computing environment for authentication. This framework would analyze user information and authentication using user profile, therefore this could be solved the inconvenience way of authentication repetitiously. However this approach had some security issues due to storing user profile on the server, user profile would get in risk.

Sharmaand Mittal [12] had mentioned that cloud computing was the results of the advancement of the current technology. It was a combination of automated computing, client-server model, grid computing, mainframe computer, utility-computing

มหาวิทยาลัยรังสิต Rangsit University

peer-to-peer, and game on cloud. Cloud computing technology has several advantages for either personnel use or organizations, however there still has some issues especially security on cloud computing utilization. The researchers had compared several authentication techniques for verification of cloud users and cloud broker. The results of this research showed that the three appropriate authentication techniques were authentication using Kerberos, authentication using key distribution center and authentication using public key infrastructure.

Peer and Bule [13] had some opinions which the amounts of biometric information from several organizations are increasing rapidly; therefore the organizations have to plan and analyze either the capacity of the storage or the capacity of computation. The researcher has suggested that cloud computing technology could be utilized the solve problems of capacity of storage and computation dynamically. However using cloud computing technology should be concerned of problems and obstructions of changing technology, standards of cloud computing and the available approaches to solve the problems. The research was implemented by using finger printing biometric authentication for accessing learning management system on cloud computing.

Fathima et al. [14] have mentioned that biometric authentication systems have obtained more attention due to the security issues. The main objective of this study is to develop a multi-modal, multi-sensor based person authentication system (PAS) using joint directors of laboratories (JDL) fusion model. This study also explores the need for multi sensors, multiple recognition algorithms and multiple fusion level by using face, fingerprint and iris biometrics. The researchers have showed the advantage of using multiple modalities for authentication with using decision fusion scheme. The results of this research showed that the proposed multisensory PAS overcomes the weaknesses of each individual sensor and gives better detection rate.

From the literature reviews, we have found that security issue is one of an importance issue which should be concerned carefully. Even though cloud computing provides easy and convenience way to access from internet, the unauthorized people may also access to cloud computing which may cause of the unpredictable damages. Furthermore, accessing to cloud computing by using mobile devices is increase dramatically which also may cause of unauthorized accessing. Therefore authentication is one of appropriate approaches to prevent unauthorized accessing for cloud computing. The results of the literatures were the study or comparison of several authentication techniques which were to find the appropriate or the best approaches to solve the security issues. The authentications include knowledge-based authentication, device/token-based authentication or biometric authentication. Besides the study of Rotika was found that there still does not have a single perfectly approach of authentications, therefore composing of multiple authentications at same time as a hybrid should be used to improve security level of authentication.

มหาวิทยาลัยรังสิต Rangsit University

3 Proposed Framework

The proposed of conceptual framework composes of three layers including client layer, application layer and database layer as Fig. 1. Client layer is an application which runs on client smart phones. Clients can use this application for either enrollment or verification. Clients will provide information such as account name, password, email, scanned face, voice and etc. The application will also display the result of authentication. Application layer is some applications which run on cloud computing platform. These applications will act as biometric authentication applications which were used in this research. For example, face authentication processes compose of face preprocessing, feature extractions, template creation, learning of face and face recognition. Database layer is database management system which also runs on cloud computing platform. DBMS is used to manage biometric information including add, delete, update or retrieval. For security enhancement, some critical information will be encrypted stored in database system.

This research puts either application layer or database layer on cloud computing because there are several advantages of cloud computing such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service as described in Importance Characteristics of cloud computing by NIST [15]. The adaptive biometrics authentication approach is sequential authentications

Fig. 1 Proposed conceptual framework of this research

มหาวิทยาลัยรังสิต Rangsit University

which also uses more than one authentication which will provides fast, flexible and secure authentication. Authentication administrators can manage the authentication techniques from knowledge-based such as password, token-based such as magnetic-striped card or biometric such as face or voice. Authentication level may be one, two or more sequence of authentications. Authentication processes will work on cloud computing which provides not only flexibility for managing and extendibility of capacity of storage and computation.

4 Research Methodology

This research methodology composes of two major parts as following subsections. The first part is the research for develop the biometric authentication system which composes of client side application, applications on server side and database on another database server.

4.1 Development Research

The development research is the systematically processes to develop the adaptive biometric system by finding and discovering related information. There are three parts to be developed as described in conceptual framework including client side, server side and database management system. The mobile application will be developed on client side. The server side will be developed some applications for adaptive biometric authentications which work on cloud computing. Finally DBMS will be a open source DBMS will also work on cloud computing.

4.1.1 Populations are related documents or information.

4.1.2 Research tools are smart phones which using iOS or android operating system, internal or external cloud computing and developing tools.

4.1.3 Data will be collected by researchers by developing the proposed biometric authentication system.

4.1.4 Data analysis will use fundamental statistics such as frequently or mean for example.

4.2 Survey Research

This part aims to gather satisfactions from users who use the system by using online survey questionnaires which compose of four sections including general information, user interface and design, system performance, and usability.

4.2.1 Populations are Thai people. This research use simple sampling method which is around 100 students from the university.

มหาวิทยาลัยรังสิต Rangsit University

4.2.2 Research tools are smart phones which using iOS or android operating system, internal or external cloud computing and developing tools.
4.2.3 Data will be collected by researchers by using survey questionnaires.
4.2.4 Data analysis will use fundamental statistics such as frequently or mean for example.

5 Conclusion

Security is one of the most importance issues which have to be concerned when deploying cloud computing technology. Therefore authentication should be used to verify the authorized users when connecting via internet. There are three majors authentication including knowledge-based, token-based and biometric authentication. Each of them may have some advantages or some drawbacks depending security level to be used. By using a single biometric authentication provides fast and easy approach, however this may not provide enough security level in this day. Therefore multi-modal is proposed to improve higher security level; however this approach is more complicate, slower and higher costs [14, 16]. Furthermore, there may some limitation of available resources or sensors on iPhone. Therefore we would like to propose adaptive biometric authentication which will provide fast, flexible and high security level. This research has two majors including development research and survey research.

References

1. Forecast: Public Cloud Services, Worldwide, 2011–2017, 4Q13. Gartner (2013)
2. Enterprise Cloud Adoption Survey 2014 Everest Global Inc., Everest Group (2014)
3. VMWare Cloud Index. Forester. http://www.vmware.com/ap/cloudindex
4. Government Cloud Service. https://www.ega.or.th/th/content/890/273/
5. Worldwide Smartphone Growth Forecast to Slow from a Boil to a Simmer as Prices Drop and Markets Mature, According to IDC. IDC (2015). http://www.idc.com/getdoc.jsp?containerId=prUS25282214
6. Smartphone Vendor Market Share, 2015 Q2. IDC. http://www.idc.com/prodserv/smartphone-market-share.jsp
7. Atmakuri, S.M.: A study of authentication techniques for mobile cloud computing. In: ProQuest LLC (2015)
8. Rokita, J.: Multimodal biometric system based on face and hand images taken by a cell phone. ProQuest Dissertations and Theses (2008)
9. Jain, A.K., Hong, L., Pankanti, S., Bolle, R.: An identity-authentication system using fingerprints. Proc. IEEE 85(9), 1365–1388 (1997)
10. Romo, J.T.: Towards seamless and secure mobile authentication. In: ProQuest LLC (2014)
11. Ahn, H., Chang, H., Jang, C., Choi, E.: User authentication platform using provisioning in cloud computing environment. In: Advanced Communication and Networking. Communications in Computer and Information Science, vol. 199, pp. 132–138 (2014)

มหาวิทยาลัยรังสิต Rangsit University

12. Sharma, S., Mittal, U.: Comparative analysis of various authentication techniques on cloud computing. Int. J. Innov. Res. Sci. Eng. Technol. 2(4) (2013)
13. Peer, P., Bule, J., Gros, J.Ž., Štruc, V.: Building cloud-based biometric services. Informatica 37, 115–122 (2013)
14. Fathima, A.A., Vasuhi, S., Babu, N.T.N., Vaidehi, V., Treesasa, T.M.: Fusion framework for multimodal biometric person authentication system. IAENG Int. J. Comput. Sci. 41(1), 18–31 (2014)
15. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology Special Publication 800-145. U.S. Department of Commerce (2011)
16. Ching, H.C.: Performance evaluation of multimodal biometric systems using fusion techniques. In: ProQuest LLC (2015)

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก ข

บทความที่ตีพิมพ์เผยแพร่ในวารสารวิชาการ TEM Journal ฐานข้อมูล Scopus Q3

Reviewed: The Face Authentication Processes for Accessing Cloud Computing Services using iPhone

มหาวิทยาลัยรังสิต Rangsit University

มหาวิทยาลัยรังสิต Rangsit University

TEM

Home
Instructions
Submit Article
Editorial Board
Archives
Contact

Publication Ethics and Publication Malpractice Statement

Open Access and copyright

TEM JOURNAL - Technology, Education, Management, Informatics

Editorial Board:

Editor-in-Chief:
Prof. dr Camil Sukic

Lector:
Irma Halilovic

Members:

Prof. dr Keiichi Kaneko
(Tokyo University of Agriculture and Technology | TUAT - Department of Computer and Information Sciences, Tokyo, Japan)

Prof. dr Klaus Tochtermann
(ZBW - Leibniz Information Centre for Economics, Germany)

Prof. dr Gillich Gilbert-Rainer
(Eftimie Murgu University in Resita,Department of Mechanical Engineering, Romania)

Samir Khatir, PhD
(Technologiepark, Ghent University, Belgium)

Prof. dr Álvaro Rocha
(University of Lisbon - ISEG, Lisbon, Portugal)

Asst. Prof. Enes Sukic
(UIKTEN - Association for Information Communication Technology Education and Science, Serbia)

Erica Magagnini, PhD
(Università Politecnica delle Marche, Italy)

Maria José Sousa, PhD
(ISCTE-Instituto Universitario de Lisboa, Portugal)

Prof. Dr. Khaled Shaalan
(Faculty of Engineering & IT, The British University in Dubai, UAE)

Asst. Prof. Isaac Lera Castro
(University of the Balearic Islands, Department of Mathematic and Computer Sciences, Spain)

Prof. dr Borut Buchmeister
(University of Maribor, Slovenia)

Ing. Darina Dupláková, PhD
(Faculty of Manufacturing Technologies with a seat in Prešov, Technical University of Košice, Slovakia)

Stamatis Papadakis, PhD
(Faculty of Education, University of Crete, Crete, Greece)

Assoc. Prof. dr. Kuaanan Techato
(Faculty of Environmental Management, Prince of Songkla University, HatYai, Songkhla, 90110, Thailand)

Prof. dr Bekim Fetaji
(University Mother Teresa, Faculty of Informatics,
Skopje, Macedonia)

Asst. Prof. Dominik Zimon
(Rzeszow University of Technology,
Department of Management Systems and Logistics, Poland)

Prof. dr Jeroslav Zivanic
(University of Kragujevac, Serbia)

Prof. dr Petre Lucian Ogrutan
(Transilvania University of Brasov,
Faculty of Electrical Engineering and Computer Science, Romania)

Prof. dr Danijela Milosevic
(University of Kragujevac, Serbia)

Prof. dr Marko Hölbl
(University of Maribor, Faculty of Electrical Engineering and Computer Science (FERI), Slovenia)

Prof. dr Aleksandar Kupusinac
(University of Novi Sad, Faculty of Technical Sciences, Serbia)

Prof. dr Marina Klacmer Calopa
(University of Zagreb, Faculty of Organization and Informatics (FOI), Croatia)

Copyright © 2012-2022 UIKTEN, All Rights reserved
Copyright licence: All articles are licenced via Creative Commons CC BY-NC-ND 4.0 licence

มหาวิทยาลัยรังสิต Rangsit University

TEM

Home
Instructions
Submit Article
Editorial Board
Archives
Contact

Open Access and copyright

Publication Ethics and Publication Malpractice Statement

Clarivate Analytics
WEB OF SCIENCE
Scopus
INDEX COPERNICUS INTERNATIONAL
DOAJ DIRECTORY OF OPEN ACCESS JOURNALS
Research Bib.
getCITED
Google scholar
EBSCO HOST
academia.edu follow research
Universität Regensburg
University Library of Regensburg
TIB German National Library of Science and Technology

Tem Journal, Vol.7, No.3, August 2018 :

Title: *Reviewed: The Face Authentication Processes for Accessing Cloud Computing Services using iPhone*

Authors: Sorapak Pukdesree, Paniti Netinant

DOI: 10.18421/TEM73-01

[abstract] full text] how to cite]

Title: Calculation and Simulation Model of a System RopeCon

Authors: Gabriel Fedorko, Vieroslav Molnár, Melichar Kopas

DOI: 10.18421/TEM73-02

[abstract] full text] how to cite]

Title: *Use of Educational Computer Games in the Initial Assessment and Therapy of Children with Special Educational Needs in Bulgaria*

Authors: Margarita Stankova, Valentina Ivanova, Tsveta Kasnerski

DOI: 10.18421/TEM73-03

[abstract] full text] how to cite]

Title: *The Effectivity of Authentic Assessment Based Character Education Evaluation Model*

Authors: Abd Azis Karim, Amir Abduh, Darman Manda, Muhammad Yunus

DOI: 10.18421/TEM73-04

[abstract] full text] how to cite]

Title: Evaluation of the Logistic Process Robotisation Using the Multiple-Criteria Decision-Making

Authors: Zdeněk Čujan, Daniela Marasová

DOI: 10.18421/TEM73-05

[abstract] full text] how to cite]

มหาวิทยาลัยรังสิต Rangsit University

Title: *Examining Technological and Pedagogical Content Knowledge of Special Education Teachers Based on Various Variables*

Authors: Mukaddes Sakalli Demirok, Basak Baglama

DOI: 10.18421/TEM73-06

[abstract] [full text] [how to cite]

Title: *Instructors' Behavioural Intention to use Learning Management System: An Integrated TAM Perspective*

Authors: Shamsul Anuar Mokhtar, Hamidon Katan, Imdadullah Hidayat-ur-Rehman

DOI: 10.18421/TEM73-07

[abstract] [full text] [how to cite]

Title: *Dynamic Quality Evaluation in Higher Education*

Authors: Silvia Gaftandzhieva, Rositsa Doneva, George Totkov

DOI: 10.18421/TEM73-08

[abstract] [full text] [how to cite]

Title: *Time Future Teacher Spend on Facebook and Playing Online Video Games*

Authors: Maja Ružić-Baf, Hany Tutan

DOI: 10.18421/TEM73-09

[abstract] [full text] [how to cite]

Title: *The Effect of Learning Strategies, Learning Models, and Learning Innovation on Educators' Performance and Education Quality in Senior High Schools in Makassar*

Authors: Erni Ratna Dewi

DOI: 10.18421/TEM73-10

[abstract] [full text] [how to cite]

Title: *The Potential of Augmented Reality to Transform Education Into Smart Education*

Authors: Gabriela Kiryakova, Nadezhda Angelova, Lina Yordanova

DOI: 10.18421/TEM73-11

[abstract] [full text] [how to cite]

Title: *Test Bench for Functionality and Reliability of Power Protection Devices*

Authors: Aurel Cornel Stanca, Anamaria Ordace, Petre Lucian Ogrutan, Lia Elena Actu

DOI: 10.18421/TEM73-12

[abstract] [full text] [how to cite]

Title: *Production of Electric Energy by Use of Wind Energy*

Authors: Naqib Daneshjo, Erika Dudáš Pajerská, Vanda Lieskovská, Jana Naščáková, Enayat Danishjoo

DOI: 10.18421/TEM73-13

[abstract] [full text] [how to cite]

มหาวิทยาลัยรังสิต Rangsit University

Title: Management in Ukraine: Stages of Formation, Development, Types

Authors: Liubov Pshenychna, Olha Skyba

DOI: 10.18421/TEM73-14

[abstract] full text] how to cite]

Title: *Comparative Analysis of European and Global Innovation Performance Barometers*

Authors: Bogdan FLEACĂ

DOI: 10.18421/TEM73-15

[abstract] full text] how to cite]

Title: *Functionality and Quality Management of Transformation of Capital Forms at an Enterprise*

Authors: Irina Gontareva, Irina Murenets, Petro Kurmaiev, Svitlana Podzihun, Oleksandr Dorokhov

DOI: 10.18421/TEM73-16

[abstract] full text] how to cite]

Title: *The AHP Method Implementation for ERP Software Selection with Regard to the Data Protection Criteria*

Authors: Marcela Malindzakova, Dominik Puskas

DOI: 10.18421/TEM73-17

[abstract] full text] how to cite]

Title: *Non-Destructive Diagnostics of Hard-to-Reach Places by Spatial Digitization*

Authors: Monika Teliškova, Jozef Török, Darina Duplákova, Jakub Kaščák, Viktória Mezencevová, Jaroslav Birčák

DOI: 10.18421/TEM73-18

[abstract] full text] how to cite]

Title: *Predicting Student Success Using Data Generated in Traditional Educational Environments*

Authors: Marian Bucos, Bogdan Drăgulescu

DOI: 10.18421/TEM73-19

[abstract] full text] how to cite]

Title: *Concept of SME Business Model for Industry 4.0 Environment*

Authors: Leos Safar, Jakub Sopko, Slavomir Bednar, Robert Poklemba

DOI: 10.18421/TEM73-20

[abstract] full text] how to cite]

Title: *EMS - A Workflow Programming Language and Environment*

Authors: George Pashev, George Totkov

DOI: 10.18421/TEM73-21

[abstract] full text] how to cite]

Title: *Analysis of Apache Logs Using Hadoop and Hive*

Authors: Aleksandar Velinov, Zoran Zdravev

มหาวิทยาลัยรังสิต Rangsit University

DOI: 10.18421/TEM73-22

[abstract] full text] how to cite].

Title: *The Impact of Edmodo Assisted Education on Project Evaluation Achievement Scores and Determination of Opinions for use in Education*

Authors: Tahir Tavukcu

DOI: 10.18421/TEM73-23

[abstract] full text] how to cite].

Title: *Towards Better Understanding of Ancient Civilizations by Storytelling and Gaming*

Authors: Maria Dimova, Desislava Paneva-Marinova, Lilia Pavlova

DOI: 10.18421/TEM73-24

[abstract] full text] how to cite].

Title: *Teachers' Self-Efficacy as a Determinant of Lesson Management Quality*

Authors: Lukáčová Veronika, Fenyvesiová Livia, Tirpáková Anna, Malá Eva

DOI: 10.18421/TEM73-25

[abstract] full text] how to cite].

Title: *Using Animation as a Means of Enhancing Learning of Individuals with Special Needs*

Authors: Basak Baglama, Yucehan Yucesoy, Ahmet Yikmis

DOI: 10.18421/TEM73-26

[abstract] full text] how to cite].

Title: *Face Detection using Min-Max Features Enhanced with Locally Linear Embedding*

Authors: Rahmat Hidayat, Fatin Nabila Jaafar, Ihsan Mohd Yassin, Aziee Zabidi, Fadhlan Hafizhelmi Kamaru Zaman, Zairi Ismael Rizman

DOI: 10.18421/TEM73-27

[abstract] full text] how to cite].

Title: *The Impact of Feedback in Facebook on Students' Language Proficiency*

Authors: Visara Ekahitanond

DOI: 10.18421/TEM73-28

[abstract] full text] how to cite].

Title: *Ontology Concept in Courses on Students*

Authors: Daniela Orozova, Magdalina Todorova

DOI: 10.18421/TEM73-29

[abstract] full text] how to cite].

มหาวิทยาลัยรังสิต Rangsit University

Copyright © 2012-2018 UIKTEN. All Rights reserved
Copyright licence: All articles are licenced via Creative Commons CC BY-NC-ND 4.0 licence

TEM Journal. Volume 7, Issue 3, Pages 475-479, ISSN 2217-8309, DOI: 10.18421/TEM73-01, August 2018.

Reviewed: The Face Authentication Processes for Accessing Cloud Computing Services using iPhone

Sorapak Pukdesree [1,2], Paniti Netinant [2]

[1] School of Information Technology and Innovation, Bangkok University, Thailand
[2] College of Information and Communication Technology, Rangsit University, Pathumthani, Thailand

Abstract – **Presently, there are several IT services that provide services for convenient access. Users can access those services by local access or remote access from anytime or anywhere including services which are on cloud computing system. Furthermore, mobile devices are very more widely used in our society as we have seen the large number of delivered mobile devices each year. However, the security for accessing the cloud services must be concerned because there are many of illicit uses of the processes easier for fraudsters. Authentication is one of the ways to prevent fraudsters. This research proposes both physical features by using face recognition and voice recognition system and behavioural feature using password. This paper describes face recognition processes in more detail. Researchers also proposed adaptive biometric authentication for accessing cloud computing services using iPhone. The research integrates the adaptive biometric authentication with multi-modal approaches which have advantages in term of flexibility and security. The status of this research is in progress.**

Keywords – **Cloud computing, Adaptive, Face Recognition, Biometric Authentication.**

DOI: 10.18421/TEM73-01
https://dx.doi.org/10.18421/TEM73-01

Corresponding author: Sorapak Pukdesree,
School of Information Technology and Innovation, Bangkok University, Thailand
Email: sarapuck.p@bu.ac.th

Received: 13 March 2018.
Accepted: 11 July 2018.
Published: 27 August 2018.

© 2018 Sorapak Pukdesree, Paniti Netinant; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.

The article is published with Open Access at www.temjournal.com

1. Introduction

The researchers have proposed the overall conceptual framework of the Adaptive Biometrics Authentication for Accessing Cloud Computing Services using iPhone [1]. Researchers describe more thoroughly details of the proposed framework. The proposed conceptual framework composes of three major layers including client layer, application layer and database layer. The overall process can also be divided into two major phases including enrollment phase and testing phase. In enrollment phase, clients can provide their information such as account name, password, email, scanned face, recorded voice and so on. System administration can also enter the prepared information manually into the database as batch processing mode. The information will be preprocessed and stored into database which is on cloud computing. The second phase is the testing phase where clients can try to use their biometric information such as face, voice or password to get the authentication for accessing the desired applications on cloud computing platform. This research uses multi-modal biometric authentication with an adaptive approach [3,4,12]. However, this paper describes in more detail just only the face recognition processes.

Figure 1. Face Recognition Processes of the proposed framework

TEM Journal. Volume 7, Issue 3, Pages 475-479, ISSN 2217-8309, DOI: 10.18421/TEM73-01, August 2018.

2. Literature Review

Bharadwaj, S., Bhatt, H. S., Singh, R., Vatsa, M., and Noore, A. [9] had proposed QFuse as a new framework in their research. They mentioned that biometrics is increasingly being used in many applications. The current techniques are unable to provide significant levels of accuracy in uncontrolled environments. This paper presented an adaptive context switching algorithm with an online learning framework. This proposed framework uses the quality of input images to dynamically select the best biometric matcher of fusion algorithm. The results showed that the algorithm can improve the optimization of accuracy and computation time.

Veeramachaneni, K., Osadciw, L. A., and Varshney, P. K. [10] had proposed AMBM algorithm to sensor management of a biometric security system which can help to improve the robustness of the system. Multiple biometric data are fused at the decision level which meets more challenging and varying accuracy requirements. This approach can be adapted to meet the varying system needs by particle swarm optimization. The AMBM algorithm selects the fusion rule and sensor operating points to optimize system performance.

Kumar, A., Kanhangad, V., and Zhang, D. [11] had proposed their research with a new framework for adaptive multimodal biometrics management. The major objective was to ensure the optimal performance for the desired level of security. The research uses score-level fusion rules which are adapted to ensure system performance using hybrid particle swam optimization model. The experimental results showed that the adaptive selection of fusion rules using hybrid PSO-based approach can give better performance than the decision-level scheme using PSO.

Latha, L. and Thangasamy, S. [12] had also studied multimodal biometric authentication using five component traits. They indicated that a single biometric authentication is often much limited therefore a multimodal approach is proposed. This research used five component traits such as iris, ear, palm print, fingerprint and retina. The scores of each biometrics will be combined using weighted sum fusion rule. The research was tested on five different datasets. The results showed that this multimodal biometric authentication system is much more dependable and precise than a single biometric modal.

Varuvanathorn, S. and Nitsuwat S. [13] had purposed their research which used the global face features along with triangle geometry of 4 segments including left eye, right eye, nose and mouth. The research objective was to improve the efficiency of identifying person using face recognition. The research used approximately 120 images of faces for training and testing. The results showed that this technique can improve the efficiency of identifying person using face recognition by 4.16% compared to the technique which used only whole features of the face.

Duangsang, B. [14] had proposed their research of human face recognition using Principle Component Analysis technique to detect human face. The research consisted of two phases including detection and recognition phases. The detecting and verify the human face used Template matching from eye region. The recognition phase used eigenfaces and neural network with color model.

Huang, Z., Liu, Y., Li, X., and Li, J. [15] had proposed the adaptive face and ear biometric recognition framework using sparse coding (ABSRC) which can effectively reduce the adverse effect of degraded modality. ABSRC consisted of two-phase sparse coding strategy. First, face and ear features are separated encoding. Then the weighted features are integrated to form a unique feature vector. The results of the experiment showed that the framework can improve robustness to various kinds of image regression and outperforms the current methodologies such as MSRC, MWGSR and also other conventional multimodal methods.

3. Face Recognition in the Research

Face Recognition Processes as shown in Figure 1 are the processes to identify the real person using automatic system. In this research, the images of a person will be gained from digital camera of an iPhone. The face recognition will compare the tested facial features of the image and the facial features in the collected database. Face Recognition Processes consist of four major processes. The result of the previous process will be the input of the next process. Therefore, the quality of the result of the previous process may affect to the result of the next processes.

3.1. Face Detection

This process is used to locate a face region on the image typically indicated by a large rectangle on the screen. The current face detection techniques are entirely dependable in the currently uses, however, the current face recognition techniques are much less reliable in the currently uses. There are many face detection techniques implemented in camera devices including iPhone or other smartphones. The current face recognition techniques are very responsive to common uses, such as the level and the direction of contrast, the noise of the image sensors, the orientation of the faces, the expression of the face, and so on. Therefore these may give unexpected results.

TEM Journal. Volume 7, Issue 3, Pages 475-479, ISSN 2217-8309, DOI: 10.18421/TEM73-01, August 2018.

From the literature review, this research will use the LBP-based technique [5,8] of face detection. LBP-based technique uses histograms method of pixel intensity collating, such as edges, corners, and flat regions; on the other hand, Haar-based technique checks the facial region by comparing the regions of the specific features with other regions in the images which it often does thousands of checking per image. LBP-based technique can be used not only to improve face detection with more dependable but also to reduce computing time. This technique [5,6,8] has several advantages than the other techniques. In conclusion, the LBP-based detectors are significantly faster than the Haar-based detectors for several times.

This research will set up LBP-based parameters for 4-channel BGRA because the images will be gathered from iPhone as image sensor. The example of LBP calculation is shown in Figure 2. The original LBP operator labels the pixels of an image by determined the threshold of each pixel using 3-by-3 values surrounding of the center pixel and considering the result as a binary number.

145	146	153
147	150	156
158	159	156

Example

0	0	1
0		1
1	1	1

Threshold

$(01111100)_2 = 124_{10}$

Pattern

Figure 2. Example of LBP calculation.

Face detection algorithm will typically works on grayscale [2,5] images therefore all the gathered images needed to be converted from color camera images to grayscale images which has values between 0-255 intensity levels of color. For images in color spaces such as RGB color which is used in standard color TV and also the camera sensors of mobile devices. Y' can be computed from gamma compressed intensities as a summation of weighted values as shown in formula (1). The example of conversion from color image into grayscale is shown in Figure 3.

$$Y' = (0.299xR) + (0.587xG) + (0.114xB) \quad (1)$$

Figure 3. Conversion from RGB color into grayscale color. [2]

The celerity of face detection will also count on the size of the input images. Therefore it may be slow for larger images but it may be fast for smaller images. Hence the images from camera censors are needed to reduce the suitable sizes. Typically face detection usually works well for image size greater than 240x240 pixels [6] therefore this research reduces the image size to 240 pixels of width. Furthermore the images are needed to keep the aspect ratio between width and height as the same as the input images as shown in Figure 4.

```
scaledHeight = Round (img.rows / scale);
resize(img, smallImg, Width, scaledHeight));
```

Figure 4. To keep the aspect ratio of width and height of image.

Face detection is also not dependable in low light conditions. Therefore the images are needed to perform histogram equalization [6,7] which helps to improve the contrast and brightness of the images. Histogram equalization is also very important process for the facial recognition process. Histogram equalization is very useful process which will distribute the intensity of the images as shown in Figure 4. This process makes the areas of lower contrast to get a higher contrast and brightness.

Figure 5. Example of histogram equalization [7].

3.2. Face Preprocessing

The quality of input images is very important process to the rest of the face recognition processes. Therefore face processing process is needed to improve the noises of the images such as low lighting conditions, face orientation, face expression, and so on. Hence it is very important to reduce these noises as much as possible. This process focuses on eye search regions, histogram equalization, and elliptical mask of the images.

Face preprocessing consists of three tasks including 1) eye search regions which consist of

TEM Journal. Volume 7, Issue 3, Pages 475-479, ISSN 2217-8309, DOI: 10.18421/TEM73-01, August 2018.

geometrical transformation and cropping: This process focuses on the alignment of eyes which would include scaling, rotating, and translating the images, and then followed by the removal of the forehead, chin, ears, and background from the images 2) histogram equalization for left and right sides. This process will diffuse the brightness and contrast on both the left- and right-hand sides of the face equally. Furthermore, this process will reduce the image noise either. 3) The elliptical mask will remove some remaining hair and some background from the face image which will result only in the facial image.

3.3. Face Training

After collecting the desired face images of each person, the face recognition system must be trained by learning the facial data using a machine-learning algorithm which suites face recognition. There are many different face recognition algorithms in the literature; the simplest algorithms are eigenfaces and Artificial Neural Networks, however eigenfaces tends to work better than the ANNs [6]. Although eigenfaces is simple method, it can do the work as well as other complex face recognition algorithms. Therefore, it has become very popular as the basic face recognition algorithm for everyday use.

It is also very important that the training set has not only having enough varieties to cover the testing set, but also having a large number of faces. Therefore the collected faces in the training set should be differences of each person. There should not be the same images of each person. The collected faces should collect direct face, left-side faces, right-side faces, and some other face directions.

3.4. Face Recognition

Face Recognition process is the process that is capable to identify or verify a person by using his face image from iPhone camera with the facial features stored in the database. In this research is used the principle component analysis which uses eigenfaces. There are also some other recognition algorithms which use fisherfaces algorithm such as linear discriminate Analysis, elastic bunch graph matching. The results of this process are the scores of matching process of each test which will be used to determine that the person is the member of a system or not. If the person is determined as a member of the system, he will be allowed to access the services provided on the cloud. If the person is determined as not to be the member of the system, he will be denied access to the services provided on the cloud.

4. Adaptive Methodology

This research uses not only biometric characteristics such as face recognition and speech recognition but also behavioral characteristic such as password as traditional methodology. Multi-biometric systems can be integrated from multiple biometric sources. This method can be used to overcome the limitations of non-universality or noisy sensor data to prevent spoof attacks or fraudsters encountered in mono biometric systems. The research also applies adaptive methodology which makes more dynamically entering the input sensor data instead of sequentially entering the data as shown in Figure 5. and 6. The system administrator can select types and also can select the numbers of input data which make the authentication more complex, more flexible and more secure.

Figure 5. Sequential entering input sensor data

Phase1	Phase2	Phase3
Face recognition/ Speech recognition / Password	Face recognition/ Speech recognition / Password	Face recognition/ Speech recognition / Password

Figure 6. Adaptive entering input sensor data

5. Conclusion

This paper described the face recognition processes which are used as a part of authentication for accessing cloud computing services using iPhone. First, starting with face detection process is the process that locates the face of the human in the images using the LBP-based technique. Second, face preprocessing process is the process that reduces the noise of facial images and also improves the quality of the images such as contrast and brightness, and face orientation. Third, the system is needed to train the preprocessed facial data using a machine-learning algorithm relying on eigenfaces. Finally, the face recognition processes perform the verification of the testing faces with facial features which are stored in the cloud computing data storage. In the research, we also deploy the adaptive approach with the proposed authentication method.

TEM Journal. Volume 7, Issue 3, Pages 475-479, ISSN 2217-8309, DOI: 10.18421/TEM73-01, August 2018.

References

[1]. Pukdesree, S., & Netinant, P. (2016). Conceptual framework: The adaptive biometrics authentication for accessing cloud computing services using iPhone. In *Recent Advances in Information and Communication Technology 2016* (pp. 209-216). Springer, Cham.

[2]. Grayscale. Retrived from: https://en.wikipedia.org/wiki/Grayscale.

[3]. Soltane, M. (2015). Face, Voice and Signature Multi-Modal Biometric Verification Fusion Systems. *Annals of the Faculty of Engineering Hunedoara*, *13*(4), 139.

[4]. Cutshaw, J. (2015). *Online authentication challenges for financial institutions in a complex digital era* (Doctoral dissertation, Utica College).

[5]. Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on pattern analysis and machine intelligence*, *24*(7), 971-987.

[6]. Emami, S. (2012). Face Recognition using Eigenfaces or Fisherfaces. *Mastering OpenCV with Practical Computer Vision Projects. Pact Publishing*.

[7]. Histogram equalization. Retrived from: https://en.wikipedia.org/wiki/Histogram_equalization

[8]. Local binary patterns. Retrived from: https://en.wikipedia.org/wiki/Local_binary_patterns.

[9]. Bharadwaj, S., Bhatt, H. S., Singh, R., Vatsa, M., & Noore, A. (2015). QFuse: Online learning framework for adaptive biometric system. *Pattern Recognition*, *48*(11), 3428-3439.

[10]. Veeramachaneni, K., Osadciw, L. A., & Varshney, P. K. (2005). An adaptive multimodal biometric management algorithm. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *35*(3), 344-356.

[11]. Kumar, A., Kanhangad, V., & Zhang, D. (2010). A new framework for adaptive multimodal biometrics management. *IEEE transactions on Information Forensics and Security*, *5*(1), 92-102.

[12]. Latha, L., & Thangasamy, S. (2013). Providing multimodal biometric authentication using five competent traits. *The Imaging Science Journal*, *61*(2), 212-218.

[13]. Varuvanathorn, S., & Nitsuwat, S. (2010). Facial recognition and using whole and segment facial features with the triangular geometry of the eyes and mouth together with the geometric face model. *The 6th National Conference on Computing and Information Technology*.

[14]. Duangsang, B. (2013). Facial recognition using Principle Component Analysis technique. Thesis. Faculty of Engineering, Kasetsart University.

[15]. Huang, Z., Liu, Y., Li, X., & Li, J. (2015). An adaptive bimodal recognition framework using sparse coding for face and ear. *Pattern Recognition Letters*, *53*, 69-76.

มหาวิทยาลัยรังสิต Rangsit University

ภาคผนวก ค

บทความที่ตีพิมพ์เผยแพร่ในวารสารวิชาการ

International Journal of Information Technology and Web Engineering

ฐานข้อมูล Scopus Q3

Biometric Cloud Services for Web-Based Examinations: An Empirical Approach

มหาวิทยาลัยรังสิต Rangsit University

มหาวิทยาลัยรังสิต Rangsit University

open Access

PDF

Help

(http://wokinfo.com/products_tools/multidisciplinary/esci/)

International Journal of Information Technology and Web Engineering (IJITWE)

This journal was converted to full Gold Open Access on January 1, 2022

Editor-in-Chief: Ghazi I. Alkhatib (/affiliate/ghazi-i-alkhatib/370253/) (The Hashemite University, Jordan (retired))

Indexed In: Compendex (Elsevier Engineering Index), INSPEC, SCOPUS, Web of Science Emerging Sources Citation Index (ESCI) and 17 more indices

Published: Continuous Volume Established: 2006

ISSN: 1554-1045
EISSN: 1554-1053
DOI: 10.4018/IJITWE

มหาวิทยาลัยรังสิต Rangsit University

Journal Metrics

Submission to Acceptance: Approx. 11 - 15 Weeks
Acceptance to Publication: Approx. 21 - 25 Weeks
Acceptance Rate: 14%

Latest Published Articles

Published: Jan 1, 2022 **DOI: 10.4018/IJITWE.288038**
Volume 17

Winning the War on Terror: Using "Top-K" Algorithm and CNN to Assess the Risk of Terrorists (/article/winning-the-war-on-terror/288038) Open Access Article

From the perspective of counter-terrorism strategies, terrorist risk assessment has become an important approach for counter-terrorism early warning research. Combining with the characteristics of... Show More

Download (PDF): Article (/pdf.aspx?tid=288038&ptid=277628&ctid=4&oa=true&isxn=)
Add to Your Personal Library: Article
Cite Article

Published: Jan 1, 2022 **DOI: 10.4018/IJITWE.288039**
Volume 17

Extracting Entity Synonymous Relations via Context-Aware Permutation Invariance (/article/extracting-entity-synonymous-relations-via-context-aware-permutation-invariance/288039) Open Access Article

Discovering entity synonymous relations is an important work for many entity-based applications. Existing entity synonymous relation extraction approaches are mainly based on lexical patterns or... Show More

Download (PDF): Article (/pdf.aspx?tid=288039&ptid=277628&ctid=4&oa=true&isxn=)
Add to Your Personal Library: Article
Cite Article PDF
Help

Published: Jan 1, 2022 **DOI: 10.4018/IJITWE.297968**
Volume 17

On Cost-Aware Heterogeneous Cloudlet Deployment for Mobile Edge Computing (/article/on-cost-aware-heterogeneous-cloudlet-deployment-for-mobile-edge-computing/297968) Open Access Article

Edge computing undertakes downlink cloud services and uplink terminal computing tasks, data interaction latency and network transmission cost are thus significantly reduced. Although a lot of... Show More

Download (PDF): Article (/pdf.aspx?tid=297968&ptid=277628&ctid=4&oa=true&isxn=)
Add to Your Personal Library: Article
Cite Article

มหาวิทยาลัยรังสิต Rangsit University

View Full Table of Contents › (/journals/open-access/table-of-contents/international-journal-information-technology-web/1093)

Description, Mission, Scope & Coverage

Description:

Organizations are continuously overwhelmed by a variety of new information technologies; many are Web-based. These new technologies are capitalizing on the widespread use of network and communication technologies for seamless integration of various issues in information and knowledge sharing... Show More

Mission & Scope:

The main objective of the International Journal of Information Technology and Web Engineering (IJITWE) is to publish refereed papers in the area covering information technology (IT) concepts, tools, methodologies, and ethnography in the contexts of global communication systems and Web engineered applications. In accordance with this emphasis on the Web and communication systems, this journal... Show More

Coverage:

- Artificial intelligence, machine learning, and deep learning for the Web
- Cloud Edge computing architectures, models, and applications in the Web
- Data analytic (data mining and big data) systems and applications in the Web
- Data and knowledge engineering- capture and quality issues - validation and verification
- Integrated user profile, provisioning, and context-based processing in the Web
- Internet of Things (IoT) and Web of things (WoT) architectures, models, and application studies
- Knowledge structure, classifications, and search algorithms and engines
- Mobile, location-aware, and ubiquitous computing
- Ontology and semantic Web studies
- Quality of service and service level agreement issues among integrated Web systems
- Radio Frequency Identification (RFID) research and applications in Web engineered systems
- Security, integrity, privacy, and policy issues of Web-based systems
- Software agent-based systems and applications in the Web
- Web systems architectures, including distributed grid computing and communication systems processing
- Web systems engineering design and implementation
- Web systems performance engineering studies
- Web user interfaces design, development, and usability engineering studies
- Web-based block-chain tools, applications, and case studies
- Web-based digital forensic tools, analysis, recovery, and applications

PDF

Help

Editorial Board

Editor-in-Chief Emeritus

Zakaria Maamar, Zayed University, United Arab Emirates

Managing Editors

Farid Meziane, University of Salford, United Kingdom https://orcid.org/0000-0001-9811-6914 (https://orcid.org/0000-0001-9811-6914)
Vanilson Buregio, Federal Rural University of Pernambuco, Brazil, Brazil

Associate Editors

Alexander Alfimtsev, Bauman Moscow State Technical University, Russian Federation https://orcid.org/0000-0002-3805-4499 (https://orcid.org/0000-0002-3805-4499)
Andres Iglesias Prieto, University of Cantabria, Spain
Evelina Pencheva, Technical University of Sofia, Bulgaria
Michele Ruta, Politecnico di Bari, Italy
Muhammad Hafidz Fazli Bin Md Fauadi, Universiti Teknikal Malaysia Melaka, Malaysia
Navin Kumar, University of Maryland Baltimore County, United States https://orcid.org/0000-0001-8078-6012 (https://orcid.org/0000-0001-8078-6012)
Thar Baker, Liverpool John Moores University, United Kingdom https://orcid.org/0000-0002-5166-4873 (https://orcid.org/0000-0002-5166-4873)
Xiaomo Liu, Thomson Reuters Corporation, United States
Yacine Atif, University of Skovde, Sweden

Editorial Review Board

Abbas Aljuboori, University of Information Technology and Communications, Iraq https://orcid.org/0000-0001-7676-9615 (https://orcid.org/0000-0001-7676-9615)
Abdelaziz OUADAH, Higher National School of Computer Science (ESI ex INI), Algeria https://orcid.org/0000-0001-7236-8056 (https://orcid.org/0000-0001-7236-8056)
Abhishek Bhattacharya, Institute of Engineering & Management, India
Alexander Alfimtsev, Bauman Moscow State Technical University, Russian Federation https://orcid.org/0000-0002-3805-4499 (https://orcid.org/0000-0002-3805-4499)
Ali Al-Frajat, Concordia University, Canada
Arti Jain, Jaypee Institute of Information Technology, Noida, India https://orcid.org/0000-0002-3764-8834 (https://orcid.org/0000-0002-3764-8834)
Atilla Elçi, Hasan Kalyoncu University, Turkey, Turkey https://orcid.org/0000-0002-3329-0150 (https://orcid.org/0000-0002-3329-0150)
Avanija Janagaraj, Sree Vidyanikethan Engineering College, Tirupati, Andhra Pradesh, India https://orcid.org/0000-0003-0605-7609 (https://orcid.org/0000-0003-0605-7609)
Belal Abuata, Yarmouk University, Jordan
Bilal Abu Salih, The University of Jordan, Australia https://orcid.org/0000-0001-9875-4369 (https://orcid.org/0000-0001-9875-4369)
Chang-ai Sun, University of Science and Technology Beijing, China
Dilip Sharma, GLA University Mathura Uttar Pradesh India, India
Dora Melo, Coimbra Business School - ISCAC, IPC, Portugal https://orcid.org/0000-0003-3744-2980 (https://orcid.org/0000-0003-3744-2980)
Feng Qiu, University of Victoria https://orcid.org/0000-0002-3012-3672 (https://orcid.org/0000-0002-3012-3672)
Fu Zhang, Northeastern University
Gregory Wanyembi, Mount Kenya University, Kenya
Gulshan Shrivastava, Sharda University, India https://orcid.org/0000-0003-3671-4921 (https://orcid.org/0000-0003-3671-4921)
Izzat Alsmadi, Texas A&M University-San Antonio, United States https://orcid.org/0000-0001-7832-5081 (https://orcid.org/0000-0001-7832-5081)
Jan Stage, Aalborg University, Denmark
Jibitesh Mishra, College of Engineering & Technology, India https://orcid.org/0000-0003-2761-470X (https://orcid.org/0000-0003-2761-470x)
Khaled Rezeg, University of Biskra, Algeria https://orcid.org/0000-0001-7458-2531 (https://orcid.org/0000-0001-7458-2531)
M. KURDI, University of Lynchburg, United States https://orcid.org/0000-0002-1524-066X (https://orcid.org/0000-0002-1524-066x)
Michele Tomaiuolo, University of Parma, Italy https://orcid.org/0000-0002-6030-9435 (https://orcid.org/0000-0002-6030-9435)
Petr Křemen, Czech Technical University in Prague, Czech Republic
Raoudha Ben Djemaa, University of Sousse, Tunisia https://orcid.org/0000-0002-7831-112X (https://orcid.org/0000-0002-7831-112x)
Samer Zain, Birzeit University, Palestinian Territory, Occupied
SANDEEP BOTHRA, Manipal University Jaipur, Jaipur, Rajasthan, India, India https://orcid.org/0000-0003-0555-569X

PDF
Help

มหาวิทยาลัยรังสิต Rangsit University

(https://orcid.org/0000-0003-0555-569x)
Sang-Bing Tsai, Nankai University, Taiwan https://orcid.org/0000-0001-6988-5829 (https://orcid.org/0000-0001-6988-5829)
Sarbjeet Singh, University Institute of Engineering and Technology, Panjab University, India
Surjit Singh, Thapar Institute of Engineering & Technology, Patiala, Punjab, India, India https://orcid.org/0000-0002-2386-7729 (https://orcid.org/0000-0002-2386-7729)
Usama Maabed, Alexandria University, Qatar https://orcid.org/0000-0002-8620-2740 (https://orcid.org/0000-0002-8620-2740)
Vijender Solanki, CMR Institute of Technology (Autonomous), India https://orcid.org/0000-0001-5784-1052 (https://orcid.org/0000-0001-5784-1052)
Wei Zhang, Thumbtack Inc., United States
Xu An Wang, Engineering University of CAPF, China
Yahia Lebbah, University Oran1, Laboratoire LITIO, BP 1524 El-M'Naouer, 31000 Oran, Algeria, Algeria
Yaser Jararweh, Jordan University of Science and Technology, Jordan
Ying Zhang, North China Electric Power University, China
Zahi Jarir, Cadi Ayyad University, Morocco https://orcid.org/0000-0002-6425-1031 (https://orcid.org/0000-0002-6425-1031)

Reviewer Application > (/journals/become-a-reviewer/)

Editorial Policy

IGI Global holds its journals to the highest ethical practices. View Full Editorial Policy (/publish/contributor-resources/open-access-journal-editorial-policy/)

Abstracting and Indexing

Compendex on Engineering Village

Compendex (Elsevier Engineering Index)

(/journals/indices/compendex-elsevier-engineering-index/7/) (/journals/indices/inspec/28/) (/journals/indices/scopus/39/) PDF

Help

IET Inspec

INSPEC

Scopus®

SCOPUS

มหาวิทยาลัยรังสิต Rangsit University

WEB OF SCIENCE

Web of Science Emerging Sources Citation Index (ESCI)

(/journals/indices/web-of-science-emerging-sources-citation-index-esci/122/)

Show More

IGI Global Open Access

As an academic publisher at the forefront of advancement for over 30 years, IGI Global OA provides quality, expediate OA publishing with a top-of-the-line production system backed by the international Committee on Publication Ethics (COPE). With a streamlined publishing process, flexible funding options, and more, researchers can freely and immediately share their peer-reviewed research with the world.

- **Rigorous and Expediate** Publishing Process
- Research Is **Fully Free and Accessible** to All (Creative Commons BY License)
- **Increased Discoverability** of Published Content (**89% Higher Download Rate**)
- **Acceleration of Citation Impact** & Increased **Indexing** Potential
- **Greater Visibility** & Wider Professional Recognition
- Opportunities for **Networking & Collaboration**
- Supports Overall **Career Advancement**
- **Affordable Article/Chapter Processing Charges** (APCs/CPCs) (Starting at US$ 500)
- And More.

Learn More (/publish/contributor-resources/open-access/)

Article Processing Charges

PDF

Help

Article Processing Charge (APC):

Payment of the APC fee (directly to the publisher) by the author or a funding body is not required until **AFTER** the manuscript has gone through the full double-blind peer review process and the Editor(s)-in-Chief at his/her/their full discretion has/have decided to accept the manuscript based on the results of the double-blind peer review process. **Please note that IGI Global cannot schedule the article for publication or publish the article until payment has been received.** ***It is also important to note that in scholarly publishing, utilizing an open access journal's resources and time with no intent to pay the open access Article Processing Charge (APC) if the article manuscript is accepted following the peer review process is considered to be unethical and exploitative.***

What Does IGI Global's Open Access APC Cover?

In the traditional subscription-based model, the cost to the publisher to produce each article is covered by the revenue generated by journal subscriptions. Under OA, all the articles are published under a Creative Commons (CC BY) license; therefore, the authors or funding body will pay a one-time article processing charge (APC) to offset the costs of all of the activities associated with the publication of the article manuscript, including:

- Digital tools used to support the manuscript management and review process
- Typesetting, formatting and layout
- Online hosting
- Submission of the journal's content to numerous abstracts, directories, and indexes

- Third-party software (e.g. plagiarism checks)
- Editorial support which includes manuscript tracking, communications, submission guideline checks, and communications with authors and reviewers
- All promotional support and activities which include metadata distribution, press releases, promotional communications, web content, ads, fliers, brochures, postcards, etc. for the journal and its published contents
- The fact that all published articles will be freely accessible and able to be posted and disseminated widely by the authors
- Professional line-by-line English language copy editing and proofreading*

**This service is only performed on article manuscripts with fully paid (not discounted or waived) APC fees.*

APC Subsidizing and Funding

To assist researchers in covering the costs of the APC in OA publishing, there are various sources of OA funding. Additionally, unlike many other publishers, IGI Global offers flexible subsidies, 100% Open Access APC funding, discounts, and more. Learn More (/publish/contributor-resources/open-access/#oa-journal-publishing)

Open Access Funding Resources

IGI Global recognizes that many researchers may not know where to begin when searching for OA funding opportunities. IGI Global recently launched an Open Access Funding Resources (/open-access-publishing/funding-resources/) page for researchers to browse. This page provides a comprehensive list of OA funding sources available for researchers to secure funds for their various OA publications.

Submit to This Journal

This journal is currently actively seeking new submissions. Interested authors should ensure that their article manuscript adheres to the journal's submission guidelines (/publish/contributor-resources/journal-guidelines-for-submission/?titleid=1093) and utilize the journal article template (https://igiprodst.blob.core.windows.net/public-publish/journal-organization-and-formatting.docx), which include originality of the manuscript, professional English language copy editing, APA formatting tips, and more. To submit an article for consideration, please begin the submission process below.

Submit › (/submission/submit-manuscript/?jid=1093)

มหาวิทยาลัยรังสิต Rangsit University

Contact

PDF

Help

Ghazi I. Alkhatib
Editor-in-Chief
International Journal of Information Technology and Web Engineering (IJITWE)
E-mail: alkhatib@hu.edu.jo (mailto:alkhatib@hu.edu.jo)

Archiving

All of IGI Global's content is archived via the CLOCKSS and LOCKSS initiative. Additionally, all IGI Global published content is available in IGI Global's InfoSci® platform.

International Journal of Information Technology and Web Engineering (IJITWE) 17(1)

Ghazi I. Alkhatib (The Hashemite University, Jordan (retired))

Copyright: © 2022

Volume: 17
Issue: 1
ISSN: 1554-1045EISSN: 1554-1053EISBN13: 9781799894001DOI: 10.4018/IJITWE.20220101

Cite Journal ✓ Favorite ★ Full-Issue Download

Organizations are continuously overwhelmed by a variety of new information technologies; many are Web-based. These new technologies are capitalizing on the widespread use of network and communication technologies for seamless integration of various issues in information and knowledge sharing within and among organizations. This emphasis on integrated approaches is unique to this journal and dictates cross platform and multidisciplinary strategy to research and practice.

Table of Contents

Full text search term(s) Reset

PDF (/gateway/article/full-text-pdf/299022)
HTML (/gateway/article/full-text-html/299022)

Article

Biometric Cloud Services for Web-Based Examinations: An Empirical Approach (/gateway/article/299022) (pages 1-25)

Meennapa Rukhiran (Rajamangala University of Technology Tawan-OK, Thailand.), Sorapak Pukdesree (Rangsit University, Thailand), Paniti Netinant (Rangsit University, Thailand)

Biometric recognition may be used in conjunction with human authentication on a smartphone to improve accuracy, reliability, and simplicity, and to aid in fraud prevention and user authentication. While single biometric...

PDF (/gateway/article/full-text-pdf/288038)
HTML (/gateway/article/full-text-html/288038)

Article

Winning the War on Terror: Using "Top-K" Algorithm and CNN to Assess the Risk of Terrorists (/gateway/article/288038) (pages 1-15)

Yaojie Wang (Engineering University of PAP, China), Xiaolong Cui (Engineering University of PAP, China), Peiyong He (Engineering University of PAP, China)

From the perspective of counter-terrorism strategies, terrorist risk assessment has become an important approach for counter-terrorism early warning research. Combining with the characteristics of known terrorists, a quantitative...

มหาวิทยาลัยรังสิต Rangsit University

PDF (/gateway/article/full-text-pdf/288039)
HTML (/gateway/article/full-text-html/288039)

Article

Extracting Entity Synonymous Relations via Context-Aware Permutation Invariance (/gateway/article/288039) (pages 1-17)

Nan Yan (Anhui Polytechnic University, China), Subin Huang (Anhui Polytechnic University, China), Chao Kong (Anhui Polytechnic University, China)

Discovering entity synonymous relations is an important work for many entity-based applications. Existing entity synonymous relation extraction approaches are mainly based on lexical patterns or distributional corpus-level...

PDF (/gateway/article/full-text-pdf/298654)
HTML (/gateway/article/full-text-html/298654)

Article

Relationship Between Personality Patterns and Harmfulness: Analysis and Prediction Based on Sentence Embedding (/gateway/article/298654) (pages 1-24)

Kazuyuki Matsumoto (Tokushima University, Japan), Ryota Kishima (Tokushima University, Japan), Seiji Tsuchiya (Doshisha University, Japan), Tomoki Hirobayashi (Yamada Denken Co., Ltd., Japan), Minoru Yoshida (Tokushima University, Japan), Kenji Kita (Tokushima University, Japan)

This paper hypothesize that harmful utterances need to be judged in context of whole sentences, and extract features of harmful expressions using a general-purpose language model. Based on the extracted features, we propose a method...

< View All Issues (/gateway/journal/1093)

Request Access

You do not own this content. Please login to recommend this title to your institution's librarian or purchase it from the IGI Global bookstore (/journal/international-journal-information-technology-web/1093).

Username or email:
paniti.n@rsu.ac.th

Password:
••••••••

Log In >

Forgot individual login password? (/gateway/login/reset-password/)

Create individual account (/gateway/login/create-account/)

มหาวิทยาลัยรังสิต Rangsit University

Research Tools
Database Search (/gateway/) | Help (/gateway/help/) | User Guide (/gateway/user-guide/) | Advisory Board (/gateway/advisory-board/)

User Resources
Librarians (/gateway/librarians/) | Researchers (/gateway/researchers/) | Authors (/gateway/authors/)

Librarian Tools
COUNTER Reports (/gateway/librarian-tools/counter-reports/) | Persistent URLs (/gateway/librarian-tools/persistent-urls/) | MARC Records (/gateway/librarian-tools/marc-records/) | Institution Holdings (/gateway/librarian-tools/institution-holdings/) | Institution Settings (/gateway/librarian-tools/institution-settings/)

Librarian Resources
Training (/gateway/librarian-corner/training/) | Title Lists (/gateway/librarian-corner/title-lists/) | Licensing and Consortium Information (/gateway/librarian-corner/licensing-and-consortium-information/) | Promotions (/gateway/librarian-corner/promotions/) | Online Symposium Series (/gateway/librarian-corner/online-symposium-series/)

Policies
Terms and Conditions (/gateway/terms-and-conditions/)

(http://www.facebook.com/pages/IGI-Global/138206739534176?ref=sgm)

(http://twitter.com/igiglobal)
(https://www.linkedin.com/company/igiglobal)

Proud Supporter of WFCF
Learn More
(http://www.world-forgotten-children.org)

(https://publicationethics.org/category/publisher/igi-global)

Copyright © 1988-2022, IGI Global - All Rights Reserved

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Biometric Cloud Services for Web-Based Examinations:
An Empirical Approach

Meennapa Rukhiran, Rajamangala University of Technology Tawan-OK., Thailand.
https://orcid.org/0000-0002-3880-8991

Sorapak Pukdesree, Rangsit University, Thailand

Paniti Netinant, Rangsit University, Thailand*
https://orcid.org/0000-0001-8376-0440

ABSTRACT

Biometric recognition may be used in conjunction with human authentication on a smartphone to improve accuracy, reliability, and simplicity, and to aid in fraud prevention and user authentication. While single biometric authentication addresses environmental degradation and sensor noise limitations, and the single point of failure scenario in biometric systems can result in more robust biometric systems, multimodal biometric authentication can improve the accuracy of identification and recognition. The purpose of this research is to propose a facial and speech authentication system that is cloud-based and supports a web-based examination approach. The system enables students' biometrics to be registered, students to be recognized, and student recognition results to be reported. The confusion matrix is used to compare the results of positive and negative detection in various ways, including accuracy score, precision value, and recall value. Adaptive multimodal biometric authentication should be designed and evaluated for further research using the optimal weights for each biometric.

KEYWORDS

Authentication, Cloud Services, Face Recognition, Multimodal Biometric, Speech Recognition

INTRODUCTION

The mobile revolution has resulted in the development of portable and convenient data manipulation and data transfer devices. Authentication is a well-known method of securing a user's access to services. Unlocking devices, authorizing transactions, and verifying users' signatures are all examples of authentication services (Wojtowicz & Joachimiak, 2016). For both service providers and users, the traditional authentication method prioritizes using a username and password (Czeskis et al., 2012). However, physical characteristics combined with one or more biometrics allow for the precise identification of an individual user (Casanova et al., 2021). Biometric recognition utilizes user

DOI: 10.4018/IJITWE.299022

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

characteristics such as hands, eyes, faces, mouth, fingerprints, and ears to identify users automatically. The unimodal biometric system's limitations include a lack of data, low accuracy, and vulnerability to attack.

Biometric authentication is defined as the process of automatically recognizing physiological characteristics to provide secure identification and verification solutions (Selwal et al., 2016). Five modules comprise the biometric system: 1) a multi-sensor system collects primary biometric data, 2) a preprocessor for the necessary feature extractor methods, 3) templates generate patterns for biometric extracts, 4) decision fusion reconciles disparate patterns, and 5) identifying and authorizing the results by matching the input and enrolled patterns (Yadav et al., 2011). The multimodal biometric system expands the number of biometric inputs from users to more than two, allowing for more reliable authentication. Multiple physical characteristics can be used to authenticate users. Multimodal biometrics integrates and improves user recognition with increased accuracy, security, reliability (Purohit & Ajmera, 2021), and fault tolerance (Khoo et al., 2018), as well as consolidating data. The multimodal biometric system requires multiple parallel systems to detect the same or distinct biometric features at various layers (Smith & Brooks, 2013). Human physiological biometrics have been studied practically in a variety of areas using multimodal biometric systems, including parallel feature fusion of periocular biometrics and touch (Casanova et al., 2021), unequal feature portions of faces and fingerprints (Yang et al., 2019), and novel techniques and algorithms for palm, fingerprint, and ear recognition (Purohit & Ajmera, 2021).

Pukdesree and Netinant (2016) proposed a biometric authentication conceptual framework and developed a cloud-based biometric authentication service; thus, the entire process of data input, processing, and output can express the multimodal biometric authentication layering architecture. The framework provided a layered design for the client, application, and cloud database. The actual authentication system is still being developed and evaluated. While biometric authentication has evolved to incorporate multiple physiological biometrics with the possibility of a single point of failure, the multimodal biometric authentication system built on this framework can be enhanced by adding a security access system to protect fraud detection services.

This paper proposes a design and implementation of multimodal biometric cloud services for authentication of web-based examinations to bridge the gap between face and voice recognition multimodal biometric applications. During the coronavirus (COVID-19) pandemic, students could verify their identities and access the exam scheduling system. The system is unburdened within acceptable responsiveness scores to exam schedules, and the system was replaced with more flexible and superior securities. A confusion matrix is used to compare nonmembers and members who have registered for the examination system. The system outcomes from this biometric authentication research can be used to define system requirements and development scopes, as well as improve the reliability and accuracy of practical web-based applications.

RELATED WORK

Errattahia et al. (2018) reviewed the methods for detecting and correcting automatic speech recognition (ASR) errors. The researchers concentrated on ASR error correction, which resulted in increased efficiency, usability, and robustness. Bah and Ming (2020) proposed a novel method for improving the precision of face recognition systems by combining the Local Binary Pattern algorithm with various image processing techniques, such as contrast, brightness, or histogram equalization. These techniques can also help improve the accuracy, reliability, and robustness of the face recognition system. According to Shakil et al. (2021), patient information is extremely valuable and should be stored, accessed, and managed with the utmost care. The researchers proposed behavioral biometric authentication via a cloud-based system based on signatures. Mason et al. (2020) reported that biometric technology adoption in the healthcare industry is accelerating. They proposed an approach

for digesting the individual patient by combining periocular biometrics and the patient index in healthcare information systems.

A single-modal biometric system has limitations, and each method has a rating based on the seven values proposed by Jain and Ross. Each biometric modality also has limitations due to environmental degradation, sensor noise, and so on. Multimodal biometrics combine multiple biometric modalities, addressing the single point of failure scenario in biometric systems and resulting in more robust biometric systems. Their multimodal biometric was a combination of speech and face. Naidu and Babu (2018) presented a multimodal biometric recognition system that utilizes face, finger, and voice recognition biometrics. When compared to existing single biometric identification systems, the system provided increased security. The results incorporated these characteristics via score-level fusion. Choudhury et al. (2021) proposed an adaptive rank-level biometric merging framework. To ensure optimal performance, the rank-level merging was implemented using the ant colony optimization technique. The article utilized the multimodal biometric by extracting three fingernail plates from the index, middle, and ring fingers. AlexNet, ResNet-18, and DenseNet-201 algorithms are used to extract these three nail plates.

Fei et al. (2021) proposed using the joint multi-instance hand-based biometric feature for biometric recognition. The researchers used preliminary aspect data derived from multiple biometric image instances. The extracted features of multi-instance biometric characteristics and the collaborative demonstrations of multi-instance biometric characteristics are thus combined to produce the final ordinary. Sarier (2021) proposed multimodal biometric authentication for mobile edge computing (MBA-MEC), a multimodal biometric authentication technique based on mobile technology. MBA-MEC is a new multimodal system that defends against invaders by utilizing the secure protocol of privacy-preserving biometric authentication (PPBA). MBA-MEC matching is carried out exhaustively in an encrypted format, and then the finalized merged matching score is hidden from other computers. Kumari and Thangaraj (2020) proposed a cloud-based system framework for rapid feature selection in multimodal biometrics. These biometric compounds of facial and fingerprint recognition are multimodal in nature. The proposed technique for feature selection uses ant colony optimization. Particle swarm optimization is used for feature extraction and classification processes.

Chang et al. (2021) proposed a biocryptosystem level fusion framework known as BIOFUSE, a multimodal biometric fusion framework that combines fuzzy commitment and fuzzy vault. These techniques were used to create an encryption pattern that preserves the format. This framework makes it extremely difficult for an attacker to gain unauthorized access to the system without simulating all of the genuine user's biometric inputs. Vijay and Indumathi (2021) proposed a multimodal biometric consisting of three traits: iris, ear, and finger vein, the features of which are extracted using the BiComp masking method. The recognition score is then calculated for each of the three traits using a multi-support vector neural network (multi-SVNN) classifier.

A single modal biometric system can be improved by applying other methodologies. Kausar (2021) mentioned biometrics in healthcare to protect patients' private data. This biometric deploys an iris-based cancelable crypto system on a smart card. The patient's data is secured by deploying symmetric key cryptography, with healthcare data stored in an encrypted format on the smart card. Piciucco et al. (2021) proposed integrating biometric recognition and wearable devices to prevent unauthorized usage of these devices. This methodology uses the fusion of electrodermal activity (EDA) and blood volume pulse (BVP) spectrograms into MobileNet v2. The study also shows that biometric recognition can be integrated with wearable devices for identifying an authorized user.

Bisogni et al. (2021) proposed a novel secured biometric system for authorizing and signing blockchain transactions. This methodology uses face recognition as a biometric, encoded using a convolutional neural network, then the encoding is fused with the Rivest-Shamir-Adleman (RSA) key. The results show that the combined key can ensure authorizing in blockchain transactions with preserving the user's privacy. Brundhaelci et al. (2019) proposed face recognition on closed-circuit television (CCTV), also known as surveillance cameras, to detect and quickly respond to criminal

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

recognition and person tracking to reduce the crime rate. The project uses deep learning neural networks to detect and recognize criminals and person tracking. Cherifi et al. (2021) proposed a continuous and real-time authentication system by capturing the user's activation using the sensors of the smartphones (e.g., gyroscope or accelerometer) to gather the positions or the coordinates. The overall processes of continuous and real-time authentication provide the real-time user's activation, feature extraction, train the HMM model, and affirm the user's entity.

Falmari and Brindha (2021) proposed a new encrypted biometric-based approach that provides more security for the biometric authentication system. The biometric information may be stored on a remote storage server on the network. Therefore, biometric information may be stolen during send or pass on the network. This methodology encrypts the biometric information, such as images of the iris, face, or fingerprint, using a secure 256-bit hash algorithm before sending the biometric information onto the network. The encryption keys are generated from the biometric images. Consequently, it is difficult to get the encrypted key without the original biometric image.

Yang et al. (2019) proposed a feature-adaptive random projection-based approach. The projection is the matrix that is derived from the local feature gathering with the basic matrix. This projection matrix will be left after use to prevent the reuse of this projection matrix, making it more difficult to get into information stored in the projection matrix.

Saeed (2021) proposed a new approach that combines soft biometric features with conventional facial features. The soft biometric features are used to model the micro-expressions from the image. On the other hand, conventional facial features were used to model facial conformation. This approach can improve the facial recognition system by approximately five percent.

Stylios et al. (2021) proposed a continuous behavioral biometric authentication technique using mobile phones. This paper provides a diagnosis of the gathering and feature extraction methodology. This paper also shows the weakness of machine learning models in preventing defiant assaults and the related preventive measures. Behera et al. (2021) focus on the new concept of person re-identiðcation on the internet of biometrics things (IoBT), a biometric authentication system on cloud computing. The proposed system tracks the person's movement on multiple and different surveillance cameras, which can help to reduce the complexity of re-identiðcation on multiple and different surveillance cameras. In smart cities scenarios, the IoBT is more widely used with intelligent surveillance cameras, which produce more network traffic.

Ajish and AnilKumar (2021) proposed an election voting system using a biometric authentication that operated on a secured mobile application for voters. The system provides secure information while transporting data on a mobile network by encrypting the voter's image. The mobile application processes the encrypted image by extracting features and storing it as a biometric template, then sends the template to the server to process the next step. The encryption process uses a wavelet-based based on advanced encryption standard (AES) algorithm, which provides better performance than the other two algorithms.

Lee et al. (2021) presented one of the most intriguing biometric authentication systems ever proposed. The study introduced Biometric Database Authentication System (BDAS), a novel biometric authentication system based on blockchain technology. BDAS offers decentralized and distributed gimmicks such as blockchain-based biometric authentication and auditing. By comparing the BDAS to some other methodologies, the researchers demonstrate that it can provide a reliable and secure biometric mechanism authentication.

Kumar et al. (2021) proposed encrypting biometric templates in two stages. To begin, the group representation of biometric templates was decomposed using two-dimensional discrete wavelets. Finally, substitution and permutation were performed using the three-dimensional Lorenz-chaotic system. Each level of decomposition consumed the encryption process, while the decryption process occurred in reverse order. The experimental results indicate that the proposed methodology can enhance security while maintaining robustness against attackers.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Jia et al. (2021) concentrated on dorsal hand vein biometric authentication, which was referred to as an urgent need for biometric technology authentication. They comprehensively survey dorsal hand veins (DHV) biometrics. The article discusses the results of the DHV biometric processes, including data collection, database structure, preprocessing, feature extraction, matching, score fusions, and the future of DHV biometrics technology.

Lee and Jeong (2021) set out to create one of the most intriguing biometric authentication systems possible. The study introduces BDAS, a novel biometric authentication system based on blockchain technology. BDAS offers decentralized and distributed gimmicks such as blockchain-based biometric authentication and auditing. By comparing the BDAS to some other methodologies, the researchers demonstrate that it can provide a reliable and secure biometric mechanism authentication.

Srivastva et al. (2021) developed a biometric recognition system based on electrocardiogram data that represents the electrical activity of the heart via electrode devices placed on the individual's skin. The researchers created PlexNet, a stacking model, by fusing the results of four fine-tuned models. PlexNet is evaluated on the basis of two publicly available datasets. According to the experimental results, the proposed biometric recognition technique has an accuracy score of up to 99.66 percent. Additionally, this methodology is robust.

Cui et al. (2021) focused on the electrocardiogram as a method for human biometric recognition, noting that this method is difficult to counterfeit. The researchers collected electrocardiogram (ECG) data during both exercise and rest. The evaluations were performed on the ECG dataset using a variety of algorithms. They conclude that the evaluation results are satisfactory for the specified circumstances, even if they are not as robust as other experimental results obtained in a different environment.

Marquez et al. (2021) focused on the use of behavioral biometrics and infrared thermography to monitor dairy cow estrus in farms. This research develops an estrus alert system that can assist farmers in detecting their cows' estrus. The research issue is that low estrus rates are associated with prolonged calving duration, low economic profit, and cow longevity. The skin temperature of dairy cows is measured using infrared thermography, and the indicator of ovulation is determined by the disappearance of the dominant follicle. Liu et al. (2021) primarily concerned themselves with biometric authentication for wearable devices.

At the moment, wearable technology is more prevalent in people's daily lives. As a result, the researchers examine current state-of-the-art user authentication for wearable devices. According to the researchers, biometrics are classified into two categories based on their frequency of use: physiological biometrics and behavioral biometrics. The researchers' objective is to establish a framework for future research in this field. Kute et al. (2021) advocated for the use of fingerprints to identify a person's facial image, particularly in criminal investigations. In forensic investigations, both face recognition and fingerprint recognition are frequently used. This methodology learns and trains using Bregman divergence regularization from fingerprint biometrics and then transfers the learning to face biometrics. The results indicate that transferring can enhance biometric identification performance and assist in identifying the correct suspect.

PROPOSED DEVELOPMENT SYSTEM

Figure 1 details the extended framework for parallel biometric authentication for a cloud-based biometric service. The system is divided into three tiers: end-user, application, and database. A system's end-user layer is the layer with which the user interacts or utilizes. Initially, the research concentrated solely on smartphone devices, as they are a highly specialized platform. As a result, the framework remains cross-platform compatible with smartphones and other devices. The application layer consists of the system application, which includes face and speech recognition components. A user may choose between biometric authentication and password authentication. Additionally, the system can authorize user recognition based on the average score of multiple biometric authentication methods. If any recognition score fails, the user can still immediately log in to the system using a

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

username and password. Thus, the database layer is responsible for database administration functions such as data inserting, updating, accessing, and deletion.

Figure 1. Extended Framework of biometric authentication cloud service

While Pukdesree and Netinant's (2016) conceptual framework outlines the design of a single security access system for detecting fraud services, the framework does not yet include a cloud-based multimodal biometric implementation. Their research extends the framework for representing multimodal biometric authentication through the use of parallel recognition layering designs to facilitate the implementation of biometric authentication systems on web-based services. The benefits of a multimodal biometric authentication system are highlighted because it enables face and speech authentication via web-based detection during an examination. The client layer of the research includes experimental testing on the end-user device using an iPhone 11 running iOS version 15 to ensure that the proposed system device collects student information such as speech, face, password, and other information during registration and recognition. A Docker container deploys the application layer on a virtual machine and a cloud virtual private server. The system is built on a web-based platform compatible with cross-platform software. Additionally, the database layer is stored and managed in the cloud via a virtual private server. Due to the development of multimodal biometric recognition for student authentication services, the authentication system processes are divided into three phases.

Registration Phase

This process collects information from newly registered members. The information includes both essential and biometric data. Face biometric registration consists of three steps: face detection, face

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

preprocessing, and face extraction. Face detection in this study is accomplished using a Local Binary Patterns (LBP) technique. The LBP-based approach collates the pixel intensity of edges, corners, and flat regions using the histogram method. The LBP-based technique can be used to increase the rate of face detection while decreasing computing time. Additionally, face detection is unreliable in low light conditions. As a result, the face images are required to perform histogram equalization, which improves the contrast and brightness of the images. Equalization of histograms is also a critical step in the facial recognition process. Face preprocessing entails three steps: 1) eye search regions that emphasize eye alignment, which involves scaling, rotating, and translating the images; and 2) removing the forehead, chin, ears, and background from the images. 2) equalization of the histogram, which evenly distributes the brightness and contrast on the left and right sides of the face. 3) The elliptical mask will eliminate some of the remaining hairs and background from the facial image, leaving only the facial image. Speech biometric registration consists of three steps: Mel Frequency Cepstral Coefficients (MFCC) extraction, Delta calculation, and a combination of MFCC extraction and Delta calculation. For audio, the MFCC extraction algorithm generates twenty-dimensional feature vectors. For audio, the delta calculation will also use twenty-dimensional feature vectors. Thus, when MFCC extraction and Delta calculation are combined, forty-dimensional feature vectors for audio are created. Finally, biometric information will be extracted as biometric templates from the critical features. A cloud database will be used to store the templates. The registration process is depicted in Figure 2.

Training Phase

After obtaining the desired biometric information for each individual, this data must be trained using a machine-learning algorithm for facial and speech templates. Training data use eigenfaces for facial training because it is a straightforward method. Nonetheless, it is capable of performing as well as more sophisticated face recognition algorithms. The proposed system employs the Gaussian Mixture algorithm for speech training. The training phase's output will be machine learning models. Models can be derived from the machine learning algorithms used in this experiment using training data. The training data set is the collection of data used to educate the model. The training data will be labeled with the labels used for recognitions or decisions in this experiment. The training process is depicted in Figure 3.

Recognition Phase

The recognition process can identify or verify an individual by comparing their biometric data to facial and speech features stored in a database. The design and development employ principal component analysis in this study, which employs eigenfaces for facial recognition. The eigenvectors are derived from the covariance matrix of the probability distribution for facial images in their high-dimensional vector space. For speech recognition, this study employs a Gaussian mixture model probability distribution. The outcome of these processes is the matching score for each biometric evaluation. The scores are combined using adaptive authentication's equality weight. The fused score will indicate whether or not the individual is a member of a system. The recognition process is depicted in Figure 4.

RESEARCH METHODOLOGY

Type of Research

This is experimental research that employs a systematic approach to studying, researching, and innovating. The purpose of this research is to create a web-based examination for undergraduate students that makes use of cloud-based biometric services. Due to the disruption in information technology today, students can learn from anywhere or anytime, as advanced network technology, particularly internet technology, has emerged. However, there would be a process in place to authenticate students taking online examinations. The purpose of this research is to use biometric

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 2. Face and speech biometric registration processes

cloud services to enable multimodal biometric authentication for a web-based exam for undergraduate students.

Research Sample

The population for this study is students enrolled in second semester 2020 courses in the department of computer science and technology at Bangkok University's school of information technology and innovation. The population is approximately 400 students. Purposive sampling was used in this study to select students from the computer organization course, which is appropriate for the current situation in our context. This course has approximately eighty students enrolled. The sampling is stratified into two categories: members and nonmembers.

Research Instrument and Procedure

The instrument of the study is a web application written in Python and using the Django framework. Sqlite3 is the database management system used by this web application. This web application can be accessed and used via an iPhone, an Android device, or a desktop computer equipped with a web browser. Researchers schedule appointments with our students before they take the final examinations via online examinations.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 3. Face and speech biometric training process

Data Collection

This research collects data through experimental testing. The sampling will enable individuals to use the multimodal biometric authentication system on their devices. The sample will be provided with the necessary information to access the system on the specified date and time.

Data Analysis

The collected data is an enumeration count of multimodal biometric authentication matches and mismatches. Qualitative data are gathered. As a result, the Chi-square test was used to analyze the data in this study, as it corresponds to the collected data. The Chi-square test is an appropriate method for determining the statistical relationship between two independent sampling groups.

มหาวิทยาลัยรังสิต Rangsit University

SYSTEM IMPLEMENTATION

System Design

The system was designed by researchers using a variety of design tools. This article, on the other hand, discusses design tools such as use case diagrams, Entity Relation (ER) diagrams, data dictionaries, and flow diagrams. According to the use case diagram depicted in Figure 5, the system involves three

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 4. Face and speech biometric recognition processes

actors: students, instructors, and administrators. Students can enroll in courses, modify previously registered courses, view previously enrolled courses, display examinations, login to tests, and enter examinations through this system. Instructors can perform various functions in this system, including displaying courses, displaying examinations, logging into tests, and entering examinations. Finally, administrators can perform a variety of functions in this system, including displaying courses, displaying examinations, logging into examinations, creating and modifying courses, assigning instructors, generating examinations, and modifying tests.

As illustrated in Figure 6, the system's ER diagram contains seven entities: students, instructors, administrators, courses students, courses, examinations, and examinations students. Each entity is connected to other entities in some way. Students can enroll in the same courses that are offered during the indifference semester and academic years. As a result, a many-to-many relationship exists.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Students can sit for the same examination for courses that span multiple semesters and academic years. As a result, a many-to-many relationship exists. As a result, these entities will be normalized to at least the third standard form. Finally, the normalized form will be converted to a data dictionary, used to create database tables.

Figure 5. Use case diagram of multimodal biometric authentication for web-based examination

Consider the flow diagram of the student's activities depicted in Figure 7. To begin, students can log in to the examination system using their devices such as iOS smartphones, Android smartphones, personnel computers, or notebook computers. Students will be required to enter their facial biometrics into the system via the built-in or web camera. The facial biometrics will be stored on the server in a temporary folder. Then, using a microphone, students will enter their speech biometrics into the system. The speech biometric will be stored on the server in a temporary folder. When students click the login button, the system extracts facial biometric features and compares them to those extracted from previously enrolled facial extractions. The system will assign a personal score to the result of the comparison based on the comparison's similarity. Following that, when students click the login button, the system extracts biometric speech features and compares them to the extracted features of

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 6. The entity-relationship diagram of multimodal biometric authentication for examination systems

Figure 7. Flow Diagram of multimodal biometric authentication for web-based examination

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

previously enrolled speech extractions. The system will provide a confidential score for the comparing result that reflects the similarity of the comparing. The system will then compute the fusion score by combining the confidential facial biometric and speech biometric scores. Finally, the system will decide on multimodal biometric authentication using the fusion score. If the student's fusion score falls within the specified range of values, the system will admit the student to the online examination. On the other hand, if the fusion score does not fall within the scope of acceptable values, the system will refuse to admit the student to the online examination. The student also has the option of using their password in the traditional manner.

Web-based Implementation

This multimodal biometric authentication system employs speech and face recognition and is deployed on a Docker container running on a virtual machine on a cloud virtual private server. The system was developed using web technology that is cross-platform compatible. Figure 8 illustrates the system's home page, from which students can register as a new user or log in as an existing user. A student must register as a new user by entering their basic information, including one speech recording and twenty face recordings, as illustrated in Figures 9 and 10. All data will be securely stored in a cloud-based database.

Additionally, the system will extract speech features and store them in a folder designated for the training process. The system will extract facial features and perform pre-processing before storing them in a specified folder for use during the training process. The paper borrows the specifics of this process as described in (Pukdesree & Netinant, 2018). Finally, the system administrator will be responsible for batch processing the training process.

Figure 8. Home pages of authentication notification and services

To log into the system during the recognition phase, a student will enter their speech recording and take a facial picture, as illustrated in Figure 11. If the multi-modal biometric result score exceeds the threshold, the system will permit the student to access online testing services, as illustrated in Figure 12. On the other hand, if the student's multi-modal biometric result falls below the threshold, the system will deny online testing services. However, if a device fails or the environment becomes uncertain, a student can enter a password to access the system. Additionally, adaptive student authentication systems, compared to Pukdesree and Netinant (2016), can support parallel recognition. The extended framework has the potential to increase security and efficiency at a low cost significantly. Password authentication is used when multimodal biometrics are deemed too complex or do not authenticate students during accurate online testing.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 9. Registration process

Figure 10. Facial enrollment

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 11. Testing processes

Figure 12. Authentication accurate results

มหาวิทยาลัยรังสิต Rangsit University

The online testing system supports three user roles: student, instructor, and administrator. The administrator role has the ability to manage student and instructor data. As illustrated in Figures 13 and 14, the instructor can manage courses exams and generate reports. The student role is entirely responsible for managing their information and taking tests.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 13. Course management

Figure 14. Examination management

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

EVALUATION METHODOLOGY

The confusion matrix is a table that is used to compare the model's predictions to the actual values. This matrix is used in predictive analytics, a branch of statistics that uses data to extract information and forecast trends and behavior patterns. Predictive analytics is a type of statistics. Predictive analytics is comprised of algorithms for deep learning, data modeling, and data mining. The framework was evaluated using the following metrics (Tharwat, 2018; Chicco & Jurman, 2020; Piryonesi & El-Diraby, 2020; Chicco et al., 2021).

1. The accuracy score is a statistical measure calculated as the ratio of genuine prediction results to the total number of tests. The following Equation (1) is used to calculate the accuracy score.

$$\text{Accuracy} = \frac{\sum\left(\text{True}_{\text{positive}}\right) + \sum\left(\text{True}_{\text{negative}}\right)}{\sum\left(\text{Total_population}\right)} \tag{1}$$

2. Precision is a term that refers to the accuracy with which predictions are made. Precision is a two-sided coin: it can be viewed positively or negatively. The precision positive value indicates the precision with which the member aspect prediction was made. The precision minus sign indicates the likelihood of correctly predicting the nonmember aspect. The precision score formula is expressed in Equations (2) and (3).

$$\text{Precision_Positive} = \frac{\left(True_{\text{positive}}\right)}{\left(True_{\text{positive}} + False_{\text{positive}}\right)} \tag{2}$$

$$\text{Precision_Negative} = \frac{\left(\text{True}_{\text{negative}}\right)}{\left(\text{True}_{\text{negative}} + \text{False}_{\text{negative}}\right)} \tag{3}$$

3. The recall value indicates the prediction results' accuracy compared to the actual values, which can be expressed as the percentage of correcting predictions made by members with recall positive and nonmembers with recall negative. Thus, the formula can represent the data in Equations (4) and (5).

$$\text{Recall_Positive} = \frac{\left(\text{True}_{\text{positive}}\right)}{\left(\text{True}_{\text{positive}} + \text{False}_{\text{negative}}\right)} \tag{4}$$

$$\text{Recall_Negative} = \frac{\left(\text{True}_{\text{negative}}\right)}{\left(\text{True}_{\text{negative}} + \text{False}_{\text{positive}}\right)} \tag{5}$$

4. By estimating the average precision and recall values, the F1 score quantifies performance. Additionally, the F1 score is referred to as the harmonic mean. The F1 score has two possible

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

values: negative and positive. Assume that the F1 score is high, indicating that the model performs satisfactorily. Equation (6) can be used to express the F1 score mathematically.

$$\text{F1 Score} = \frac{2PR}{(P+R)} \tag{6}$$

EXPERIMENTAL RESULTS

Around one hundred students participate in this study, registering their information into the system, including biometrics such as speech and facial recognition. Each student will enter basic information, one speech proposition, and twenty faces during the registration process. The data will be stored on a virtual private server hosted in the cloud. Eighty times, the system's authentication was evaluated by allowing registered and unregistered members to authenticate themselves to access online testing services. Additionally, the system provides a password for authentication if multimodal biometrics are deemed too complicated or fail to authenticate students during accurate online testing.

This study evaluates a multimodal biometric authentication method that combines face and speech recognition for cloud service access. The confusion matrix's results are summarized in Table 1.

The True Positive value is 49, indicating that the prediction results are valid for system member authentication. 2) The True Negative value is 8, indicating the probability of correctly predicting a non-member of the system. 3) The False Positive value is 9, indicating that the authentication of a non-member of the system failed due to a false prediction. 4) False Negative value is 14, indicating a prediction by an incorrect system member. The confusion matrix is depicted in Figure 15.

Table 1. Confusion matrix table of multimodal biometric using face and speech recognition

	N=80	Nonmember /Negative (0)	Member /Positive (1)
Actual	Nonmember /Negative (0)	8	9
	Member /Positive (1)	12	51

The confusion matrix results can explain in several ways, such as accuracy score, precision values, recall values, and F1 scores, as shown in Table 2 and Figure 16. The accuracy score in this experimental evaluation is 0.712500 or 71.25 percent, representing the ratio of valid prediction results to total testing numbers. This accuracy rating is on the moderate side. One factor affecting the system's accuracy is that the environment enters biometric data, such as when speech or face information is entered, as mentioned in several research papers.

Precision refers to the accuracy with which results are predicted. Precision can be viewed in two ways: positively or negatively. Precision positive refers to the accuracy with which the member aspect is expected. The precision negative represents the probability of correctly predicting the nonmember aspect. In this experimental evaluation, the precision positive value is 0.844828, indicating that the actual member's correct result prediction is 84.4828 percent. The precision negative value is 0.363636, indicating that the nonmember's accurate result prediction is 36.3636 percent.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Figure 15. Graph of confusion matrix

Figure 16. Graph evaluation scores

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Table 2. Evaluation scores of multimodal biometrics using face and speech recognition

Accuracy Score	0.712500			
	Precision	Recall	F1 Score	Support
Nonmember	0.363636	0.470588	0.410256	17
Member	0.844828	0.777778	0.809917	63

The recall value indicates how accurately the results were predicted in comparison to the actual values, taking into account the percentages of correcting prediction and actual members, as well as the percentages of correcting prediction and nonmembers. The recall positive value is 0.777778, which represents the actual member's percentage of correct predictions. In this experiment, there are 63 actual members and 49 correct predictions of the actual member. As a result, the recall positive will be 49 out of 63, or 77.7778 percent accurate prediction. The recall negative value is 0.470588, which indicates the nonmember's percentage of correct predictions. The nonmembers in this experiment have some 17, while the prediction has eight accurate predictions of the nonmember's faces. As a result, the recall negative will be eight out of seventeen, or 47.0588 percent correct.

The F1 score represents performance by averaging the precision and recall values. The F1 score may also be referred to as the harmonic mean if it contains high values, indicating the model's superior performance. The positive value for the F1 score is 0.809917, or 80.9917 percent. The negative value of the F1 score is 0.410256 or 41.0256 percent.

Additionally, the results from the confusion matrix table using Pearson's Chi-square statistic to determine the research hypothesis's validity as illustrated in Table 3. The Chi-square statistic can be used with either quality or classification variables. Variables can be classified into k groups based on their value. Then, the frequency of each group could be specified. Chi-square is a nonparametric statistic. Independent of two variables testing can be used to evaluate research hypotheses involving two group variables. The test can be used to determine the independence of two populations' properties. If the observed and expected frequencies are almost identical, the observed frequency will be compared to the expected frequency. If the observed frequency is different from the observed frequency, it can be concluded that these two frequencies are independent. If the observed frequency is different from the observed frequency, it can be concluded that these two frequencies are dependent.

Table 3. Confusion matrix table and Pearson's Chi-square statistic

	N=80	Nonmember /Negative (0)	Member /Positive (1)	Total
Actual	Nonmember /Negative (0)	8 (4.25)	9 (12.75)	17
	Member /Positive (1)	12 (15.75)	51 (47.25)	63
	Total	20	60	80

มหาวิทยาลัยรังสิต Rangsit University

Step 1: Identifying the statistical hypotheses H0 and H1:

Hypothesis Zero (H0): The proposed multimodal authentication does not rely on the user's authentication for an undergraduate web-based examination.

Hypothesis One (H1): The proposed multimodal authentication is predicated on the user's authentication for an online examination for undergraduate students.

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Step 2: Establishing that the significance level is equal to 0.05.

Step 3: Statistic calculation Chi-square analysis

The Chi-square test value for this scenario is 3.841, which can be found in the Chi-square test table. In this experiment, the Chi-square test value can be calculated using the Chi-square test formula, which equals 5.602241. Since the degree of freedom is equal to one, the Chi-square test value must be optimized using Yate's continuity correction. Then the Chi-square value is equal to 4.465842. The Chi-square test formula is denoted by Equation (7).

$$\text{Chi-square test} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{\left(\left|Oij-Eij\right|-0.5\right)^2}{Eij} \tag{7}$$

Step 4: Establish a critical region

The Chi-square test value can obtain from the predefined table with a significance level of 0.05 and *df* equal to 1. From the predefined table, the Chi-square test result is 3.841. The value of 4.465842 is the calculated Chi-square test value. As a result, the area of the experiment's critical region is more significant than 3.841. Additionally, the probability value (*p*-value) is equal to 0.03458.

Moreover, the calculated Chi-square test value is 4.465842, which is more significant than the Chi-square test value of 3.841 for the predefined table. As a result, H0 is rejected at the 0.05 level of significance. Additionally, one can deduce the *p*-value. The *p*-value is 0.03458, which is less than the 0.05 level of significance. The Chi-square test computed falls within the bounds of the rejected hypothesis H0. The findings suggest that either the research hypothesis is correct or that the proposed multimodal authentication is conditional on the user authenticating for a web-based examination for undergraduate students. Figure 17 illustrates the critical region of the Chi-square test.

Figure 17. Critical region of Chi-square test

มหาวิทยาลัยรังสิต Rangsit University

International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

CONCLUSION

This paper aims to propose a framework for multimodal biometric authentication for student examinations that utilize cloud computing services and conduct both development and experimental research on a smartphone. The framework aims to enhance the security and robustness of biometric authentication while also making it easier to deploy in cloud computing environments. This system was developed using web technology to enable students to register, authenticate, and take online exams using their biometrics. As a result, the web-based system is compatible with smartphones and platforms, enhancing facial image and speech data compression capabilities. The research outcome is devoted to evaluating multimodal biometric authentication services, particularly face and speech recognition. The confusion matrix compares the model's predictions to observed recognition values, including an accuracy score of 71.25 percent, a precision positive value of 84.48 percent, a recall value of 77.78 percent, and an F1 score of 77.78 percent (80.99 percent). As a result, the overall scores from the experimental evaluation can be used in practice. Additionally, practical evaluation is conducted through experimental testing. During Thailand's coronavirus pandemic in 2020, students who took online examinations could automatically authenticate themselves using the proposed multimodal biometric authentication system. The optimal detection and recognition parameters for the multimodal biometric authentication system can be adjusted and evaluated for future research. The adaptive multimodal biometric authentication technique could be implemented, and the adaptation weight associated with each biometric recognition could be determined. Furthermore, the system can increase security using encrypted data transmitted across a network using a secure socket layer, preventing eavesdropping and tampering. The designs can be configured to utilize various encryption techniques for additional investigation, including public-key cryptosystems and symmetric keys.

มหาวิทยาลัยรังสิต Rangsit University

REFERENCES

Ajish, S. (2021). Secure mobile internet voting system using biometric authentication and wavelet based AES. *Journal of Information Security and Applications*, *61*, 102908. doi:10.1016/j.jisa.2021.102908

Bah, S. M., & Ming, F. (2020). An improved face recognition algorithm and its application in attendance management system. *Array*, *5*, 100014. doi:10.1016/j.array.2019.100014

Behera, N. K. S., Behera, T. K., Nappi, M., Bakshi, S., & Saa, P. K. (2021). Futuristic person re-identification over internet of biometrics things (IoBT): Technical potential versus practical reality. *Pattern Recognition Letters*, *151*, 163–171. doi:10.1016/j.patrec.2021.08.007

Bisogni, C., Iovane, G., Landi, R. E., & Nappi, M. (2021). ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions. *Journal of Information Security and Applications*, *59*, 102814. doi:10.1016/j.jisa.2021.102814

Brundhaelci, J., Punith, R., Gowda, S. C., Shivaprasad, B. M., & Buvaneshwaran, V. S. (2019). Criminal recognition and tracking system. *International Research Journal of Computer Science*, *6*(6), 118–125. doi:10.26562/IRJCS.2019.JNCS10095

Casanova, A., Cascone, L., Castglione, A., Meng, W., & Pero, C. (2021). User recognition based on periocular biometrics and touch dynamics. *Pattern Recognition Letters*, *148*, 114–120. doi:10.1016/j.patrec.2021.05.006

Chang, D., Garg, S., Ghosh, M., & Hasan, M. (2021). BIOFUSE: A framework for multi-biometric fusion on biocrypto system level. *Information Sciences*, *546*, 481–511. doi:10.1016/j.ins.2020.08.065

Cherifi, F., Omar, M., & Amroun, K. (2021). An efficient biometric-based continuous authentication scheme with HMM prehensile movements modeling. *Journal of Information Security and Applications*, *57*, 102739. doi:10.1016/j.jisa.2020.102739

Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, *21*(6), 6. Advance online publication. doi:10.1186/s12864-019-6413-7 PMID:31898477

Chicco, D., Toetsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining*, *14*(13), 13. Advance online publication. doi:10.1186/s13040-021-00244-z PMID:33541410

Choudhury, S. H., Kumar, A., & Laskar, S. H. (2021). adaptive management of multimodal biometrics-A deep learning. *Applied Soft Computing*, *106*, 107344. doi:10.1016/j.asoc.2021.107344

Cui, W., Wang, Z., & Li, Y. (2021). ECG-Based biometric recognition under exercise and rest situations. *Biomedical Engineering Advances*, *2*, 100008. doi:10.1016/j.bea.2021.100008

Czeskis, A., Dietz, M., Kohno, T., Wallach, D., & Balfanz, D. (2012). Strengthening user authentication through opportunistic cryptographic identity assertions. In *Proceedings of the 2012 ACM conference on Computer and communications security (CCS'12)*. ACM. doi:10.1145/2382196.2382240

Errattahi, S., Hannania, A. E., & Ouahmane, H. (2018). automatic speech recognition errors detection and correction: A review. *Procedia Computer Science*, *128*, 32–37. doi:10.1016/j.procs.2018.03.005

Falmari, V. R., & Brindha, M. (2021). Privacy preserving biometric authentication using chaos on remote untrusted server. *Measurement*, *177*, 109257. Advance online publication. doi:10.1016/j.measurement.2021.109257

Fei, L., Zhang, B., Tian, C., Teng, S., & Wen, J. (2021). Jointly learning multi-instance hand-based biometric descriptor. *Information Sciences*, *562*, 1–12. doi:10.1016/j.ins.2021.01.086

Jia, W., Xia, W., Zhang, B., Zhao, Y., Fei, L., Kang, W., Huang, D., & Guo, G. (2021). A survey on dorsal hand vein biometrics. *Pattern Recognition*, *120*, 108122. doi:10.1016/j.patcog.2021.108122

Kausar, F. (2021). Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal*, *22*(4), 447–453. doi:10.1016/j.eij.2021.01.004

Khoo, Y., Goi, B., Chat, T., Lai, Y., & Jin, Z. (2018). Multimodal biometrics system using feature-level fusion of iris and fingerprint. In *Proceedings of the 2nd International Conference on Advances in Image Processing (ICAIP'18)*. ACM. doi:10.1145/3239576.3239599

Kumar, D., Joshi, A. B., & Singh, S. (2021). A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system. *Results in Optics*, *5*, 100146. doi:10.1016/j.rio.2021.100146

Kumari, P., & Thangaraj, P. (2020). A fast feature selection technique in multi modal biometrics using cloud framework. *Microprocessors and Microsystems*, *79*, 103277. doi:10.1016/j.micpro.2020.103277

Kute, R., Vyas, V., & Anuse, A. (2021). (in press). Transfer learning for face recognition using fingerprint biometrics. *Journal of King Saud University •. Engineering and Science*. Advance online publication. doi:10.1016/j.jksues.2021.07.011

Lee, M. J., Teoh, A. B. J., Uhl, A., Liang, S., & Jina, Z. (2021). A tokenless cancellable scheme for multimodal biometric systems. *Computers & Security*, *108*, 102350. doi:10.1016/j.cose.2021.102350

Lee, Y. K., & Jeong, J. (2021). Securing biometric authentication system using blockchain. *ICT Express*, *7*(3), 322–326. doi:10.1016/j.icte.2021.08.003

Liu, S., Shao, W., Li, T., Xu, W., & Song, L. (2021). Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, *7*, 103120. doi:10.1016/j.dsp.2021.103120

Marquez, H. J. P., Ambrose, D. J., Schaefera, A. L., Cook, N. J., & Bench, C. J. (2021). Evaluation of infrared thermography combined with behavioral biometrics for estrus detection in naturally cycling dairy cows. *Animal*, *15*(7), 100205. doi:10.1016/j.animal.2021.100205 PMID:34171567

Mason, J., Dave, R., Chatterjee, P., Allen, I. G., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. *Array*, *8*, 100042. doi:10.1016/j.array.2020.100042

Naidu, B. R., & Babu, M. S. P. (2018). Biometric authentication data with three traits using compression technique, HOG, GMM and fusion technique. *Data in Brief*, *18*, 1976–1986. doi:10.1016/j.dib.2018.03.115 PMID:29900333

Piciucco, E., Lascio, E. D., Maiorana, E., Santini, S., & Campisi, P. (2021). Biometric recognition using wearable devices in real-life settings. *Pattern Recognition Letters*, *146*, 260–266. doi:10.1016/j.patrec.2021.03.020

Piryonesi, S. M., & El-Diraby, T. E. (2020). Data analytics in asset management: Cost-effective prediction of the pavement condition index. *Journal of Infrastructure Systems*, *26*(1), 1–25. doi:10.1061/(ASCE)IS.1943-555X.0000512

Pukdesree, S., & Netinant, P. (2016). Conceptual framework: The adaptive biometrics authentication for accessing cloud computing services using iPhone. *Advances in Intelligent Systems and Computing*, *463*, 209–216. doi:10.1007/978-3-319-40415-8_20

Pukdesree, S., & Netinant, P. (2018). Reviewed: The face authentication processes for accessing cloud computing services using iPhone. *TEM Journal*, *7*(3), 475–479. doi:10.18421/TEM73-01

Purohit, H., & Ajmera, P. K. (2021). Optimal feature level fusion for secured human authentication in multimodal biometric system. *Machine Vision and Applications*, *32*(1), 1–12. doi:10.1007/s00138-020-01146-6

Saeed, U. (2021). Facial micro-expressions as a soft biometric for person recognition. *Pattern Recognition Letters*, *143*, 95–103. doi:10.1016/j.patrec.2020.12.021

Sarier, N. D. (2021). Multimodal biometric authentication for mobile edge computing. *Information Sciences*, *573*, 82–99. doi:10.1016/j.ins.2021.05.036

Selwal, A., Gupta, S. K., Jangra, S., & Rautela, A. (2016). Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry. *Perspectives in Science*, *8*, 705–708. doi:10.1016/j.pisc.2016.06.065

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University • Computer and Information Sciences*, *32*(1), 57–64. .10.1016/j.jksuci.2017.07.001

Smith, C. L., & Brooks, D. J. (2013). Integrated identification technology. *Security Science: The Theory and Practice of Security*, *7*, 153–174. doi:10.1016/B978-0-12-394436-8.00007-2

Srivastva, R., Singh, A., & Singh, Y. N. (2021). PlexNet: A fast and robust ECG biometric system for human Recognition. *Information Sciences*, *558*, 208–228. doi:10.1016/j.ins.2021.01.001

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion*, *66*, 76–99. doi:10.1016/j.inffus.2020.08.021

Tharwat, A. (2018). Classification assessment methods. *Applied Computing and Informatics*, *17*(1), 168–192. doi:10.1016/j.aci.2018.08.003

Vijay, M., & Indumathi, G. (2021). Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications. *Journal of Information Security and Applications*, *58*, 102707. doi:10.1016/j.jisa.2020.102707

Wojtowicz, A., & Joachimiak, K. (2016). Model for adaptable context-based biometric authentication for mobile devices. *Personal and Ubiquitous Computing*, *20*(2), 195–207. doi:10.1007/s00779-016-0905-0

Yadav, S. S., Gothwal, J. K., & Singh, R. (2011). Multimodal biometric authentication system: Challenges and solutions. *Global Journal of Computer Science and Technology*, *11*(16), 56–60.

Yang, W., Wang, S., Zheng, G., & Valli, C. (2019). Impact of feature proportion on matching performance of multi-biometric systems. *ICT Express*, *5*(1), 37–40. doi:10.1016/j.icte.2018.03.001

Meennapa Rukhiran is an assistant professor in the Department of Computer Science at the Rajamangala University of Technology Tawan-OK, Chanthaburi Campus, Thailand. She received her Ph.D. degree in Information Technology from Rangsit University, Thailand. Her research interests lie in information technology applications, information retrieval, information services, and quality of information design. She has published international journals such as the Journal of Information and Communication Technology, TEM Journal, and Journal of Current Science and Technology.

Sorapak Pukdesree is a senior lecturer in the computer science department at Bangkok University in Thailand. He earned a Master of Science in Computer Science from the University of Tennessee at Chattanooga, Tennessee, United States of America. He is currently pursuing a doctorate in information technology from Rangsit University in Thailand. His research interests include information modeling and frameworks, software development and cloud computing, and the Internet of Things. He has published in international journals such as the TEM Journal, WSEAS Computer Transactions, and Advances in Intelligent Systems and Computing.

Paniti Netinant is an associate dean of the graduate school and an associate professor in Rangsit University's Department of Information Technology. He earned his M.S. and Ph.D. in Computer Science from Illinois Institute of Technology in the United States of America. His research interests include information modeling and frameworks, information technology design and development, the Internet of Things, and the layers and services of information. ***He has published in various international journals, including ACM Communications, ACM Computing Surveys, Journal of Information and Communication Technology, TEM Journal, and Journal of Current Science and Technology. He is the corresponding author of this article.***

ภาคผนวก ง

บทความที่รอตีพิมพ์เผยแพร่ในวารสารวิชาการ ICIC Express Letters

ฐานข้อมูล Scopus Q3

Development and Evaluation of Biometric Authentication System based on Facial and Voice Recognition

มหาวิทยาลัยรังสิต Rangsit University

ICIC Express Letters

Editorial Board

Editors-in-Chief
Yan Shi, Tokai University, Japan
Junzo Watada, Waseda University, Japan

Advisory Board
Ramesh Agarwal, USA
Lakhmi C. Jain, Australia
Witold Pedrycz, Canada
Steve P. Banks, UK
Jerry M. Mendel, USA
Takeshi Yamakawa, Japan
Tom Heskes, Netherlands
Masaharu Mizumoto, Japan

Associate Editors
Malek Adjouadi, USA
Roberto Barchino, Spain
Ozer Ciftcioglu, Netherlands
Yunfu Huo, China
Dongsoo Kim, Korea
Magdi Mahmoud, Saudi Arabia
Nikos Nikolaidis, Greece
Takashi Samatsu, Japan
Jianqiang Yi, China
Jamal Ameen, UK
Rawshan Basha, UAE
Vasile Dragan, Romania
Gerardo Iovane, Italy
Minsoo Kim, Korea
Anatolii Martynyuk, Ukraine
Pavel Pakshin, Russia
Hirotaka Takahashi, Japan
Zhong Zhang, Japan
Hyerim Bae, Korea
Michael V. Basin, Mexico
Kei Eguchi, Japan
Amphawan Julsereewong, Thailand
Fanbiao Li, China
Subhas Misra, India
Huafeng Qin, China
Edwin Engin Yaz, USA
Yuxin Zhao, China

Copyright (c) Since 2007 ICIC International. All rights reserved.

มหาวิทยาลัยรังสิต Rangsit University

ICIC Express Letters
Volume 16, Number 4, April 2022

ICIC International ©2020 ISSN 1881-803X
pp. 1-8

Development and Evaluation of Biometric Authentication System based on Facial and Voice Recognition

Meennapa Rukhiran[1], Sorapak Pukdesree[2] and Paniti Netinant[2*]

[1]Department of Social Technology, Rajamangala University of Technology Tawan-OK
Chanthaburi Campus, 22210, Thailand
meennapa_ru@rmutto.ac.th

[2] College of Innovation Digital Technology,
Rangsit University, Pathumthani, 12000, Thailand
*Corresponding author: paniti.n@rsu.ac.th

Received October 2019; accepted January 2020

ABSTRACT. *End users are required to submit a variety of strong usernames and passwords to authenticate with various online applications. Biometric features can serve as a more effective substitute for a traditional restriction technique. Recently, customers reported feeling at ease and secured using their biometric to enter into the system. Biometrics has been utilized for security purposes in a variety of applications recently. However, multimodal biometrics that employs feature-level fusion integrate data from various sources, regardless of how good or bad the combination is. Voice biometric authentication is more comfortable for end-users since it does not require as many motions. It is fascinating to investigate the effect of feature fusions on the matching performance of a multimodal biometric system using face and voice biometrics. This research seeks to design and compare two biometrics that can be accurately integrated to determine authentication accuracy. We propose to analyze biometric authentication using the authentication accuracy matrix. The most advanced biometric authentication with a high degree of accuracy has been devised. On web-based applications, face authentication is the recommended biometric authentication method. Chi-square statistics analysis findings help check and validate significant levels.*

Keywords: Biometric, Authentication, Evaluation, Face Recognition, Voice Recognition

1. Introduction.

Username and password verification is the most common method of user authentication. The username and password are standard and straightforward [1, 2], but it has several drawbacks for both users and service providers. A user may have some online or offline services that require a password combination. As a result, even a complex password with uppercase and lowercase letters, special characters, and numbers may be challenging to remember. To crack a password, an attacker uses a massive dataset of leaked passwords [3].

Biometric characteristics such as the face, fingerprint, iris, ear, and hand can be used to authenticate services with more excellent reliability, simplicity, and integrity [4, 5, 6] than conventional username and password authentication. Unimodal biometrics has limitations for safe identification and verification [7, 8]. Mason et al. [9] state that biometric technology is rapidly evolving in healthcare. A new method for combining periocular biometrics and patient indexes in a healthcare information system is described. Environmental deterioration, sensor noise, and other factors limit each biometric modality. User information must be kept, accessed, retrieved, and managed securely, according to Shakil et al. [10]. Signatures are used in a cloud-based behavioral biometric authentication platform. Cloud computing

services have been researched for their biometric identification capabilities in a variety of fields. Face recognition using cloud services can result in much-reduced latency values compared to local servers [11].

Multimodal biometrics manage to avoid a single point of failure and make biometric systems more resilient [12, 13, 14]. Srivastva et al. [15], an ECG-based biometric recognition system, represents the heart's electrical activity using electrode devices attached to the skin. PlexNet, a stacking model, was created by combining four fine-tuned models. PlexNet is evaluated using two public datasets. The intended biometric recognition system has a 99.66 percent accuracy score in testing. Face and palmprint biometrics identification are accomplished by the integration of non-stationary features [16]. With new goals, the algorithm can improve recognition rates. Kumari and Thangaraj [7] propose a cloud-based system for multimodal biometric feature selection. Multimodal biometrics combines facial and fingerprint recognition. The recommended feature selection method used Ant Colony Optimization. Particle Swarm Optimization is used to extract and classify features. Sarier [17] proposes a biometric identification method for Mobile Edge Computing (MEC). MEC is a secure cloud computing platform that a secure protocol defends against intruders. The new multimodal biometric authentication protocol allows for completely encrypted matching, with the final merged matching score hidden from other computers. Compared to traditional cloud computing, this method reduces latency by 75%.

FIGURE 1. Framework of Biometrics Authentication Cloud Services.

Figure 1 shows our previous system for biometric cloud service authentication using face and voice [18]. Our framework consisted of three layers: end-user, application server, and database server layers. The end-user layer is the user layer that interacts with or utilizes the system. During registration or recognition, the system collects user information such as voice, face, and password. The application server layer contains system applications like speaker and facial recognition. The program runs on a virtual machine and a cloud VPS via a docker container. This application was developed using web technologies and is cross-platform. The database server layer manages data storage, inserting, updating,

มหาวิทยาลัยรังสิต Rangsit University

accessing, and deleting. The system's database is also hosted on a virtual private server in the cloud.

The proposed conceptual framework describes component layer concepts and procedures for a practical authentication system. However, multimodal biometrics combining face and voice authentication has been rarely found in most researches. Face and voice recognition may be more pleasant for end-users without requiring much movement than the well-known face and fingerprint recognition as well as face and ear recognition. The accuracy rates [19, 20] of facial and speech recognition for test schedule authentication systems are essential concerns when performing multimodal biometrics authentication. By utilizing multimodal biometric authentication of facial and voice recognition, the primary contribution is to achieve the highest accuracy possible for genuine recognition. This research aims to develop and evaluate practically accurate factors of facial and voice authentication systems.

This article continues as follows: Section 2 describes related research. Section 3 describes the proposed system. Section 4 summarizes the results. Section 5 is the conclusion.

2. Material and Method.

2.1. Type of Research.

This research is exploratory in nature and takes a systematic approach to research, exploring, and inventing in a trustworthy manner. This research aims to develop a web-based biometric authentication system for undergraduate students' online examinations that makes use of cloud-based services. Students may now learn from anywhere or at any time, thanks to advancements in network technology, notably internet technology. However, a previous process for authenticating students taking online tests will be in place. This study aims to provide multimodal biometric authentication for web-based biometric cloud services that are compatible with mobile devices.

2.2 Research Sample.

The demographic for this study is students enrolled in the computer science and technology department at Bangkok University's school of information technology and innovation during the first semester of 2021. The population is around four-hundred undergraduate students. Purposive sampling was used in this study to choose students from the computer organization course, which is appropriate for the current circumstances in our environment. This course had around eighty students enrolled per class. Seventy-two genuine students and eight phony students are included in the sampling.

2.3. Research Instrument and Procedure.

The study's instrument is a web application written in Python 3.9 and based on the Django framework. This web application makes use of the sqlite3 database management system. This web application may be accessed and used on iOS, Android devices, and a personal computer equipped with a web browser. Before students take the final examinations via online assessments, researchers organize meetings with them.

2.4. Data Collection.

This research collects data through experimental testing. The sampling will enable anyone to use the multimodal biometric authentication system on their devices. The sampling will be provided with the information necessary to log into the system on a specific day and time. To ensure the accuracy of biometric information, the outcome variables of each student's

training and testing processes must achieve a 65 percent accuracy rate for face and fingerprint recognition findings. Eighty students are engaged in this study project, which is divided into two groups. Each sample group has forty students, thirty-six authentic and four fictitious. We create fictitious students with similar looks or voices to those on the biometric database's student identification.

2.5. **Data Analysis.**

The gathered data is an enumeration count of multimodal biometric authentication matches and mismatches. Qualitative data is gathered. Because of this, the Chi-square test is used to analyze and compare one sample group's statistical data. The model's prediction accuracy is compared to the actual values in the table. This matrix is used in predictive analytics, a branch of statistics that uses data to forecast trends and behavior patterns. Predictive analytics uses data modeling, machine learning, artificial intelligence, deep learning algorithms, and data mining. The framework was evaluated using the metrics below.

1) A statistical metric's authentication accuracy score is the ratio of accurate prediction results to comprehensive testing. Equation (1) can be expressed the accuracy.

$$Authentication\ Accuracy\ (ACC) = \frac{Genuine\ pass\ authentication + Fake\ fail\ authentication}{\sum (Total\ Authentications)} \quad (1)$$

2) Authentication precision denotes the precision of the prediction's outcome. Authentication precision can be seen in two ways: positively or negatively. Authentication precision positive refers to the precision with which the member aspect is predicted, whereas negative refers to the precision with the nonmember aspect is predicted. Equations (2) and (3) can be used to express the authentication accuracy score.

$$Authentication\ Precision\ Positive = \frac{Genuine\ pass\ authentication}{(Genuine\ pass\ authentication + Fake\ fail\ authentication)} \quad (2)$$

$$Authentication\ Precision\ Negative = \frac{Fake\ fail\ Authentication}{(Fake\ fail\ Authentication + Genuine\ fail\ authentication)} \quad (3)$$

3) An authentication recall measures the prediction results' accuracy compared to the actual authentication values; it may be thought of as the percentage of correcting predictions made by members named authentication recall positive and the percentage of correcting predictions made by nonmembers named authentication recall negative. Equations (4) and (5) can be used to express the recalled formula.

$$Authentication\ Recall\ Positive = \frac{Genuine\ pass\ authentication}{(Ggenuine\ pass\ authentication + Fake\ pass\ authentication)} \quad (4)$$

$$Authentication\ Recall\ Negative = \frac{Fake\ fail\ Authentication}{(Fake\ fail\ Authentication + Genuine\ fail\ authentication)} \quad (5)$$

4) The F-test of authentication accuracy score is calculated by averaging the accuracy and recall values. The metric score is sometimes referred to as the harmonic mean. The F-test of authentication accuracy metric score has two values: F-test Score Negative and F-test Positive. Assume the score is high, indicating the model is doing well. Equation (6) can be used to express the F-test of authentication accuracy scoring.

มหาวิทยาลัยรังสิต Rangsit University

$$F\text{-test Authentication Accuracy} = \frac{2 \times \text{Genuine pass authentication}}{(\text{Fake fail Authentication} + \text{Fake pass authentication})} \quad (6)$$

3. **Proposed System Implementation.**

The system was created by researchers utilizing a variety of design techniques. On the other hand, this research includes design tools such as a use case diagram and a flow diagram. According to the use case model depicted in Figure 2, the system interacts with three actors: students, teachers, and administrators. Students can register, retrieve, edit, display, and learn courses as well as tests using this system. Teachers can create an account in the system, update their information, show courses and tests, and log into examinations. Finally, administrators can create, retrieve, edit, and remove courses and tests, as well as assign teachers to the course.

FIGURE 2. Use Case Biometrics Authentication System

FIGURE 3. Biometrics Authentication Components.

To begin, students can register biometric into the system using their devices, such as personnel and laptop computers and smartphones, as seen in Figure 3. Students must enter their facial biometric information into the system authentication through the camera; the facial biometric information is stored in a temporary folder on the server. Then, students must enter their voice into the system using a microphone; the speech biometric is stored in a temporary folder on the server. When students click the login button, the system extracts facial biometric characteristics and compares them to biometric template stored in the system, therefore confirming facial biometric authentication. The OpenCV based on LBPH algorithm [5, 21, 22] produces a matching score for the face biometric that represents the degree of similarity between the comparisons. The system then obtains speech biometric characteristics and compares them to the voice biometric authentication performed by when students click the login button. The Mel-frequency Cepstral Coefficients (MFCC) algorithm [23] generates a matching score for the compared speech biometric as a secret score indicating the similarity of the comparisons [24, 25, 26]. The technology then calculates the fusion scores by combining the secret face and voice biometrics scores.

Finally, the system makes an automatic judgment based on the fusion scores obtained from the multimodal biometric authentications. If the fusion scores fall between the range of 60 percent, the system permits the learner to access a home page. On the other hand, if the fusion scores fall beyond the system's threshold values range, the system decides to reject the student authentication. The student has the option of utilizing their password for login in a conventional manner.

4. **Performance and Result Analysis.**

The suggested system's recognition accuracy and methodological validity have been evaluated. The sample group evaluates several techniques for biometric authentication. A sample group of eighty students is composed of seventy-two genuine students and eight phony students. Three steps comprise the examination of three techniques. The first phase is to train all legitimate students' facial and voice biometrics. The following phase secures the system using a variety of biometric authentication methods. For the face and voice authentication of a sample group provided in Table 1, the accuracy metrics of several identity authentications are computed.

TABLE 1. Chi-square different statistics of face and voice recognition comparison

Model	Authentication Metric		Chi Square Values		X^2	*df*	*p*
	Negative	Positive	Negative	Positive			
Genuine Student	13	59	0.3457	0.0933	4.3905	1	0.0361
Fake Student	4	4	3.1117	0.8397			

FIGURE 4. Factors accuracy rates of biometric authentications

FIGURE 5. Accuracy rate and process time per images and voice durations

Figure 4 illustrates the authentication accuracy rate for several biometrics. Equation 1's accuracy metric is used to calculate authentication and F-test accuracies. Face authentication has an accuracy of 0.9650, whereas the F-test has an accuracy of 0.9375. The Chi-Square X^2, *df*, and *p* values are, respectively, 5.3333, 1, and 0.0209. The authentication accuracy of voice authentication is 0.8437, whereas the F-test authentication accuracy is 0.75. The Chi-Square X^2, *df*, and *p* values are, respectively, 8.5714, 1, and 0.0034. Face and voice authentications have an accuracy of 0.8740, while the F-test has an accuracy of

0.7875. The Chi-Square X^2, *df*, and *p* values are 4.3905, 1, and 0.0361, respectively, as shown in Table 1. As indicated in Figure 5, three essential assessing variables that impact biometric authentication are processing time, voice lengths, and authentication accuracy. Seconds are the unit of processing time, and the number of students is the unit of accuracy rate. The brief processing time appears to be preferable on the surface, particularly for face technology. The more face photos provided, the higher the authentication accuracy rate. The voice dramatically increases processing time as the duration of the speech increases. As a result, the longer the duration of the voice, the longer the processing time, and the lower the authentication accuracy rate. The optimal duration of a voice is around four seconds.

5. Conclusions.

We propose a framework to reflect the compatibility of three system layers in this article and the creation of facial and voice authentication systems for cloud services that operate within the exam system. The web-based program detects and matches the students' faces using real-time optimized OpenCV libraries based on the LBPH algorithm. To identify the students' speech, the MFCC algorithm is used. Additionally, we assess the authentication accuracy rates of unimodal and multimodal biometrics, emphasizing the face and voice. The assessment findings are based on a random sample of physical and bogus detections. The Chi-square test is used to verify statistical connections. The statistical metric of face authentication accuracy score delves into the most precise kind of biometric authentication. Biometric authentication elements demonstrate a potentially adaptable and compatible system for optimizing additional face images and voice durations. Further study and refinement of authentication accuracy rates and processing methodologies are required.

REFERENCES

[1] A. Czeskis, M. Dietz, T. Kohno, D. Wallach and D. Balfanz, Strengthening user authentication through opportunistic cryptographic identity assertions, *Proc. of 2012 ACM conference on Computer and communications security*, Raleigh, USA, pp.404-414, 2012.

[2] B. R. Naidu and M. S. P. Babu, Biometric authentication data with three traits using compression technique, HOG, GMM and fusion technique, *Data in Brief*, vol. 18, pp.1976-1986, 2018.

[3] J. Blocki and A. Datta, CASH: A cost asymmetric secure hash algorithm for optimal password protection, *Proc. of IEEE 29th Computer Security Foundations Symposium (CSF)*, Lisbon, Portugal, pp.371–386, 2016.

[4] J. Blasco, T. M. Chen, J. Tapiador and P. Peris-Lopez, A survey of wearable biometric recognition systems, *ACM Computing Surveys*, vol.49, no.3, pp.1-35, 2016.

[5] M. Rukhiran, P. Netinant and T. Elrad, Effecting of environmental conditions to accuracy rates of face recognition based on IoT solution, *Journal of Current Science and Technology*, vol.10, no.1, pp.21-33, 2020.

[6] N. M. Al-Saidi, A. J. Mohammed, R. J. Al-Azawi and A. H. Ali, Iris features via fractal functions for authentication protocols, *International Journal of Innovative Computing, Information and Control*, vol.15, no.4, pp.1349-4198, 2019.

[7] P. Kumari and P. Thangaraj, A fast feature selection technique in multi modal biometrics using cloud framework, *Microprocessors and Microsystems*, vol.79, no.2, pp.103277, 2020.

[8] F. Kausar, Iris based cancelable biometric cryptosystem for secure healthcare smart card, *Egyptian Informatics Journal*, In Press, 2021.

[9] J. Mason, R. Dave, P. Chatterjee , I. G. Allen , A. Esterline and K. Roy, An Investigation of Biometric Authentication in the Healthcare Environment, *Array*, vol. 8, pp.100042, 2020.

[10] K. A. Shakil, F. J. Zareen, M. Alam and S. Jabin, BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud, *Journal of King Saud University - Computer and Information Sciences*, vol.32, pp.57-64, 2020.

[11] M. D. M. Soares, *MEC vs MCC: Performance analysis of real-time applications*, Master's thesis, Polytechnic Institute of Porto, Portugal, 2019.

[12] S. Wong-In and P. Netinant, Revised Software Model Design for Biometric Examiner Personal Verification System, *Proc. of 2017 International Conference on Information Technology*, New York, USA, pp.237-242, 2017.

[13] S. Sarhan, S. Alhassan and S. Elmougy, Multimodal biometric systems: a comparative study, *Arabian Journal for Science and Engineering*, vol.42, no.2, pp.443-457, 2017.

[14] I. Stylios, S. Kokolakis, O. Thanou and S. Chatzis, Behavioral biometrics & continuous user authentication on mobile devices: A survey, *Information Fusion* vol.66, pp.76-99, 2021.

[15] R. Srivastva, A. Singh and Y. N. Singh, PlexNet: A fast and robust ECG biometric system for human Recognition. *Information Sciences*, vol.558, pp.208-228, 2021.

[16] M. I. Ahmad, W. L. Woo and S. Dlay, Non-stationary feature fusion of face and palmprint multimodal biometrics. *Neurocomputing*, vol.177, pp.59-61, 2016.

[17] N. D. Sarier, Multimodal Biometric Authentication for Mobile Edge Computing, *Information Sciences*, vol.573, pp.82-99, 2021.

[18] S. Pukdesree and P. Netinant, Biometric Authentication for Accessing Cloud Computing Services Using iPhone, *Advances in Intelligent Systems and Computing*, vol.463, pp.209-216, 2016.

[19] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, Security and Accuracy of Fingerprint-based Biometrics: A Review. *Symmetry*, vol.11, no.2, pp.141, 2019.

[20] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy and M. Gerla, Challenges of multi-factor authentication for securing advanced IoT applications, *IEEE Network*, vol.33, no.2, pp. 82-88, 2019.

[21] M. Ahsan, Y. Li, J. Zhang, T. Ahad and S. Yazdan, Face Recognition in an Unconstrained and Real-Time Environment Using Novel BMC-LBPH Methods Incorporates with DJI Vision Sensor, *Journal of Sensor and Actuator Networks*, vol.9, no.4, pp.1-12, 2020.

[22] K. Deepti, Implementation of Safety Survilliance System with Face Recognition using IoT, *International Journal of Engineering Research & Technology*, vol.9, no.5, pp.434- 437, 2021.

[23] Q. Li, Y. Yang, T. Lan, H. Zhu, Q. Wei, F. Qiao, X. Liu and H. Yang, MSP-MFCC: Energy-Efficient MFCC Feature Extraction Method With Mixed-Signal Processing Architecture for Wearable Speech Recognition Applications, *IEEE Access*, vol.8, pp.48720-48730, 2020.

[24] R. D. Kumar, A. B. Ganesh and S. S. Kala, Speaker identification system using Gaussian Mixture Model and Support Vector Machines (GMM-SVM) under noisy conditions, *Indian Journal of Science and Technology*, vol.9, no.19, pp.1-6, 2016.

[25] E. S. Wahyuni, Arabic speech recognition using MFCC feature extraction and ANN classification. *Proc. of 2nd International conferences on Information Technology, Information Systems and Electrical Engineering*, Yogyakarta, Indonesia, pp.22-25, 2017.

[26] N. P. Patel and A. Kale, Optimize Approach to Voice Recognition Using IoT, *Proc. of International Conference On Advances in Communication and Computing Technology*, pp.251-256, 2018.

ประวัติผู้วิจัย

ชื่อ	สรพรรค ภักดีศรี
วัน เดือน ปีเกิด	14 พฤษภาคม 2516
สถานที่เกิด	จังหวัดนครพนม ประเทศไทย
ประวัติการศึกษา	มหาวิทยาลัยกรุงเทพ
	ปริญญาวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์, 2537
	University of Tennessee, USA
	Master of Science in Computer Science, 1998
ที่อยู่ปัจจุบัน	111/1003 หมู่บ้านเฟิส์ทโฮม ถ.ร่วมมิตรพัฒนา แยก7 แขวงท่าแร้ง เขตบางเขน กรุงเทพมหานคร 10220
สถานที่ทำงาน	คณะเทคโนโลยีสารสนเทศและนวัตกรรม มหาวิทยาลัยกรุงเทพ
ตำแหน่งปัจจุบัน	อาจารย์ประจำ

มหาวิทยาลัยรังสิต Rangsit University