



การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2

โดย

นายชฎานนท์ ชันฤทธิ์

โครงการพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตร์บัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์

ปีการศึกษา 2567

ลิขสิทธิ์ของมหาวิทยาลัยธรรมศาสตร์

การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2

โดย

นายชญานนท์ ชันฤทธิ์

โครงการพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

วิทยาศาสตร์บัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์

ปีการศึกษา 2567

ลิขสิทธิ์ของมหาวิทยาลัยธรรมศาสตร์

Towards an Affordable Life Logging Device
and Open Data Platform Version 2

BY

Mr. Chayanon Khanrit

A FINAL-YEAR PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF BACHELOR OF SCIENCE

COMPUTER SCIENCE

FACULTY OF SCIENCE AND TECHNOLOGY

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2024

COPYRIGHT OF THAMMASAT UNIVERSITY

มหาวิทยาลัยธรรมศาสตร์
คณะวิทยาศาสตร์และเทคโนโลยี

รายงานโครงการพิเศษ

ของ

นายชยานนท์ ชันธุธิ์

เรื่อง

การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

เมื่อ วันที่ 30 พฤษภาคม พ.ศ. 2568



อาจารย์ที่ปรึกษา

(ผศ. ดร.วนิดา พงธุธิ์วิทยา)

กรรมการสอบโครงการพิเศษ



(ผศ. ดร.ประภาพร รัตนธารัง)

กรรมการสอบโครงการพิเศษ



(ผศ. ดร.ฐาปนา บุญชู)

มหาวิทยาลัยธรรมศาสตร์
คณะวิทยาศาสตร์และเทคโนโลยี

รายงานโครงการพิเศษ

ของ

นายชญานนท์ ชันฤทธิ์

เรื่อง

การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

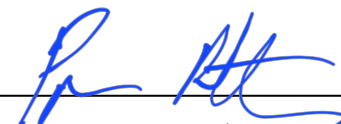
เมื่อ วันที่ 30 พฤษภาคม พ.ศ. 2568

อาจารย์ที่ปรึกษา



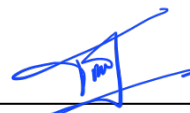
(ผศ. ดร.วนิดา พุทธิวิทยา)

กรรมการสอบโครงการพิเศษ



(ผศ. ดร.ประภาพร รัตนอารง)

กรรมการสอบโครงการพิเศษ



(ผศ. ดร.ฐานา บุญชู)

หัวข้อโครงการพิเศษ

การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับ
จัดเก็บข้อมูลเวอร์ชัน 2

ชื่อผู้เขียน

นายชญานนท์ ชันฤทธิ์

ชื่อปริญญา

วิทยาศาสตร์บัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

สาขาวิชา/คณะ/มหาวิทยาลัย

สาขาวิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์และเทคโนโลยี

มหาวิทยาลัยธรรมศาสตร์

อาจารย์ที่ปรึกษาโครงการพิเศษ

ผศ. ดร.วนิดา พงษ์วิทยา

ปีการศึกษา

2567

บทคัดย่อ

โครงการนี้มุ่งศึกษาการพัฒนาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชันที่ 2 ซึ่งเป็นการปรับปรุงและต่อยอดอุปกรณ์จากเวอร์ชันแรก โดยในเวอร์ชันก่อนหน้าได้พัฒนาอุปกรณ์ที่สามารถบันทึกภาพ ตรวจสอบข้อมูลสภาพแวดล้อมของผู้ใช้ และส่งขึ้นแพลตฟอร์มคลาวด์ (Cloud) เพื่อประมวลผลโดยตรง โดยข้อมูลที่ส่งขึ้นไปถูกนำไปใช้เป็นฐานข้อมูลสำหรับระบบบันทึกและสืบค้นความทรงจำของผู้ใช้ อย่างไรก็ตาม แนวทางดังกล่าวมีความเสี่ยงต่อการรั่วไหลของข้อมูลส่วนบุคคล และกระทบต่อความเป็นส่วนตัวของผู้ใช้ เนื่องจากข้อมูลทั้งหมดถูกส่งออกไปจัดเก็บและประมวลผลภายนอกอุปกรณ์

เวอร์ชันที่ 2 นี้จึงมุ่งเน้นการพัฒนาเพื่อเพิ่มความสามารถในการควบคุมข้อมูลส่วนบุคคลของผู้ใช้ ลดความเสี่ยงในการถูกละเมิดความเป็นส่วนตัว โดยนำแนวคิดการประมวลผลที่ขอบเครือข่าย (Edge Computing) มาใช้สำหรับการจัดการภาพถ่ายก่อนส่งขึ้นคลาวด์ ช่วยให้สามารถปกป้องความเป็นส่วนตัวของผู้ใช้ ในขณะที่ยังคงรักษาให้ผู้ใช้สามารถใช้ประโยชน์จากภาพถ่ายที่ถูกส่งไปจัดเก็บและประมวลผลที่แพลตฟอร์มคลาวด์ได้เช่นเดิม

อุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 ที่พัฒนาขึ้นมีความสามารถในการบันทึกภาพอย่างต่อเนื่องและทำงานร่วมกับสมาร์ทโฟนซึ่งทำหน้าที่เป็นอุปกรณ์สำหรับการประมวลผลที่ขอบเครือข่าย (Edge Device) โดยสมาร์ทโฟนจะรับภาพถ่ายจากอุปกรณ์ แล้วดำเนินการตรวจจับใบหน้าของบุคคลในภาพ หากตรวจพบใบหน้า ระบบจะทำการเบลอใบหน้าเพื่อปกป้องความเป็นส่วนตัวของบุคคลในภาพ นอกจากนี้ยังใช้เทคนิคการจดจำใบหน้าเพื่อเปรียบเทียบกับภาพที่ผู้ใช้ลงทะเบียนไว้ในสมาร์ทโฟน และกำกับเป็นข้อมูลประกอบภาพ (annotation) เพื่อเป็นการรักษาอรรถประโยชน์ในการนำภาพถ่ายไปใช้ในระบบบันทึกและสืบค้นความทรงจำของผู้ใช้ ภาพถ่ายที่ผ่านการประมวลผลแล้วจะถูกส่งไปจัดเก็บยังแพลตฟอร์มคลาวด์ (Cloud) เพื่อใช้ประโยชน์ต่อไป

ผู้พัฒนาโครงการได้ดำเนินการทดลองใช้งานอุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 ในสถานการณ์ต่าง ๆ ที่กำหนดขึ้น (Use Case) เพื่อประเมินความสามารถและประสิทธิภาพของระบบเบื้องต้น ผลการทดลองแสดงให้เห็นว่าอุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 ทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้ และยังสามารถพัฒนาสคริปต์อัตโนมัติเพื่ออำนวยความสะดวกในการพัฒนาต่อยอดระบบและผู้ใช้ในอนาคต

คำสำคัญ: อุปกรณ์บันทึกชีวิต, ความเป็นส่วนตัว, การประมวลผลที่ขอบเครือข่าย, การจดจำใบหน้า, แพลตฟอร์มคลาวด์, การกรองภาพ, การสืบค้นความทรงจำ, สคริปต์อัตโนมัติ

Thesis Title	Towards an Affordable Life Logging Device and Open Data Platform Version 2
Author	Mr. Chayanon Khanrit
Degree	Bachelor of Science
Major Field/Faculty/University	Computer Science Faculty of Science and Technology Thammasat University
Project Advisor	Asst. Prof. Wanida Putthividhya, Ph.D.
Academic Years	2024

ABSTRACT

Towards an Affordable Life Logging Device and Open Data Platform Version 2 is a project that presents the development of the second version of a lifelogging device and its corresponding data platform. It builds upon the first version, which was designed to capture images and environmental data from the user's surroundings and send them directly to a cloud platform for processing. The collected data was used to support a memory recording and retrieval system. However, this approach raised concerns about privacy, as all data was transmitted and processed outside the user's control.

The second version aims to enhance user control over personal data and reduce the risk of privacy violations. The system applies the concept of edge computing to process captured images before sending them to the cloud. This allows the system to protect user privacy while still enabling meaningful use of the stored data.

The updated lifelogging device continuously captures images and works in conjunction with a smartphone, which acts as an edge device. The smartphone receives images from the device, detects human faces in the photos, and blurs them to protect the privacy of individuals appearing in the images. Facial recognition is also used to compare captured images with registered user photos. For images that match, annotations are added to support future memory retrieval. Only the processed images are uploaded to the cloud platform.

The system was tested in predefined use-case scenarios to evaluate its basic functionality and performance. The results show that the device performs as intended. Additionally, the developer created automated scripts to support future development and integration of the system.

Keywords: Lifelogging device, Privacy, Edge computing, Facial recognition, Cloud platform, Image filtering, Memory retrieval, Automatic Script (Cloud Formation)

กิตติกรรมประกาศ

โครงการการศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2 นี้ได้รับความช่วยเหลือจากผู้ช่วยศาสตราจารย์ ดร.วนิดา พงษ์วิทย์ และผู้ช่วยศาสตราจารย์ ดร.ประภาพร รัตนธารง ที่ให้คำแนะนำ ให้คำปรึกษา ตรวจสอบ และแก้ไขข้อบกพร่องในการดำเนินโครงการนี้มาตลอด และนอกจากนี้ ขอขอบพระคุณ รองศาสตราจารย์ ดร.ชัยพร ใจแก้ว จากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ ม.เกษตรศาสตร์ ที่กรุณาสละเวลาให้คำปรึกษาและแนะนำในการพัฒนาอุปกรณ์ IoT เป็นอย่างดี จึงขอขอบพระคุณเป็นอย่างสูง

สุดท้ายขอขอบพระคุณผู้มีส่วนเกี่ยวข้องทั้งหมดที่ช่วยให้คำแนะนำ ปรึกษาและแก้ไขในการดำเนินโครงการนี้

นายชญานนท์ ชันฤทธิ์

สารบัญ

	หน้า
บทคัดย่อ	2
ABSTRACT	4
กิตติกรรมประกาศ	5
สารบัญ	6
สารบัญตาราง	12
สารบัญภาพ	13
รายการสัญลักษณ์และคำย่อ	15
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของโครงการ	1
1.2 วัตถุประสงค์	1
1.3 ขอบเขตของโครงการ	2
1.4 ผลที่คาดว่าจะได้รับ	3
1.5 ข้อจำกัดของโครงการ	3
บทที่ 2 วรรณกรรมและงานวิจัยที่เกี่ยวข้อง	4
2.1 แนวคิดเกี่ยวกับข้อมูลและความเป็นส่วนตัว	4
2.1.1 การบันทึกชีวิตและเทคโนโลยีการบันทึกชีวิต (Lifelog and Lifelogging)	4
2.1.2 ข้อมูลส่วนบุคคล (Personal Data)	5
2.1.2.1 ข้อมูลส่วนบุคคล (Personal Data)	5

2.1.2.2 ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)	5
2.1.3 ปกป้องข้อมูลส่วนบุคคล (Personal Data Protection)	6
2.1.4 ความเป็นส่วนตัวของข้อมูล (Data Privacy) และการปกป้องความเป็นส่วนตัว (Privacy Protection)	7
2.1.4.1 ความเป็นส่วนตัวของข้อมูล (Data privacy)	7
2.1.4.2 การปกป้องความเป็นส่วนตัว (Privacy Protection)	7
2.1.5 การประมวลผลที่ขอบเครือข่าย (Edge computing)	8
2.1.6 การประมวลผลที่คลาวด์ (Cloud computing)	9
2.1.6.1 Infrastructure as a Service (IaaS)	9
2.1.6.2 Platform as a Service (PaaS)	9
2.1.6.3 Software as a Service (SaaS)	10
2.2 เทคโนโลยีพื้นฐานที่เกี่ยวข้อง	10
2.2.1 ปัญญาประดิษฐ์ การเรียนรู้ของเครื่อง และการเรียนรู้เชิงลึก (Artificial Intelligence, Machine Learning, Deep Learning)	10
2.2.1.1 ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	11
2.2.1.2 การเรียนรู้ของเครื่อง (Machine Learning: ML)	11
2.2.1.3 การเรียนรู้เชิงลึก (Deep Learning: DL)	11
2.2.2 การตรวจจับใบหน้า (Face Detection)	12
2.2.2.1 Haar Cascade	12
2.2.3 การจดจำใบหน้า (Face Recognition)	13
2.2.4 Infrastructure as Code (IaC)	13
2.2.4.1 ใช้งานกับ Amazon Web Service	14
2.2.4.2 ไม่ขึ้นกับผู้ให้บริการคลาวด์รายใด (Vendor-neutral)	14
2.2.5 การแฮช (Hash)	14

2.2.5.1 ข้อมูลรับเข้า (Input)	14
2.2.5.2 ฟังก์ชันแฮช (Hash Function)	15
2.2.5.3 ผลลัพธ์แฮช (Hash Output)	15
2.3 เทคโนโลยีและเครื่องมือที่ใช้ในโครงการ	15
2.3.1 Mobile Application	15
2.3.2 Wi-Fi	15
2.3.3 HTTP (Hypertext Transfer Protocol)	16
2.3.4 OpenCV (Open Source Computer Vision Library)	16
2.3.5 ML Kit และเทคโนโลยีการตรวจจับใบหน้า	16
2.3.6 FaceNet Model	16
2.3.7 การเปรียบเทียบระหว่าง ML Kit และ Haar Cascade	16
2.3.8 เปรียบเทียบระหว่าง FaceNet และ DeepFace	17
2.4 งานวิจัยที่เกี่ยวข้อง	17
2.4.1 ด้านการปกป้องความเป็นส่วนตัวของข้อมูล	17
2.4.2 ด้านการใช้อุปกรณ์เอดจ์เก็บข้อมูลและการประมวลผลที่ขอบเครือข่าย	19
บทที่ 3 วิธีการวิจัย	22
3.1 ภาพรวมของโครงการ	23
3.1.1 ส่วนที่ยังใช้สถาปัตยกรรมเดิม	24
3.1.1.1 ส่วนที่รับข้อมูลเซนเซอร์ที่อุปกรณ์ส่งมา	24
3.1.1.2 ส่วนที่จัดเก็บข้อมูลที่ใช้เก็บข้อมูลรูปภาพ	24
3.1.1.3 ส่วนฐานข้อมูลที่ใช้เก็บข้อมูลที่ได้จากเซนเซอร์	24
3.1.1.4 ส่วนของการตรวจจับสิ่งของภายในภาพ (Label Detection)	25
3.1.1.5 ส่วนของเว็บแอปพลิเคชัน (Web application)	25

3.1.2	ส่วนที่เพิ่มเข้ามาในอุปกรณ์บันทึกชีวิตเวอร์ชัน 2 (LifeLog V.2)	25
3.1.2.1	การส่งข้อมูลจากอุปกรณ์ไปยังโทรศัพท์เคลื่อนที่	26
3.1.2.2	รายละเอียดของการประมวลผลที่ขอบเครือข่าย (Edge Computing)	26
3.1.3	รายละเอียดของสคริปต์อัตโนมัติ (Automate script)	28
3.1.3.1	การรับข้อมูลจากเซนเซอร์มาเก็บไว้ในฐานข้อมูล	28
3.1.3.2	การรับข้อมูลรูปภาพจากอุปกรณ์เอดจ์ (Edge) มาจัดเก็บในที่เก็บข้อมูล	28
3.1.3.3	การวิเคราะห์รูปภาพและบันทึกผลลัพธ์ในฐานข้อมูล	29
3.2	การวิเคราะห์ขอบเขตและความต้องการของระบบ	29
3.2.1	โมดูลอุปกรณ์การรวบรวมและบันทึกข้อมูลชีวิตประจำวัน	29
3.2.1.1	ส่วนประกอบสำคัญ	30
3.2.1.2	หน้าที่ของโมดูล	33
3.2.2	โมดูลเอดจ์ (Edge)	33
3.2.2.1	ส่วนประกอบสำคัญ	33
3.2.2.2	หน้าที่ของโมดูล	33
3.2.2.3	แผนภาพกิจกรรมของระบบ (Activity Diagram)	34
3.2.3	โมดูลสำหรับจัดเก็บข้อมูลที่เก็บได้จากเซนเซอร์บนคลาวด์	36
3.2.3.1	ส่วนประกอบสำคัญ	36
3.2.3.2	หน้าที่ของโมดูล	36
3.2.4	โมดูลสำหรับจัดเก็บข้อมูลรูปภาพบนคลาวด์	36
3.2.4.1	ส่วนประกอบสำคัญ	36
3.2.4.2	หน้าที่ของโมดูล	36
3.2.5	โมดูลการวิเคราะห์รูปภาพบนคลาวด์	36
3.2.5.1	ส่วนประกอบสำคัญ	36
3.2.5.2	หน้าที่ของโมดูล	37

3.2.6	เว็บแอปพลิเคชัน (Web application)	37
3.2.6.1	ส่วนประกอบสำคัญ	37
3.2.6.2	หน้าที่ของโมดูล	37
3.3	ประเด็นที่น่าสนใจและสิ่งที่ท้าทาย	37
3.4	ผลลัพธ์ที่คาดหวัง	38
3.5	การดำเนินงาน	38
3.5.1	ส่วนอุปกรณ์ฮาร์ดแวร์	38
3.5.2	การพัฒนาสคริปต์อัตโนมัติ (Automate script)	39
3.5.3	ส่วนของซอฟต์แวร์ในโทรศัพท์เคลื่อนที่	40
3.5.3.1	หน้าหลักของแอปพลิเคชัน	40
3.5.3.2	หน้าลงทะเบียนใบหน้า	40
3.5.3.3	หน้าการทำงานหลักสำหรับดึงข้อมูลจากอุปกรณ์และจดจำใบหน้า	41
3.5.4	ส่วนของซอฟต์แวร์ในเว็บแอปพลิเคชัน	42
3.5.4.1	หน้าการแสดงรูปภาพที่ผ่านกระบวนการปกป้องความเป็นส่วนตัวส่วนตัวแล้ว	43
3.5.4.2	หน้าการค้นหาด้วยชื่อของคนที่ยังลงทะเบียน	44
3.5.5	การทดลองเพื่อหาค่าเกณฑ์ (Threshold) ในการจับคู่ใบหน้าในระบบจดจำใบหน้าที่เหมาะสมกับระบบ	44
3.5.6	การทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า	45
3.5.7	การทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น	47
บทที่ 4	ผลการดำเนินงาน	53
4.1	การจัดเตรียมฮาร์ดแวร์และซอฟต์แวร์	53
4.1.1	ฮาร์ดแวร์ที่ใช้ในการพัฒนาอุปกรณ์ IoT	53

4.1.2 ภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนา	53
4.1.2.1 กลุ่มของภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนาอุปกรณ์ IoT	53
4.1.2.2 กลุ่มของภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนาแอปพลิเคชันในโทรศัพท์เคลื่อนที่	53
4.1.2.3 กลุ่มของภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนาแอปพลิเคชันบนทีกและสืบค้นความทรงจำของผู้ใช้	54
4.1.2.4 บริการบนคลาวด์ (Cloud service) Amazon Web Services	54
4.1.3 คอมพิวเตอร์ที่ใช้ในการพัฒนา	55
4.2 การทดสอบระบบ	56
4.2.1 การสร้างทรัพยากรด้วยสคริปต์อัตโนมัติ	56
4.2.2 การทดสอบการเบลอใบหน้าที่ตรวจจับได้ในรูปภาพ	56
4.2.3 การทดสอบกระบวนการส่งรูปภาพ	57
4.2.4 การทดสอบการแฮชชื่อและจัดเก็บค่าแฮชบนคลาวด์	57
4.2.5 ผลการทดลองเพื่อหาค่าเกณฑ์ (Threshold) ในการจับคู่ใบหน้าในระบบจดจำใบหน้าที่เหมาะสมกับระบบ	59
4.2.6 ผลการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า	60
4.2.7 ผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น	61
บทที่ 5 สรุป	63
5.1 อภิปรายผลการทดลอง	63
5.2 สรุปผลการดำเนินงาน	64
5.3 แนวทางการพัฒนาต่อ	64
รายการอ้างอิง	65

สารบัญตาราง

	หน้า
ตารางที่ 2.1 เปรียบเทียบงานวิจัยที่เกี่ยวข้อง	21
ตารางที่ 3.1 ตารางแสดงชุดข้อมูลสำหรับการทดลองหาค่า Threshold ที่เหมาะสม	45
ตารางที่ 3.2 ตารางแสดงชุดข้อมูลสำหรับการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไป เข้าโมเดลจดจำใบหน้า	46
ตารางที่ 3.3 ตารางแสดงชุดการทดลองชุดที่ 1	47
ตารางที่ 3.4 ตารางแสดงชุดการทดลองชุดที่ 2	48
ตารางที่ 3.5 ตารางแสดงชุดการทดลองชุดที่ 3	49
ตารางที่ 3.6 ตารางแสดงชุดการทดลองชุดที่ 4	50
ตารางที่ 3.7 ตารางแสดงชุดการทดลองชุดที่ 5	51
ตารางที่ 4.1 คอมพิวเตอร์ที่ใช้ในการพัฒนา	55
ตารางที่ 4.2 ตารางแสดงผลจากการทดลองหาค่า Threshold ที่เหมาะสม	59
ตารางที่ 4.3 ตารางแสดงผลจากการทดลองทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้า โมเดลจดจำใบหน้า	60
ตารางที่ 4.4 ตารางแสดง Precision ของโมเดล	61

สารบัญภาพ

		หน้า
ภาพที่ 2.1	แสดงการทำงานของ Haar-like features	13
ภาพที่ 2.2	สถาปัตยกรรมของ Lifelog Ver.1	18
ภาพที่ 2.3	Flow การทำงานของระบบ EFR	19
ภาพที่ 3.1	แสดงสถาปัตยกรรมของระบบในเวอร์ชันที่ 2 ที่พัฒนาต่อจากเวอร์ชันที่ 1	23
ภาพที่ 3.2	สถาปัตยกรรมส่วนที่เพิ่มเข้ามาในเวอร์ชัน 2	25
ภาพที่ 3.3	กระบวนการทำงานของการประมวลผลที่ขอบเครือข่าย (Edge Computing)	27
ภาพที่ 3.4	รายละเอียดการสร้างโครงสร้างพื้นฐานผ่านเทมเพลต	29
ภาพที่ 3.5	โมดูลไมโครคอนโทรลเลอร์ ESP32-CAM	30
ภาพที่ 3.6	เซนเซอร์วัดอุณหภูมิและความชื้น SHT21	30
ภาพที่ 3.7	โมดูลจีพีเอส (GPS) GY-NEO-6M Ublox	31
ภาพที่ 3.8	เซนเซอร์วัดความเข้มของรังสีอัลตราไวโอเลต Grove – Sunlight Sensor	31
ภาพที่ 3.9	โมดูลสำหรับชาร์จแบตเตอรี่ TP4056 1A USB-C Charger	32
ภาพที่ 3.10	แบตเตอรี่ 3.7 โวลต์ 5000 มิลลิแอมป์ชั่วโมงลิเทียมโพลิเมอร์	32
ภาพที่ 3.11	Activity Diagram ของฟังก์ชันลงทะเบียนใบหน้าในโทรศัพท์เคลื่อนที่	34
ภาพที่ 3.12	Activity Diagram ของฟังก์ชันการตรวจจับและจดจำใบหน้าในโทรศัพท์เคลื่อนที่	35
ภาพที่ 3.13	อุปกรณ์สำหรับการบันทึกชีวิตในเวอร์ชันที่ 1	39
ภาพที่ 3.14	แสดงเทมเพลตที่ถูกสร้างโดย AWS CloudFormation	39
ภาพที่ 3.15	แสดงหน้าหลักของแอปพลิเคชัน	40
ภาพที่ 3.16	แสดงหน้าลงทะเบียนใบหน้าของแอปพลิเคชัน	40
ภาพที่ 3.17	แสดงหน้าต่างให้ผู้ใช้อกรอกชื่อคนที่ลงทะเบียน	41
ภาพที่ 3.18	แสดงหน้าการทำงานหลักสำหรับดึงข้อมูลจากอุปกรณ์และจดจำใบหน้า	41
ภาพที่ 3.19	แสดงภาพที่ดึงมาจากเซิร์ฟเวอร์ของอุปกรณ์	42
ภาพที่ 3.20	แสดงรูปภาพที่ผ่านกระบวนการปกป้องความเป็นส่วนตัวแล้ว	43
ภาพที่ 3.21	แสดงหน้าการค้นหาด้วยชื่อของคนที่ลงทะเบียน	44
ภาพที่ 4.1	แสดงรูปภาพที่แสดงผลในเว็บและมีการเบลอใบหน้า	56
ภาพที่ 4.2	ตัวอย่างของรูปภาพที่ถูกส่งมาเก็บใน Amazon S3	57
ภาพที่ 4.3	ตัวอย่างของรูปภาพที่จับคู่ตรงกับใบหน้าที่ลงทะเบียนและแฮชชื่อนั้น	58
ภาพที่ 4.4	ตัวอย่างค่าแฮชที่ถูกจัดเก็บใน Amazon DynamoDB	58

ภาพที่ 4.5 แผนภูมิแสดงผลการทดลองหาค่า Threshold ที่เหมาะสม	59
ภาพที่ 4.6 แผนภูมิแสดงผลการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า	60
ภาพที่ 4.7 แผนภูมิแสดงผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น (Precision)	61
ภาพที่ 4.8 แผนภูมิแสดงผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น (Recall)	62

รายการสัญลักษณ์และคำย่อ

สัญลักษณ์/คำย่อ

คำเต็ม/คำจำกัดความ

AWS

Amazon Web Service

OTA

Over The Air

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของโครงการ

อุปกรณ์บันทึกชีวิต (Lifelogging Device) เป็นเทคโนโลยีที่ช่วยให้ผู้ใช้สามารถบันทึกภาพและข้อมูลจากสภาพแวดล้อมรอบตัวในชีวิตประจำวัน เพื่อใช้เป็นข้อมูลประกอบความทรงจำหรือการย้อนทบทวนเหตุการณ์ที่ผ่านมา โครงการ การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูล ในปีการศึกษาที่ผ่านมา [1] ได้พัฒนาอุปกรณ์บันทึกชีวิตเวอร์ชันแรก ซึ่งสามารถบันทึกภาพและตรวจวัดข้อมูลสภาพแวดล้อมของผู้ใช้ แล้วส่งข้อมูลทั้งหมดขึ้นไปยังแพลตฟอร์มคลาวด์ (Cloud Platform) เพื่อจัดเก็บและประมวลผล โดยมีเป้าหมายในการใช้ข้อมูลดังกล่าวเป็นฐานข้อมูลในระบบบันทึกและสืบค้นความทรงจำของผู้ใช้ในอนาคต

อย่างไรก็ตาม แนวทางการส่งข้อมูลภาพถ่ายและข้อมูลสภาพแวดล้อมไปประมวลผลภายนอกอุปกรณ์ทั้งหมด อาจก่อให้เกิดความกังวลเรื่องความเป็นส่วนตัวของผู้ใช้ เนื่องจากผู้ใช้ไม่สามารถควบคุมกระบวนการประมวลผลได้โดยตรง และข้อมูลอาจตกอยู่ในความเสี่ยงจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต

โครงการนี้จึงมุ่งพัฒนาอุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 โดยนำแนวคิดการประมวลผลที่ขอบเครือข่าย (Edge Computing) มาใช้ เพื่อให้การจัดการข้อมูลส่วนบุคคลของผู้ใช้สามารถเกิดขึ้นภายในอุปกรณ์ที่ผู้ใช้เชื่อถือได้ (trusted edge devices) ก่อนส่งข้อมูลผ่านการคัดกรองแล้วไปจัดเก็บยังแพลตฟอร์มคลาวด์อย่างเหมาะสม โดยยังคงธรรมาภิบาลของข้อมูลไว้เพื่อนำไปใช้ในระบบบันทึกและสืบค้นความทรงจำ

1.2 วัตถุประสงค์

การพัฒนาอุปกรณ์บันทึกชีวิตในโครงการนี้มีวัตถุประสงค์หลักเพื่อสร้างสมดุลระหว่าง การปกป้องความเป็นส่วนตัวของผู้ใช้ (privacy protection) และ การคงธรรมาภิบาลของข้อมูล (utility retention) ซึ่งเป็นสิ่งจำเป็นในการนำข้อมูลไปใช้ประโยชน์ต่อในระบบบันทึกและสืบค้นความทรงจำ โครงการจึงมุ่งเน้นการจัดการข้อมูลภายในอุปกรณ์ของผู้ใช้ หรืออุปกรณ์ที่ผู้ใช้ให้ความเชื่อถือ (trusted edge devices) ก่อนส่งออกไปจัดเก็บบนแพลตฟอร์มคลาวด์เพื่อใช้ประโยชน์ต่อไป โดยออกแบบกระบวนการจัดการภาพถ่าย ซึ่งประกอบด้วย การปกปิดใบหน้าของบุคคลด้วยวิธีการเบลอ (face blurring) การจดจำใบหน้าบุคคล (face recognition) และการกำกับข้อมูลใน

ภาพ (annotation) เพื่อให้สามารถเลือกจัดเก็บเฉพาะข้อมูลที่เกี่ยวข้องกับผู้ใช้ได้อย่างเหมาะสม โดยไม่ละเมิดสิทธิของบุคคลอื่นที่ปรากฏอยู่ในภาพ

เพื่อให้บรรลุแนวทางดังกล่าว โครงการจึงมีวัตถุประสงค์ย่อย ดังนี้

1. เพื่อพัฒนาอุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 ให้สามารถเชื่อมต่อกับ
สมาร์ตโฟนซึ่งทำหน้าที่ประมวลผลข้อมูลในระดับขอบเครือข่าย (Edge
Computing)
2. เพื่อออกแบบกระบวนการจัดการภาพถ่ายที่คำนึงถึงความเป็นส่วนตัว ซึ่ง
ประกอบด้วยขั้นตอนต่าง ๆ ดังนี้ การตรวจจับใบหน้า การปกปิดใบหน้าของ
บุคคลด้วยวิธีการเบลอ และการจดจำใบหน้า
3. เพื่อกำกับข้อมูลประกอบภาพ (annotation) เพื่อยังคงอรรถประโยชน์รองรับ
การใช้งานในระบบบันทึกและสืบค้นความทรงจำได้
4. เพื่อจัดเก็บเฉพาะภาพที่ผ่านการจัดการโดยคำนึงถึงความเป็นส่วนตัวและ
อรรถประโยชน์ของข้อมูลแล้วบนแพลตฟอร์มคลาวด์ (Cloud Platform)
5. เพื่อประเมินความสามารถของระบบผ่านการทดลองในสถานการณ์ที่กำหนด
(Use Case)

1.3 ขอบเขตของโครงการ

โครงการการศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลรุ่นที่ 2 ที่
พัฒนาปรับปรุงประสิทธิภาพต่อจากรุ่นที่ 1 มีขอบเขตของโครงการดังนี้

1. โครงการนี้มุ่งเน้นการพัฒนาอุปกรณ์บันทึกชีวิตที่สามารถบันทึกภาพและ
เชื่อมต่อกับสมาร์ตโฟนเพื่อประมวลผลข้อมูลในระดับขอบเครือข่าย
2. กระบวนการจัดการภาพถ่ายทั้งหมด เช่น การตรวจจับใบหน้า การเบลอ การ
จดจำใบหน้า และการกำกับ annotation จะดำเนินการในสมาร์ตโฟน
3. ภาพถ่ายที่ผ่านการจัดการโดยคำนึงถึงความเป็นส่วนตัวและอรรถประโยชน์ของ
ข้อมูลแล้วเท่านั้นที่จะถูกจัดเก็บบนแพลตฟอร์มคลาวด์
4. มีการจัดทำสคริปต์อัตโนมัติเพื่ออำนวยความสะดวกในการพัฒนาต่อยอระบบ
ในอนาคต และอำนวยความสะดวกในการใช้งานอุปกรณ์บันทึกชีวิตในอนาคต
5. มีการทดลองใช้งานระบบในสถานการณ์จำลองเพื่อประเมินความสามารถใน
เบื้องต้น

1.4 ผลที่คาดว่าจะได้รับ

1. ได้อุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 ที่สามารถทำงานร่วมกับสมาร์ทโฟนได้อย่างเหมาะสม
2. ได้ระบบจัดการภาพถ่ายที่สามารถปกป้องความเป็นส่วนตัวของผู้ใช้และบุคคลในภาพได้อย่างมีประสิทธิภาพ
3. ได้ข้อมูลที่ยังคงอรรถประโยชน์ต่อการจัดเก็บและใช้งานในระบบบันทึกและสืบค้นความทรงจำ
4. ได้เครื่องมือสนับสนุนการพัฒนาต่อยอดระบบ lifelogging ภายใต้แนวคิด privacy-aware ได้ในอนาคต

1.5 ข้อจำกัดของโครงการ

1. การใช้สคริปต์อัตโนมัติ ผู้ใช้จำเป็นต้องมีบัญชีของ AWS อยู่แล้วและต้องมีความรู้เบื้องต้นในการใช้งานบริการ Cloud formation ของผู้ให้บริการ AWS
2. สคริปต์อัตโนมัติสามารถสามารถสร้างทรัพยากรบนคลาวด์ส่วนใหญ่ได้แต่ยังมีส่วนที่ผู้ใช้ต้องสร้างเองหลังจากใช้สคริปต์แล้วนั่นก็คือ สร้าง Thing ในเซอร์วิส AWS IoT Core ซึ่งจำเป็นต้องดาวน์โหลด Certificate และ Private Key สำหรับเชื่อมต่อเซอร์วิสกับอุปกรณ์ IoT และต้องจัดเตรียม RSA key pair สำหรับสร้างเซอร์วิส Amazon EC2
3. แอปพลิเคชันมือถือที่เป็นการการประมวลผลที่ขอบเครือข่าย (Edge Computing) ใช้ได้กับระบบปฏิบัติการแอนดรอยด์ (Android) เท่านั้น
4. การค้นหารูปภาพจากชื่อสามารถค้นหาได้จากชื่อที่ใช้ลงทะเบียนเท่านั้น

บทที่ 2

วรรณกรรมและงานวิจัยที่เกี่ยวข้อง

การออกแบบและพัฒนาอุปกรณ์บันทึกชีวิตฯ เวอร์ชันที่ 2 จำเป็นต้องอาศัยความเข้าใจในแนวคิดและเทคโนโลยีที่เกี่ยวข้องหลายด้าน ทั้งในเชิงของแนวคิดการบันทึกชีวิตและความท้าทายด้านความเป็นส่วนตัว ตลอดจนเทคโนโลยีพื้นฐานที่รองรับกระบวนการต่าง ๆ ตั้งแต่การจัดเก็บการประมวลผล และการปกป้องข้อมูล โครงการนี้จึงศึกษาและอ้างอิงองค์ความรู้จากงานวิจัยที่เกี่ยวข้อง รวมถึงแนวคิดทางเทคนิคที่เป็นรากฐานสำคัญในการออกแบบระบบ

เนื้อหาในบทนี้แบ่งออกเป็น 4 ส่วน ได้แก่ แนวคิดเกี่ยวกับข้อมูลและความเป็นส่วนตัว (หัวข้อ 2.1) เทคโนโลยีพื้นฐานที่เกี่ยวข้อง (หัวข้อ 2.2) เทคโนโลยีและเครื่องมือที่ใช้ในโครงการ (หัวข้อ 2.3) และ งานวิจัยที่เกี่ยวข้อง (หัวข้อ 2.4)

2.1 แนวคิดเกี่ยวกับข้อมูลและความเป็นส่วนตัว

2.1.1 การบันทึกชีวิตและเทคโนโลยีการบันทึกชีวิต (Lifelog and Lifelogging)

การบันทึกชีวิต (lifelog) หมายถึงกระบวนการรวบรวมข้อมูลส่วนตัวจากชีวิตประจำวันของบุคคล เพื่อนำไปใช้ในการติดตาม วิเคราะห์ หรือทบทวนเหตุการณ์ในอดีต โดยข้อมูลที่เก็บรวบรวมอาจครอบคลุมทั้งด้านพฤติกรรม สุขภาพ และบริบทแวดล้อม ในขณะที่เทคโนโลยีการบันทึกชีวิต (lifelogging) หมายถึงการใช้ระบบอิเล็กทรอนิกส์หรืออุปกรณ์ดิจิทัลเพื่อสนับสนุนกระบวนการดังกล่าว โดยสามารถตรวจจับ จัดเก็บ และประมวลผลข้อมูลได้อย่างต่อเนื่องและอัตโนมัติ เช่น ภาพถ่าย เสียง สถานที่ และกิจกรรมต่าง ๆ ในชีวิตประจำวัน

แหล่งข้อมูลสำหรับการบันทึกชีวิตโดยใช้เทคโนโลยีดิจิทัลมีหลากหลายรูปแบบ เช่น อุปกรณ์สวมใส่ (wearable devices) เช่น สมาร์ทวอตช์ (smart watch) และฟิตเนสแทร็กเกอร์ (fitness tracker) ที่ใช้บันทึกข้อมูลด้านสุขภาพ เช่น อัตราการเต้นของหัวใจ คุณภาพการนอนหลับ เซ็นเซอร์ซึ่งตรวจวัดข้อมูลสภาพแวดล้อม เช่น อุณหภูมิ ความชื้น ความเข้มแสงยูวี (UV) และตำแหน่งจากระบบจีพีเอส (GPS) รวมถึงกล้องสวมใส่ (wearable camera) ซึ่งสามารถบันทึกเหตุการณ์รอบตัวผู้ใช้ได้โดยอัตโนมัติทั้งในรูปแบบของภาพนิ่งและคลิปวิดีโอ

เทคโนโลยีการบันทึกชีวิตได้รับความสนใจและนำไปประยุกต์ใช้ในหลากหลายบริบท เช่น การช่วยกระตุ้นความจำในผู้สูงอายุหรือผู้มีภาวะสูญเสียความทรงจำ [3] การวิเคราะห์

พฤติกรรมและรูปแบบการใช้ชีวิตของผู้ใช้ [4][5] รวมถึงการสนับสนุนการดูแลสุขภาพ เช่น การเลิกบุหรี่ หรือการติดตามพฤติกรรมกรรมการบริโภคอาหาร [6]

อย่างไรก็ตาม เทคโนโลยีนี้ยังเผชิญกับข้อกังวลด้านจริยธรรมและความเป็นส่วนตัว โดยเฉพาะอย่างยิ่งเมื่อมีการบันทึกภาพหรือข้อมูลของบุคคลอื่นโดยไม่ได้รับความยินยอม ซึ่งอาจละเมิดสิทธิส่วนบุคคลได้

2.1.2 ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคล (personal data) หมายถึง ข้อมูลใด ๆ ที่สามารถใช้ระบุตัวตนของบุคคลได้ไม่ว่าโดยทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล หมายเลขบัตรประจำตัวประชาชน ที่อยู่ อีเมล หมายเลขโทรศัพท์ รวมถึงข้อมูลที่เกิดจากการใช้เทคโนโลยี เช่น รหัสอุปกรณ์ (device ID) ที่อยู่ไอพี (IP address) หรือพิกัดตำแหน่งที่ได้จากระบบ GPS [7]

ในบริบทของการบันทึกชีวิต ข้อมูลส่วนบุคคลอาจได้มาจากอุปกรณ์หรือเซนเซอร์ต่าง ๆ เช่น กล้องที่บันทึกใบหน้า ไมโครโฟนที่บันทึกเสียง และอุปกรณ์ที่ติดตามตำแหน่ง ซึ่งข้อมูลเหล่านี้สามารถนำไปวิเคราะห์เพื่อสร้างแบบจำลองพฤติกรรมผู้ใช้ หรือแม้แต่อนุมานข้อมูลที่จะเสียก่อน เช่น สถานะสุขภาพ ความสนใจ หรือกิจวัตรประจำวัน

ข้อมูลส่วนบุคคล [7] แบ่งออกเป็น 2 ประเภท ได้แก่

2.1.2.1 ข้อมูลส่วนบุคคลทั่วไป

ข้อมูลส่วนบุคคลทั่วไป คือข้อมูลที่สามารถระบุตัวบุคคลได้โดยตรงหรือโดยอ้อม เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล เพศ วันเกิด รูปร่าง เสียง หรือภาพเคลื่อนไหว ข้อมูลเหล่านี้มักพบในระบบหรือแอปพลิเคชันที่มีการบันทึกข้อมูลผู้ใช้งานในชีวิตประจำวัน

2.1.2.2 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว คือ ข้อมูลที่หากรั่วไหลอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล เช่น ข้อมูลสุขภาพ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา เชื้อชาติ พฤติกรรมทางเพศ หรือข้อมูลชีวภาพ เช่น

ลายนิ้วมือ หรือภาพใบหน้า [8] ข้อมูลประเภทนี้มักต้องการมาตรการคุ้มครองที่เข้มงวดเป็นพิเศษ

นอกจากนี้ L.-D. Tran และคณะ [2] ได้ชี้ให้เห็นว่าการบันทึกชีวิต (lifelogging) เป็นกระบวนการรวบรวมข้อมูลส่วนบุคคลที่เกี่ยวข้องกับกิจกรรมและประสบการณ์ในชีวิตประจำวันอย่างครอบคลุมและต่อเนื่อง โดยในสังคมปัจจุบัน ข้อมูลส่วนบุคคลจำนวนมากไม่ได้ถูกรวบรวมโดยเจ้าของข้อมูลเองเท่านั้น แต่ยังถูกบันทึกโดยบุคคลที่สาม ไม่ว่าจะเป็นอุปกรณ์ สมาร์ทโฟน หรือแอปพลิเคชันต่าง ๆ ที่มีการเข้าถึงข้อมูลของผู้ใช้ การที่ข้อมูลส่วนตัวกระจัดกระจายอยู่ในหลายแหล่ง ทำให้ผู้ใช้เผชิญกับความท้าทายในการเข้าถึง วิเคราะห์ และควบคุมข้อมูลเหล่านี้ได้อย่างมีประสิทธิภาพ

ด้วยการเติบโตอย่างรวดเร็วของเทคโนโลยี เช่น โมเดลภาษาขนาดใหญ่ (Large Language Models: LLM) อาจนำมาใช้เพื่อสนับสนุนการจัดการข้อมูลส่วนบุคคลได้ดีขึ้น อย่างไรก็ตาม ก็ยังมีความกังวลด้านความปลอดภัยและความเป็นส่วนตัว เนื่องจากบุคคลที่สามอาจสามารถเข้าถึงข้อมูลเหล่านี้ได้โดยไม่ได้รับอนุญาต

2.1.3 การปกป้องข้อมูลส่วนบุคคล (Personal Data Protection)

การปกป้องข้อมูลส่วนบุคคล (Personal Data Protection) หมายถึง กระบวนการหรือมาตรการที่ใช้เพื่อควบคุมการรวบรวม ใช้ เผยแพร่ หรือจัดเก็บข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อป้องกันมิให้ข้อมูลดังกล่าวถูกนำไปใช้ในทางที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล โดยมีจุดมุ่งหมายเพื่อรักษาสีทธิในความเป็นส่วนตัวของบุคคล

ในหลายประเทศได้มีการบัญญัติกฎหมายและมาตรฐานที่เกี่ยวข้อง เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) หรือ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลของประเทศไทย (PDPA) ซึ่งได้กำหนดหลักการพื้นฐานในการจัดการข้อมูลส่วนบุคคล เช่น การต้องขอความยินยอมก่อนเก็บรวบรวม การเปิดเผยวัตถุประสงค์การใช้งาน การจำกัดการเข้าถึง และการจัดเก็บข้อมูลไว้อย่างปลอดภัย [9]

สำหรับเทคโนโลยีการบันทึกชีวิต การออกแบบระบบที่สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลจึงเป็นสิ่งสำคัญ เช่น การประมวลผลข้อมูลภายในอุปกรณ์ของผู้ใช้ก่อน

ส่งออก การทำให้ข้อมูลไม่สามารถระบุตัวตนได้ (data anonymization) การใช้เทคนิคเบลอไบหน้า หรือการควบคุมสิทธิ์การเข้าถึงข้อมูล

การตระหนักถึงการปกป้องข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนออกแบบระบบ หรือที่เรียกว่า "Privacy by Design" จึงเป็นแนวทางที่ได้รับการสนับสนุนอย่างกว้างขวางในการพัฒนาเทคโนโลยีที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2.1.4 ความเป็นส่วนตัวของข้อมูล (Data Privacy) และการปกป้องความเป็นส่วนตัว (Privacy Protection)

ในงานโครงการที่เกี่ยวข้องกับอุปกรณ์บันทึกชีวิตและแพลตฟอร์มจัดเก็บข้อมูล [1] การบันทึกภาพถ่ายอาจรวมถึงใบหน้าของบุคคล ซึ่งถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ดังนั้น ประเด็นเรื่องความเป็นส่วนตัวและการปกป้องความเป็นส่วนตัวจึงเป็นประเด็นสำคัญที่เชื่อมโยงโดยตรงกับโครงการนี้

2.1.4.1 ความเป็นส่วนตัวของข้อมูล (Data Privacy)

ความเป็นส่วนตัวของข้อมูล (Data privacy) [8] หมายถึง สิทธิในการควบคุมการเข้าถึงและใช้ข้อมูลส่วนบุคคลของตน โดยเน้นที่การกำหนดขอบเขตและวัตถุประสงค์ของการเปิดเผยข้อมูล ซึ่งเป็นสิทธิขั้นพื้นฐานของบุคคลในสังคมดิจิทัล

2.1.4.2 การปกป้องความเป็นส่วนตัว (Privacy Protection)

การปกป้องความเป็นส่วนตัว (Privacy Protection) เป็นแนวคิดสำคัญในยุคที่ข้อมูลถูกเก็บและประมวลผลในรูปแบบดิจิทัล ซึ่งก่อให้เกิดความเสี่ยงต่อการละเมิดสิทธิส่วนบุคคล หลักการสำคัญของการปกป้องความเป็นส่วนตัว คือ การที่เจ้าของข้อมูลสามารถควบคุมข้อมูลของตนเอง และจำกัดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

Chi Liu และคณะ [9] จากมหาวิทยาลัยเทคโนโลยีซิดนีย์ (University of Technology Sydney) ได้กล่าวว่า ปัจจุบันการแชร์ภาพถ่ายในสื่อสังคมออนไลน์ได้รับความนิยมสูง และสามารถทำได้ง่ายทุกที่ทุกเวลา ทำให้ผู้ใช้สามารถโต้ตอบ

กับผู้อื่นได้ทันที ความสะดวกนี้ส่งผลให้เกิดความเสี่ยงต่อความเป็นส่วนตัว แม้แต่ภาพถ่ายที่ดูเหมือนไม่มีข้อมูลสำคัญก็อาจเปิดเผยข้อมูลอ่อนไหวได้

Chi Liu และคณะเสนอว่า เนื้อหาที่ปรากฏชัดเจนในภาพ เช่น ใบหน้า ทะเบียนรถ และป้ายสถานที่ จัดอยู่ในหมวดหมู่ความเป็นส่วนตัวที่สังเกตได้ (Observable Privacy) และเสนอแนวทางการปกป้องด้วยเทคนิคการทำให้เนื้อหาภาพคลุมเครือหรือสับสน (Visual Obfuscation) เช่น การเบลอภาพ (blurring) และการทำให้ภาพเป็นพิกเซล (pixelation) ซึ่งเป็นวิธีที่ได้รับความนิยมในการป้องกันการเปิดเผยข้อมูลที่ไม่พึงประสงค์ในภาพถ่าย

2.1.5 การประมวลผลที่ขอบเครือข่าย (Edge Computing)

ข้อมูลที่ได้จากอุปกรณ์บันทึกชีวิตมักถูกรวบรวมจากอุปกรณ์ที่อยู่ใกล้ตัวผู้ใช้งาน เช่น กล้องสวมใส่ เช่น เซอร์ตรวจจับสภาพแวดล้อม และอุปกรณ์เคลื่อนที่ L.-D. Tran และคณะ [2] ชี้ให้เห็นว่า ก่อนจะส่งข้อมูลเหล่านี้ไปยังระบบจัดเก็บ ควรมีการประมวลผลล่วงหน้าเพื่อตรวจสอบและคัดกรองข้อมูลที่เกี่ยวข้อง ทั้งในแง่ของคุณภาพข้อมูลและการรักษาความเป็นส่วนตัว

การประมวลผลที่ขอบเครือข่าย (Edge Computing) [10][11] คือแนวทางที่นำการวิเคราะห์และจัดเก็บข้อมูลไปดำเนินการในตำแหน่งที่ใกล้กับแหล่งกำเนิดข้อมูลมากที่สุด เช่น บนอุปกรณ์ IoT หรืออุปกรณ์ปลายทาง แทนที่จะส่งข้อมูลทั้งหมดไปยังศูนย์กลางหรือคลาวด์ การทำเช่นนี้ช่วยลดความล่าช้าในการประมวลผล (latency) และลดการใช้แบนด์วิดท์ (bandwidth) ซึ่งมีความสำคัญอย่างยิ่งในงานที่ต้องการการตอบสนองแบบเรียลไทม์ เช่น การตรวจจับใบหน้า หรือระบบยานพาหนะอัตโนมัติ

ข้อดีของการประมวลผลที่ขอบเครือข่าย ได้แก่

- การกระจายภาระงาน (Distributed Processing): ช่วยลดภาระของศูนย์ประมวลผลหลัก โดยแบ่งงานไปยังอุปกรณ์ใกล้แหล่งข้อมูล
- การตอบสนองแบบเรียลไทม์: เหมาะสำหรับงานที่ต้องการความเร็วในการประมวลผล เช่น การรู้จำใบหน้าหรือวัตถุ

- เพิ่มความปลอดภัยและความเป็นส่วนตัว: เนื่องจากข้อมูลสามารถประมวลผลในอุปกรณ์ edge ได้โดยไม่ต้องส่งข้อมูลที่ละเอียดอ่อนไปยังศูนย์กลาง

2.1.6 การประมวลผลที่คลาวด์ (Cloud Computing)

การประมวลผลที่คลาวด์ (cloud computing) [12] หมายถึงรูปแบบการให้บริการทรัพยากรด้านเทคโนโลยีสารสนเทศผ่านอินเทอร์เน็ต โดยผู้ใช้งานสามารถเข้าถึงบริการต่าง ๆ ได้ตามความต้องการ เช่น การประมวลผล พื้นที่จัดเก็บข้อมูล ฐานข้อมูล หรือแพลตฟอร์มพัฒนาแอปพลิเคชัน โดยไม่จำเป็นต้องจัดการกับโครงสร้างพื้นฐานหรือระบบฮาร์ดแวร์ด้วยตนเอง ผู้ให้บริการคลาวด์ที่ได้รับความนิยม เช่น Amazon Web Services (AWS), Microsoft Azure และ Google Cloud Platform

บริการคลาวด์สามารถแบ่งออกเป็น 3 ประเภทหลัก ได้แก่

2.1.6.1 Infrastructure as a Service (IaaS)

IaaS เป็นรูปแบบการให้บริการที่มอบทรัพยากรพื้นฐานด้านไอที เช่น เครื่องคอมพิวเตอร์เสมือน (virtual machines), พื้นที่จัดเก็บข้อมูล, และระบบเครือข่าย ผู้ใช้งานสามารถควบคุมและปรับแต่งทรัพยากรเหล่านี้ได้อย่างยืดหยุ่นตามความต้องการ ซึ่งเหมาะสำหรับองค์กรที่ต้องการควบคุมระบบอย่างละเอียดโดยไม่ต้องลงทุนกับฮาร์ดแวร์

2.1.6.2 Platform as a Service (PaaS)

PaaS เป็นบริการที่ให้แพลตฟอร์มสำหรับการพัฒนา ทดสอบ และปรับใช้แอปพลิเคชัน โดยผู้ใช้งานไม่ต้องจัดการกับโครงสร้างพื้นฐาน เช่น ระบบปฏิบัติการหรือเซิร์ฟเวอร์ ทำให้สามารถมุ่งเน้นไปที่การพัฒนาแอปพลิเคชันได้อย่างเต็มที่ ตัวอย่างของ PaaS เช่น Google App Engine และ Heroku

2.1.6.3 Software as a Service (SaaS)

SaaS เป็นการให้บริการซอฟต์แวร์ที่ใช้งานได้โดยตรงผ่านเว็บเบราว์เซอร์ โดยไม่จำเป็นต้องติดตั้งหรือตั้งค่าระบบ เช่น Gmail, Microsoft 365 หรือ Dropbox ผู้ใช้สามารถใช้งานซอฟต์แวร์ได้ทันที โดยไม่ต้องดูแลด้านเทคนิคหรือการบำรุงรักษา

การประมวลผลที่คลาวด์มีข้อดีหลายประการ ได้แก่

- ความคล่องตัว (Agility): ผู้ใช้สามารถเข้าถึงเครื่องมือและบริการด้านไอทีที่หลากหลาย และสามารถปรับเปลี่ยนทรัพยากรได้อย่างรวดเร็วตามความจำเป็น
- ความยืดหยุ่น (Scalability): สามารถขยายหรือลดขนาดของทรัพยากรได้ตามปริมาณงานหรือความต้องการใช้งานในแต่ละช่วงเวลา
- ความคุ้มค่า (Cost-efficiency): ลดต้นทุนการลงทุนล่วงหน้ากับฮาร์ดแวร์ โดยเปลี่ยนมาเป็นการจ่ายค่าบริการตามการใช้งานจริง

การประมวลผลที่คลาวด์จึงเป็นแนวทางที่เหมาะสมสำหรับระบบที่ต้องการความสามารถในการขยายตัวสูงและการเข้าถึงข้อมูลแบบเรียลไทม์ เช่น ระบบบันทึกชีวิตหรือการวิเคราะห์ข้อมูลขนาดใหญ่

2.2 เทคโนโลยีพื้นฐานที่เกี่ยวข้อง

2.2.1 ปัญญาประดิษฐ์ การเรียนรู้ของเครื่อง และการเรียนรู้เชิงลึก (Artificial Intelligence, Machine Learning, Deep Learning)

ในการศึกษานี้ มีการนำกระบวนการตรวจจับใบหน้าและทำการเบลอภาพมาใช้ ซึ่งอาศัยเทคนิคด้านการเรียนรู้ของเครื่อง (Machine Learning) เพื่อช่วยให้ระบบสามารถแยกแยะและประมวลผลภาพที่มีใบหน้าคนได้อย่างแม่นยำและอัตโนมัติ [13]

2.2.1.1 ปัญญาประดิษฐ์ (Artificial Intelligence: AI)

ปัญญาประดิษฐ์ (AI) คือ ระบบที่สามารถวิเคราะห์และประมวลผลข้อมูล โดยเลียนแบบพฤติกรรมกรคิด การเรียนรู้ และการตัดสินใจของมนุษย์ AI มีความสามารถในการเข้าใจบริบท สร้างคำตอบหรือคำแนะนำที่ชาญฉลาด และเรียนรู้จากข้อมูล ตัวอย่างการใช้งาน ได้แก่ ผู้ช่วยเสมือน เช่น Siri ที่สามารถตอบคำถามหรือควบคุมอุปกรณ์ต่าง ๆ ด้วยการประมวลผลภาษาธรรมชาติและการเรียนรู้จากบริบท

2.2.1.2 การเรียนรู้ของเครื่อง (Machine Learning: ML)

การเรียนรู้ของเครื่อง (ML) เป็นสาขาย่อยของ AI ที่มุ่งเน้นการพัฒนาอัลกอริทึมและโมเดลให้คอมพิวเตอร์สามารถเรียนรู้และพัฒนาตนเองจากข้อมูล โดยไม่ต้องเขียนโปรแกรมกำหนดพฤติกรรมไว้ล่วงหน้า รูปแบบการเรียนรู้ของเครื่องแบ่งออกเป็น 3 ประเภทหลัก

- การเรียนรู้แบบมีผู้สอน (Supervised Learning): ใช้ข้อมูลที่มีการป้ายกำกับเพื่อฝึกโมเดล
- การเรียนรู้แบบไม่มีผู้สอน (Unsupervised Learning): ใช้ข้อมูลที่ไม่มีป้ายกำกับเพื่อค้นหารูปแบบหรือโครงสร้างซ่อนเร้น
- การเรียนรู้แบบเสริมกำลัง (Reinforcement Learning): ระบบเรียนรู้จากการปฏิสัมพันธ์กับสิ่งแวดล้อม โดยได้รับรางวัลหรือบทลงโทษตามการกระทำ

ตัวอย่างการประยุกต์ใช้ เช่น การตรวจจับการฉ้อโกงในธุรกรรมธนาคาร โดยใช้เทคนิคการตรวจจับความผิดปกติ (Anomaly Detection)

2.2.1.3 การเรียนรู้เชิงลึก (Deep Learning: DL)

การเรียนรู้เชิงลึก (DL) เป็นแขนงหนึ่งของการเรียนรู้ของเครื่องที่ใช้โครงข่ายประสาทเทียมหลายชั้น (Deep Neural Networks) ในการเรียนรู้และประมวลผลข้อมูลที่ซับซ้อน โดยเลียนแบบการทำงานของเซลล์ประสาทในสมองมนุษย์ ระบบจะทำการแยกแยะข้อมูลออกเป็นหลายระดับชั้นเพื่อวิเคราะห์และสรุป

ผลลัพธ์ ตัวอย่างการใช้งานที่สำคัญ ได้แก่ ระบบจดจำใบหน้า (Facial Recognition) ซึ่งสามารถตรวจจับ เปรียบเทียบ และยืนยันตัวตนของบุคคลจากภาพใบหน้าได้อย่างแม่นยำ

2.2.2 การตรวจจับใบหน้า (Face Detection)

การตรวจจับใบหน้า (Face Detection) คือเทคนิคหนึ่งในสาขาการประมวลผลภาพและคอมพิวเตอร์วิทัศน์ (computer vision) ที่มีจุดมุ่งหมายในการระบุตำแหน่งของใบหน้ามนุษย์โดยอัตโนมัติในภาพถ่ายหรือวิดีโอ [14] เทคนิคนี้มักถูกใช้เป็นขั้นตอนเริ่มต้นในกระบวนการต่าง ๆ เช่น การจดจำใบหน้า การวิเคราะห์ใบหน้า และการเบลอใบหน้าเพื่อคุ้มครองความเป็นส่วนตัว ในบริบทของโครงการนี้ การตรวจจับใบหน้าถูกใช้ร่วมกับกระบวนการเบลอใบหน้า เพื่อป้องกันการระบุตัวตนของบุคคลในภาพถ่ายที่ได้จากการบันทึกชีวิต

L.-D. Tran และคณะ [2] ได้กล่าวว่าการประมวลผลภาพซึ่งรวมถึงการตรวจจับใบหน้า เป็นขั้นตอนสำคัญในการจัดการข้อมูลส่วนบุคคล โดยเฉพาะในการปรับปรุงคุณภาพภาพและการควบคุมความเป็นส่วนตัวก่อนจัดเก็บหรือแบ่งปันข้อมูลภาพต่อไปยังระบบอื่น

ในการดำเนินโครงการนี้ ได้มีการเลือกใช้เทคนิคการตรวจจับใบหน้าแบบ Haar Cascade ซึ่งสามารถอธิบายได้ดังนี้

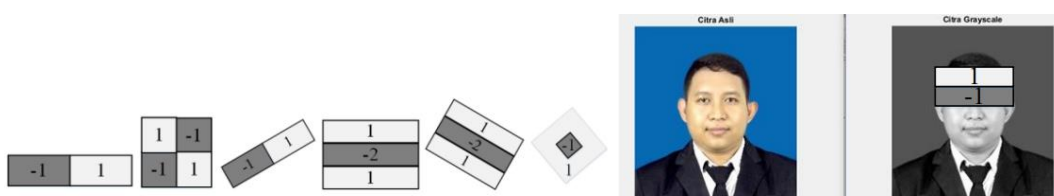
2.2.2.1 Haar Cascade

Haar Cascade เป็นอัลกอริทึมประเภท Machine Learning ที่ใช้สำหรับการตรวจจับวัตถุในภาพ โดยเฉพาะอย่างยิ่งการตรวจจับใบหน้า [15] เทคนิคนี้อาศัยการวิเคราะห์ลักษณะเฉพาะของภาพที่เรียกว่า Haar-like features ซึ่งเป็นรูปแบบของพิกเซลในลักษณะเรขาคณิต เช่น สีเหลี่ยมสีดำ-ขาว ที่ใช้เปรียบเทียบความแตกต่างของค่าความสว่าง (intensity) ระหว่างส่วนต่าง ๆ ของใบหน้า เช่น ดวงตา จมูก และปาก

ขั้นตอนการทำงานของ Haar Cascade ประกอบด้วยการฝึกโมเดลจำแนกลักษณะ (classifier) โดยใช้ชุดข้อมูลที่ประกอบด้วยภาพใบหน้า (positive images) และภาพที่ไม่มีใบหน้า (negative images) จากนั้นระบบจะใช้หน้าต่างการสแกน (sliding window) เคลื่อนที่ไปทั่วทั้งภาพเพื่อระบุบริเวณที่มีความ

เป็นไปได้ว่าเป็นใบหน้า (potential face) โดยพิจารณาจากผลของ classifier ที่ถูกฝึกมาแล้ว

เพื่อเพิ่มประสิทธิภาพและลดความผิดพลาดจากการตรวจจับผิด (false positives) ระบบจะทำการกรองใบหน้าที่ตรวจจับได้ โดยใช้เงื่อนไขเพิ่มเติม เช่น ขนาด ตำแหน่ง และรูปร่างของใบหน้า การตรวจจับใบหน้าโดยใช้ Haar Cascade จึงเป็นเครื่องมือสำคัญที่ช่วยสนับสนุนทั้งด้านความปลอดภัย และการปกป้องความเป็นส่วนตัวในส่วนตัวในโครงการนี้



ภาพที่ 2.1 แสดงการทำงานของ Haar-like features

2.2.3 การจดจำใบหน้า (Face Recognition)

การจดจำใบหน้า (Face Recognition) เป็นกระบวนการวิเคราะห์ใบหน้าที่ตรวจจับได้ เพื่อนำไประบุหรือยืนยันตัวบุคคลโดยเปรียบเทียบกับฐานข้อมูลที่มีอยู่ โดยระบบจะทำการวัดลักษณะเฉพาะบนใบหน้า เช่น ระยะห่างระหว่างดวงตา รูปร่างของคาง หรือจมูกและปาก เพื่อนำข้อมูลเหล่านี้แปลงเป็นตัวเลขในลักษณะของเวกเตอร์ และใช้เปรียบเทียบกับแบบจำลองที่มีอยู่ในฐานข้อมูล [34]

เทคโนโลยีนี้ถูกนำมาใช้ในหลากหลายบริบท เช่น ระบบรักษาความปลอดภัย ระบบเข้าใช้งานแบบไม่ต้องใช้รหัสผ่าน หรือการติดตามพฤติกรรมผู้ใช้งาน การจดจำใบหน้ามีบทบาทสำคัญในโครงการ lifelogging โดยใช้เป็นกลไกในการจัดการกับข้อมูลภาพถ่ายหรือวิดีโอที่อาจละเมิดความเป็นส่วนตัวของบุคคล

2.2.4 Infrastructure as Code (IaC)

Infrastructure as Code (IaC) คือแนวทางการบริหารจัดการโครงสร้างพื้นฐานของระบบคอมพิวเตอร์ผ่านโค้ด โดยไม่ต้องตั้งค่าแบบแมนนวล ช่วยให้สามารถควบคุม สร้าง หรือ

ปรับสภาพแวดล้อมได้อย่างอัตโนมัติ [16] ตัวอย่างเช่น การกำหนดค่าระบบปฏิบัติการ เครือข่าย และพื้นที่จัดเก็บ เพื่อให้ระบบสามารถ deploy ได้อย่างรวดเร็วและมีความสอดคล้องกัน

2.2.4.1 เครื่องมือ IaC สำหรับ Amazon Web Services (AWS)

- AWS CLI (Command Line Interface) : ใช้คำสั่งผ่าน command line เพื่อจัดการทรัพยากรบน AWS
- AWS SDK : ชุดเครื่องมือสำหรับนักพัฒนาในการเรียกใช้งาน AWS ผ่านภาษาโปรแกรม เช่น Python (Boto3)
- AWS CloudFormation : ใช้เทมเพลตในรูปแบบ JSON หรือ YAML เพื่อสร้างและจัดการทรัพยากรแบบอัตโนมัติ

2.2.4.2 เครื่องมือที่ไม่ขึ้นกับผู้ให้บริการ (Vendor-Neutral)

- Terraform: ใช้ภาษาการกำหนดค่าที่ชื่อว่า HCL เพื่อบริหารจัดการทรัพยากรบนคลาวด์หลายค่าย เช่น AWS, Azure, GCP

IaC ช่วยลดความผิดพลาดจากมนุษย์ เพิ่มความเร็วในการปรับใช้ และสามารถทำซ้ำสภาพแวดล้อมเดิมได้ง่ายโดยไม่ต้องตั้งค่าใหม่ทั้งหมด

2.2.5 การแฮช (Hash)

การแฮชคือกระบวนการเปลี่ยนข้อมูลใด ๆ ให้กลายเป็นรหัสที่มีความยาวคงที่ ซึ่งไม่สามารถย้อนกลับได้อย่างง่ายดาย เรียกว่าค่าแฮช (Hash Value) [35] เทคนิคนี้ถูกใช้ในงานที่ต้องการตรวจสอบความถูกต้องของข้อมูล หรือการเก็บข้อมูลที่ไม่ต้องการให้ถูกเปิดเผยโดยตรง เช่น รหัสผ่าน

2.2.5.1 ข้อมูลรับเข้า (Input)

สามารถเป็นข้อมูลใดก็ได้ เช่น ไฟล์หรือข้อความ ที่ต้องการย่อให้เป็นรหัสแฮช

2.2.5.2 ฟังก์ชันแฮช (Hash Function)

เป็นอัลกอริทึมที่ใช้สร้างค่าแฮช เช่น SHA-256 โดยข้อมูลอินพุตที่แตกต่างกันเพียงเล็กน้อยจะให้ค่าแฮชที่แตกต่างกันอย่างมาก

2.2.5.3 ผลลัพธ์แฮช (Hash Output)

คือค่าที่ได้จากกระบวนการแฮช มักอยู่ในรูปสตริงของอักขระและตัวเลข ความยาวของผลลัพธ์จะคงที่ ไม่สัมพันธ์กับความยาวของอินพุต ช่วยเสริมความปลอดภัยของระบบข้อมูล

2.3 เทคโนโลยีและเครื่องมือที่ใช้ในโครงการ

โครงการนี้ได้นำแนวคิดการประมวลผลที่ขอบเครือข่าย (Edge Computing) มาใช้ โดยใช้สมาร์ทโฟนเป็นอุปกรณ์เอดจ์ (Edge Device) ซึ่งอยู่ใกล้กับแหล่งบันทึกข้อมูล ทำหน้าที่รับภาพจากอุปกรณ์ต้นทางมาประมวลผลก่อนส่งต่อไปยังระบบคลาวด์ จึงจำเป็นต้องพัฒนาแอปพลิเคชันมือถือเพื่อรับภาพ ทำการประมวลผล และสื่อสารกับระบบคลาวด์อย่างมีประสิทธิภาพ

2.3.1 Mobile Application

Mobile Application [18] คือซอฟต์แวร์ที่ออกแบบมาเพื่อทำงานบนสมาร์ทโฟนหรือแท็บเล็ต โดยเฉพาะในระบบปฏิบัติการยอดนิยมอย่าง Android และ iOS แอปพลิเคชันสามารถเข้าถึงกล้อง, GPS, อินเทอร์เน็ต และฮาร์ดแวร์อื่น ๆ เพื่อให้บริการเฉพาะทาง เช่น การถ่ายภาพ วิเคราะห์ข้อมูล หรือติดต่อกับเซิร์ฟเวอร์ภายนอก

2.3.2 Wi-Fi

การสื่อสารระหว่างสมาร์ทโฟนกับระบบคลาวด์ใช้ Wi-Fi [20] ซึ่งเป็นมาตรฐาน IEEE 802.11 ในการเชื่อมต่อเครือข่ายไร้สาย ช่วยให้สามารถส่งข้อมูลภาพที่ผ่านการประมวลผลขึ้นคลาวด์ได้อย่างรวดเร็วและประหยัดต้นทุน

2.3.3 HTTP (Hypertext Transfer Protocol)

โปรโตคอล HTTP [23] เป็นกลไกการสื่อสารระหว่างฝั่งไคลเอนต์และเซิร์ฟเวอร์ โดยแบ่งออกเป็น

- HTTP Request [24]: ประกอบด้วย URL, HTTP Method, Header เพื่อร้องขอบริการจากเซิร์ฟเวอร์
- HTTP Response [24]: ส่งผลลัพธ์กลับมายังไคลเอนต์ ประกอบด้วย Status Code, Header และเนื้อหา

2.3.4 OpenCV (Open Source Computer Vision Library)

OpenCV [25, 26] คือไลบรารีโอเพ่นซอร์สสำหรับการประมวลผลภาพ เช่น การเบลอ การตรวจจับใบหน้า และการเพิ่มคุณภาพของวิดีโอ รองรับหลายภาษา (Python, C++, Java) และทำงานได้บนหลายแพลตฟอร์ม รวมถึง Android ซึ่งเป็นเป้าหมายหลักของโครงการนี้

2.3.5 ML Kit และเทคโนโลยีการตรวจจับใบหน้า

ML Kit [30, 31] เป็นเฟรมเวิร์คจาก Google ที่ให้บริการโมเดล Machine Learning สำหรับมือถือ โดยสามารถทำงานแบบ on-device เช่น ตรวจจับใบหน้า ตรวจจับรอยยิ้ม หรือการหลับตาได้แบบเรียลไทม์โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ต เพิ่มความเร็วและความเป็นส่วนตัวในการใช้งาน

2.3.6 FaceNet Model

FaceNet [32, 33] เป็นโมเดล Deep Learning จาก Google ที่เปลี่ยนภาพใบหน้าให้เป็นเวกเตอร์ 128 มิติในรูปแบบ embedding โดยใช้เทคนิค Triplet Loss ทำให้สามารถใช้ในการยืนยันตัวบุคคล (Verification) หรือจัดกลุ่มใบหน้าได้อย่างแม่นยำ รองรับการใช้งานผ่าน TensorFlow Lite บนอุปกรณ์มือถือ

2.3.7 การเปรียบเทียบระหว่าง ML Kit และ Haar Cascade

ML Kit ใช้โมเดล Deep Learning ที่มีความแม่นยำสูงและสามารถทำงานบนมือถือได้แบบเรียลไทม์ ขณะที่ Haar Cascade [36, 37, 38] เป็นอัลกอริทึมแบบคลาสสิกที่เบาและ

รวดเร็ว เหมาะกับอุปกรณ์ที่มีข้อจำกัดด้านทรัพยากร เช่น ESP32 หรือ Raspberry Pi การเลือกใช้งานขึ้นกับบริบทของโครงการ หากเน้นความแม่นยำบน Android ให้เลือก ML Kit หากเน้นความเบาและเร็ว ให้เลือก Haar Cascade

2.3.8 การเปรียบเทียบระหว่าง FaceNet และ DeepFace

FaceNet และ DeepFace ต่างก็เป็นโมเดลรู้จำใบหน้าที่ใช้ Deep Learning โดย DeepFace [39] จาก Facebook ใช้ CNN 9 ชั้นและ softmax classifier ในขณะที่ FaceNet [40] ใช้ Triplet Loss เพื่อสร้างเวกเตอร์ฝังตัว (embedding) โดยไม่ต้องฝึก classifier เพิ่มเติม

DeepFace เหมาะกับกรณีที่ต้องการความแม่นยำสูงแต่มีทรัพยากรเพียงพอ

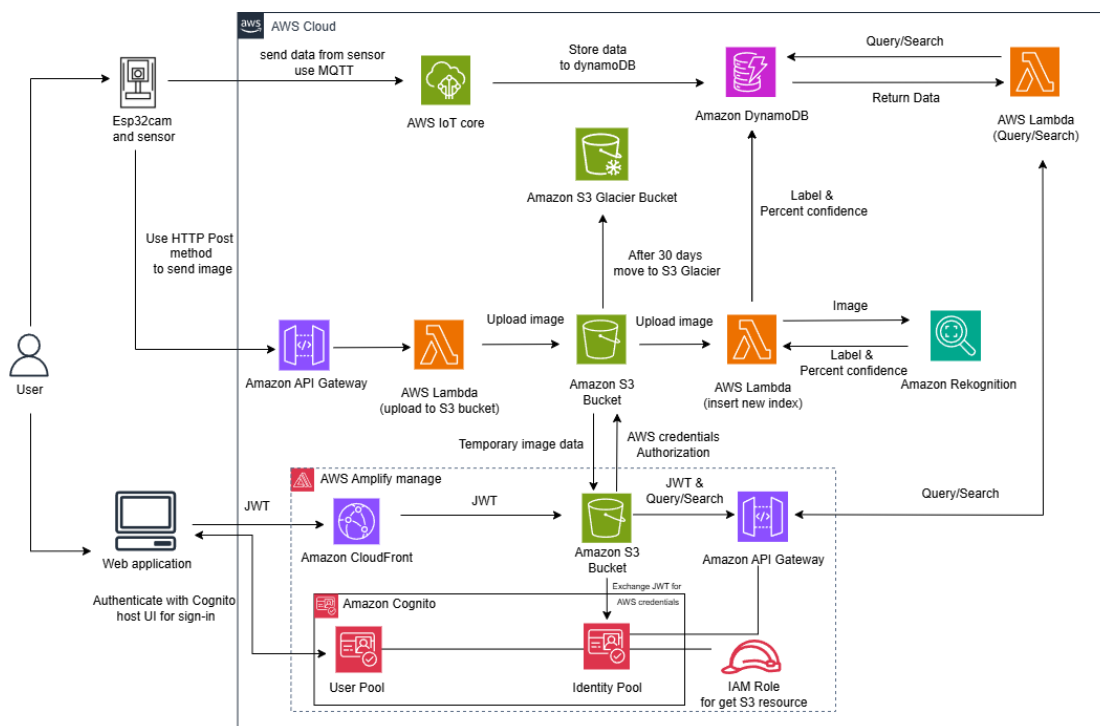
FaceNet เหมาะสำหรับงานที่ต้องการความยืดหยุ่นในการใช้งานและสามารถทำงานบนอุปกรณ์ที่มีข้อจำกัดได้

2.4 งานวิจัยที่เกี่ยวข้อง

ในบทนี้จะทบทวนวรรณกรรมที่เกี่ยวข้องกับการใช้อุปกรณ์เอดจ์ในการประมวลผลข้อมูล และแนวทางการปกป้องความเป็นส่วนตัวของข้อมูลจากภาพใบหน้า โดยเน้นงานที่เกี่ยวข้องกับอุปกรณ์สวมใส่ การตรวจจับใบหน้า และระบบรู้จำใบหน้าแบบกระจาย รวมถึงการใช้เทคนิคด้านความเป็นส่วนตัว เช่นการแฮชภาพและ Local Differential Privacy ซึ่งสามารถเปรียบเทียบประเด็นที่เกี่ยวข้องในตารางที่ 2.1

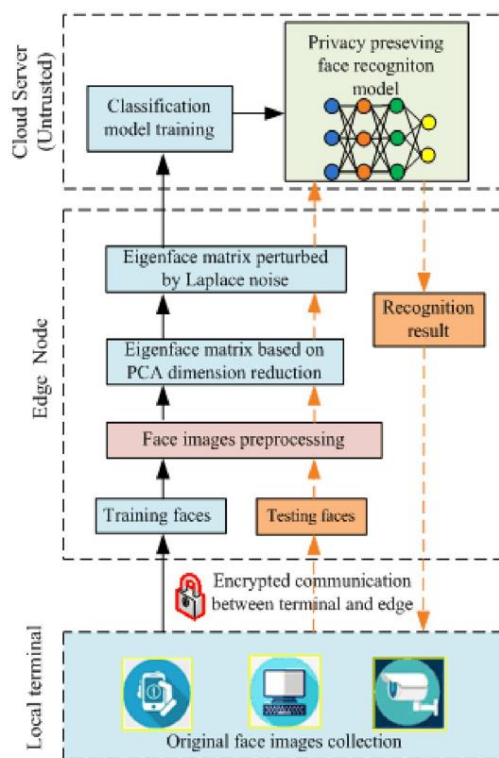
2.4.1 ด้านการปกป้องความเป็นส่วนตัวของข้อมูล

งานของปรานต์สกล และนฤพร [1] ได้พัฒนาอุปกรณ์บันทึกชีวิตราคาประหยัดที่สามารถถ่ายภาพและส่งขึ้นคลาวด์โดยอัตโนมัติ อย่างไรก็ตามไม่มีการประมวลผลภาพเพื่อป้องกันข้อมูลส่วนตัวก่อนส่ง เช่น กรณีที่ใบหน้าผู้อื่นปรากฏในภาพ อาจเกิดความเสี่ยงในการละเมิดสิทธิส่วนบุคคลหากข้อมูลถูกส่งไปยังบริการของบุคคลที่สาม



ภาพที่ 2.2 สถาปัตยกรรมของ Lifelog Ver.1

งานของ Xie et al. [28] ได้พัฒนาระบบ Edge-based Face Recognition (EFR) โดยเน้นความเป็นส่วนตัวของภาพใบหน้าที่ส่งจากอุปกรณ์เอดจ์ไปยังคลาวด์ ด้วยการใช้เทคนิค Local Differential Privacy (LDP) และ Principal Component Analysis (PCA) เพื่อลดมิติ และสร้างเวกเตอร์แทนภาพก่อนส่ง ลดความเสี่ยงจากการรั่วไหลของข้อมูลสำคัญในระหว่างการส่งผ่านเครือข่าย



ภาพที่ 2.3 Flow การทำงานของระบบ EFR [28]

ในขณะที่ Sun et al. [29] ได้นำเสนอระบบ iRyP ซึ่งเน้นการปกป้องสิทธิของบุคคลที่ไม่ต้องการถูกถ่ายภาพในที่สาธารณะ โดยใช้สมาร์ทโฟนเป็นอุปกรณ์เอดจ์ ทำการเปรียบเทียบใบหน้ากับฐานข้อมูลที่เข้ารหัสแบบ pHash และเบลอใบหน้าทันทีหากผู้ใช้ไม่อนุญาตให้บันทึกภาพ วิธีการนี้ช่วยป้องกันการละเมิดความเป็นส่วนตัวโดยไม่ต้องส่งภาพไปยังคลาวด์

2.4.2 ด้านการใช้อุปกรณ์เอดจ์เก็บข้อมูลและการประมวลผลที่ขอบเครือข่าย

Bangash [27] ได้เสนอระบบ IoMT ที่ใช้สมาร์ทโฟนเป็นอุปกรณ์เอดจ์ โดยผสมการทำงานกับเซนเซอร์ภายในและภายนอกเพื่อเก็บข้อมูลสุขภาพ เช่น GPS, อุณหภูมิ, การเต้นของหัวใจ ข้อมูลจะถูกส่งผ่าน MQTT ไปยัง AWS IoT Core และประมวลผลต่อบน AWS Analytics

Xie et al. [28] ใช้อุปกรณ์เอดจ์ไม่ระบุชนิด แต่เน้นการใช้ PCA เพื่อประมวลผลใบหน้า และลดภาระของระบบคลาวด์ โดยทำการเข้ารหัสเวกเตอร์ใบหน้าที่ก่อนส่งเสมอ

Sun et al. [29] ใช้สมาร์ทโฟนและสมาร์ตวอตช์เป็นอุปกรณ์เอดจ์ที่สามารถประมวลผลภาพได้โดยตรง ไม่พึ่งพาคLOUD และรองรับการประมวลผลนโยบายความเป็นส่วนตัวแบบเรียลไทม์

ตารางที่ 2.1 เปรียบเทียบงานวิจัยที่เกี่ยวข้อง

อ้างอิง	Infrastructure as Code	อุปกรณ์เอดจ์ (Edge device)	การใช้อุปกรณ์ เอดจ์ (Edge device) รวบรวมข้อมูล	การการประมวลผล ที่ขอบเครือข่าย (Edge Computing)	การปกปิดข้อมูล ที่อ่อนไหวใน รูปภาพ	การส่งข้อมูล ไปยังคลาวด์ (Cloud)
Lifelog V. 1 ปรานต์สกล และนฤพร [1]	-	-	-	-	-	จัดเก็บข้อมูล และ ประมวลผล บนคลาวด์ (Cloud)
Bangash [27]	-	โทรศัพท์เคลื่อนที่	เซนเซอร์และ กล้องภายใน โทรศัพท์เคลื่อนที่	-	-	ประมวลผล บนคลาวด์ (Cloud)
Xie, et al [28]	-	ไม่ระบุ	-	ประมวลผลรูปภาพ เพื่อเตรียมข้อมูล (Preprocessing) ปกป้องความเป็น ส่วนตัวของข้อมูล และลดแบนด์วิธ (Bandwidth)	รบกวนข้อมูล (perturbation) และเข้ารหัส ระหว่างส่ง ข้อมูล	ประมวลผล บนคลาวด์ (Cloud)
Sun, et al [29]	-	โทรศัพท์เคลื่อนที่ สมาร์ทวอตช์ และ คอมพิวเตอร์	กล้อง โทรศัพท์เคลื่อนที่	ประมวลผลรูปภาพ เพื่อปกป้องความ เป็นส่วนตัวของ ข้อมูล	เบลอน้ำมมนุษย์ ในรูปภาพ	-
Lifelog V. 2	มีเทมเพลต (Template) สำหรับสร้าง ทรัพยากร อัตโนมัติ	โทรศัพท์เคลื่อนที่	-	ประมวลผลรูปภาพ เพื่อปกป้องความ เป็นส่วนตัวของ ข้อมูล	เบลอน้ำมมนุษย์ ในรูปภาพ	จัดเก็บข้อมูล และ ประมวลผล บนคลาวด์ (Cloud)

บทที่ 3

วิธีการวิจัย

บทนี้นำเสนอแนวทางการออกแบบและพัฒนาระบบโดยมุ่งเน้นที่ ไปป์ไลน์สำหรับการจัดการภาพถ่าย (image processing pipeline) ที่ได้จากอุปกรณ์บันทึกชีวิต (lifelogging device) เพื่อการปกป้องความเป็นส่วนตัว (privacy protection) ของบุคคลที่อาจปรากฏในภาพ เช่น ใบหน้า ซึ่งถือเป็นข้อมูลส่วนบุคคลที่อ่อนไหว ทั้งนี้ยังคง รักษาอรรถประโยชน์ของข้อมูล (data utility retention) เพื่อให้สามารถนำไปใช้เป็นฐานข้อมูลสำหรับแอปพลิเคชันบันทึกและสืบค้นความทรงจำของผู้ใช้ในภายหลังได้อย่างมีประสิทธิภาพ

ไปป์ไลน์จัดการภาพถ่ายในโครงการนี้ถูกออกแบบภายใต้สมมติฐานว่าสมาร์ทโฟนของผู้ใช้ยังเป็นส่วนหนึ่งของ แพลตฟอร์มที่เชื่อถือได้ (trusted platform) ซึ่งอยู่ภายใต้การควบคุมของผู้ใช้โดยตรง ไปป์ไลน์ฯ จึงใช้สมาร์ทโฟนเป็นอุปกรณ์เอดจ์ (edge device) ในการประมวลผลภาพถ่ายเบื้องต้น ก่อนจะส่งออกไปจัดเก็บบนระบบคลาวด์ (cloud) ที่ใช้เป็นพื้นที่กลางในการจัดเก็บข้อมูลภาพเพื่อนำไปใช้ประโยชน์ต่อไป

บทที่สามของโครงงานฉบับนี้แบ่งออกเป็น 5 หมวด ดังนี้

3.1 ภาพรวมของโครงงาน

นำเสนอภาพรวมของระบบที่พัฒนาขึ้น โดยอธิบายองค์ประกอบหลัก เช่น อุปกรณ์บันทึกภาพ แอปพลิเคชันบนสมาร์ทโฟน และบริการคลาวด์ พร้อมแสดงลำดับขั้นตอนการทำงานของระบบแบบครบวงจร ตั้งแต่การบันทึกภาพ การถ่ายโอนข้อมูล การประมวลผลเพื่อปกป้องความเป็นส่วนตัว จนถึงการจัดเก็บข้อมูลบนคลาวด์ อธิบายส่วนประกอบของระบบที่ยังคงใช้องค์ประกอบของเวอร์ชันที่ 1 และส่วนที่พัฒนาต่อในเวอร์ชันที่ 2 รวมถึงอธิบายรายละเอียดของการสร้างเซอร์วิสบนคลาวด์โดยใช้สคริปต์อัตโนมัติ

3.2 การวิเคราะห์ขอบเขตและความต้องการของระบบ

อธิบายส่วนประกอบสำคัญและหน้าที่ของโมดูลต่างๆในระบบซึ่งประกอบด้วย โมดูลอุปกรณ์การรวบรวมและบันทึกข้อมูลชีวิตประจำวัน โมดูลเอดจ์ โมดูลการสำหรับจัดเก็บข้อมูลที่เก็บได้จากเซนเซอร์บนคลาวด์ โมดูลสำหรับจัดเก็บข้อมูลรูปภาพบนคลาวด์ โมดูลการวิเคราะห์รูปภาพบนคลาวด์ และเว็บแอปพลิเคชัน

3.3 ประเด็นที่น่าสนใจและสิ่งที่ท้าทาย

อธิบายประเด็นที่น่าสนใจและสิ่งที่ท้าทายในการทำโครงการนี้ เช่น ความท้าทายในการพัฒนาระบบเข้าโดยตามรอยการพัฒนาอุปกรณ์บันทึกชีวิตเวอร์ชัน 1 รวมถึงประเด็นที่น่าสนใจของการปกป้องความเป็นส่วนตัวและการเพิ่มรรถประโยชน์ในการใช้งานอุปกรณ์

3.4 ผลลัพธ์ที่คาดหวัง

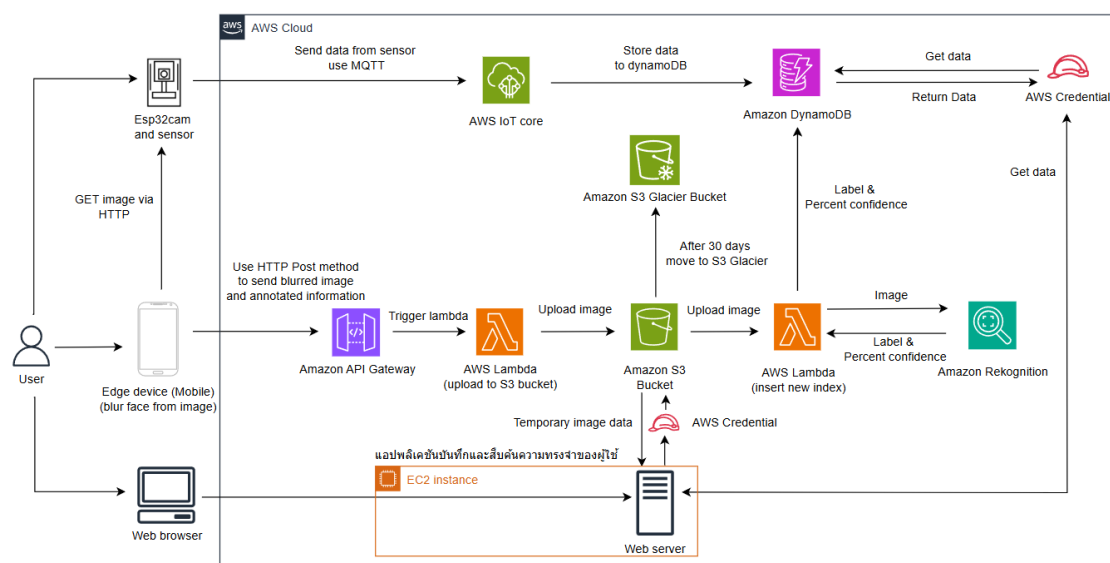
อธิบายผลลัพธ์ที่ผู้จัดทำคาดหวังในการจัดทำโครงการนี้ ไม่ว่าจะเป็นการพัฒนาสคริปต์อัตโนมัติ การปกป้องความเป็นส่วนตัว และการเพิ่มรรถประโยชน์ในการใช้งานอุปกรณ์

3.5 การดำเนินงาน

นำเสนอขั้นตอนการดำเนินงานตั้งแต่การพัฒนาสคริปต์อัตโนมัติ การพัฒนาแอปพลิเคชันในโทรศัพท์เคลื่อนที่ การพัฒนาฟังก์ชันสำหรับเพิ่มรรถประโยชน์ในการใช้งานในเว็บแอปพลิเคชัน จนถึงการออกแบบและดำเนินการทดลองต่าง ๆ

3.1 ภาพรวมของโครงการ

ภาพที่ 3.1 แสดงสถาปัตยกรรมของระบบในเวอร์ชันที่ 2 ที่พัฒนาต่อจากเวอร์ชันที่ 1 ซึ่งยังมีการใช้งานร่วมกับ Amazon Web Service อยู่ โดยข้อมูลจะถูกจัดเก็บไปยังเซิร์ฟเวอร์ของ AWS และมีเซิร์ฟเวอร์สำหรับการวิเคราะห์รูปภาพบนคลาวด์ที่เรียกใช้เพื่อทำ Object Detection ในรูปภาพที่ถูกส่งมาจัดเก็บเหมือนในเวอร์ชันที่ 1 มีเว็บแอปพลิเคชันบันทึกและสืบค้นความทรงจำของผู้ใช้ และมีส่วนที่เพิ่มเข้ามาคืออุปกรณ์เอดจ์ (Edge device) สำหรับประมวลผลรูปภาพเพื่อปกป้องความเป็นส่วนตัวของข้อมูล โดยมีรายละเอียดสถาปัตยกรรมโดยรวมดังนี้



ภาพที่ 3.1 แสดงสถาปัตยกรรมของระบบในเวอร์ชันที่ 2 ที่พัฒนาต่อจากเวอร์ชันที่ 1

3.1.1 ส่วนที่ยังใช้สถาปัตยกรรมเดิม

3.1.1.1 ส่วนที่รับข้อมูลเซนเซอร์ที่อุปกรณ์ส่งมา

อุปกรณ์ปลายทางส่งข้อมูลที่บ้านที่กักได้จากเซนเซอร์ ได้แก่ อุณหภูมิ, ความชื้น, ความเข้มแสงยูวี (UV), ละติจูดและลองจิจูด มายังส่วน AWS IoT Core โดยมีเกตเวย์ช่วยจัดการสำหรับโปรโตคอลเพื่อตรวจสอบว่าอุปกรณ์ปลายทางเป็นอุปกรณ์ที่เชื่อถือได้และสามารถสื่อสารอย่างปลอดภัยและมีประสิทธิภาพ มีการใช้ Rule เพื่อกำหนดเส้นทางของข้อมูลที่ถูกส่งมาที่ AWS IoT Core ให้ไปจัดเก็บยัง Amazon DynamoDB

3.1.1.2 ส่วนที่จัดเก็บข้อมูลที่ใช้เก็บข้อมูลรูปภาพ

เมื่ออุปกรณ์ปลายทางบ้านที่รูปภาพแล้วจะนำข้อมูลมาเก็บไว้ที่บริการเก็บข้อมูลบนคลาวด์ (Cloud) ของ AWS ดังนี้

(1) AWS S3 Standard

ใช้ในการเก็บข้อมูลรูปภาพ โดยชื่อของรูปภาพปรับเปลี่ยนจากเวอร์ชัน 1 คือจะเป็นชื่ออุปกรณ์ตามด้วยเวลาที่ถ่ายภาพ

(2) AWS S3 Glacier

ใช้ในการเก็บข้อมูลรูปภาพที่เก็บไว้นานเกิน 30 วันโดยไม่ถูกเรียกใช้แต่ยังสามารถนำออกมาใช้ได้ ในส่วนนี้ช่วยลดค่าใช้จ่ายเนื่องจากค่าบริการในส่วนนี้มีค่าบริการต่ำกว่า AWS S3 Standard

3.1.1.3 ส่วนฐานข้อมูลที่ใช้เก็บข้อมูลที่ได้จากเซนเซอร์

ในส่วนนี้จะเซอร์วิสบนคลาวด์ (Cloud service) ของ AWS ที่ชื่อว่า Amazon DynamoDB เป็นฐานข้อมูล NoSQL ที่ใช้จัดเก็บข้อมูลที่บ้านที่กักได้จากเซนเซอร์ทั้งหมดได้แก่ อุณหภูมิ, ความชื้น, ความเข้มแสงยูวี (UV), ตำแหน่งที่ตั้งละติจูดและลองจิจูด และข้อมูลที่ได้มาจาก Amazon Rekognition

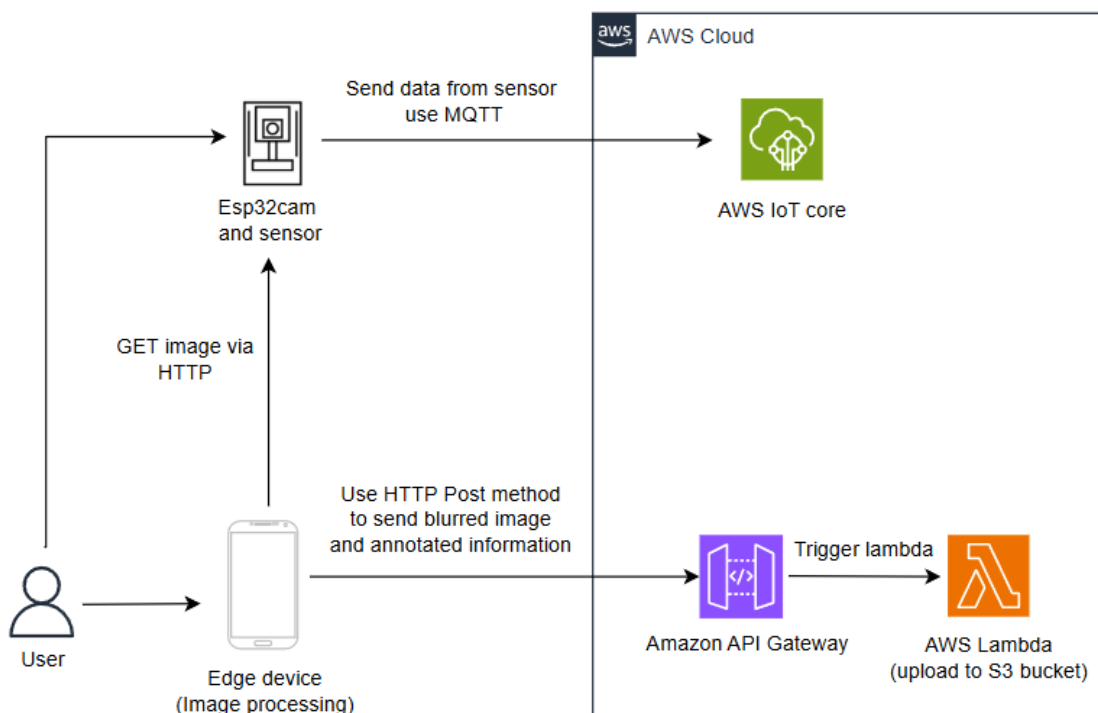
3.1.1.4 ส่วนของการตรวจจับสิ่งของภายในภาพ (Label Detection)

ส่วนนี้จะใช้เซอร์วิสบนคลาวด์ (Cloud service) ของ AWS ที่ชื่อว่า Amazon Rekognition เป็นบริการการวิเคราะห์ภาพและวิดีโอบนคลาวด์ (Cloud) บริการนี้ใช้การเรียนรู้เชิงลึก (Deep learning technology) ที่ได้รับการยอมรับแล้ว การทำงานคือเมื่อมีรูปภาพใหม่เข้ามาที่ Amazon S3 จะไปกระตุ้น AWS Lambda ให้เรียกใช้งาน Amazon Rekognition เพื่อตรวจจับสิ่งของภายในภาพ และส่งผลลัพธ์ของสิ่งที่ตรวจจับได้พร้อมทั้งชื่อรูปภาพไปจัดเก็บไว้ที่ Amazon DynamoDB

3.1.1.5 ส่วนของเว็บแอปพลิเคชัน (Web application)

เป็นส่วนที่จะทำให้ผู้ใช้สามารถเรียกดูรูปภาพและข้อมูลที่ผ่านการวิเคราะห์ทั้งในส่วนของกราฟข้อมูลและคำแนะนำการปฏิบัติตัว ผู้ใช้สามารถเรียกใช้หน้าเว็บผ่านทางเครือข่ายโดยใช้เว็บเบราว์เซอร์ (Web browser)

3.1.2 ส่วนที่เพิ่มเข้ามาในอุปกรณ์บันทึกชีวิตเวอร์ชัน 2 (Lifelog V.2)



ภาพที่ 3.2 สถาปัตยกรรมส่วนที่เพิ่มเข้ามาในเวอร์ชัน 2

ส่วนที่เพิ่มเข้ามาในเวอร์ชันนี้คืออุปกรณ์เอดจ์ (Edge device) ซึ่งก็คือ โทรศัพท์เคลื่อนที่ของผู้ใช้ โดยเมื่ออุปกรณ์ทำการบันทึกข้อมูล โทรศัพท์เคลื่อนที่ที่รับข้อมูลรูปภาพจากอุปกรณ์ผ่าน HTTP Protocol ข้อมูลส่วนที่บันทึกจากเซนเซอร์ได้แก่ อุณหภูมิ, ความชื้น, ความเข้มแสงยูวี (UV), ละติจูดและลองจิจูด จะถูกส่งไปยังคลาวด์ (Cloud) ผ่านโปรโตคอล MQTT ตามเดิมโดยมีรายละเอียดดังนี้

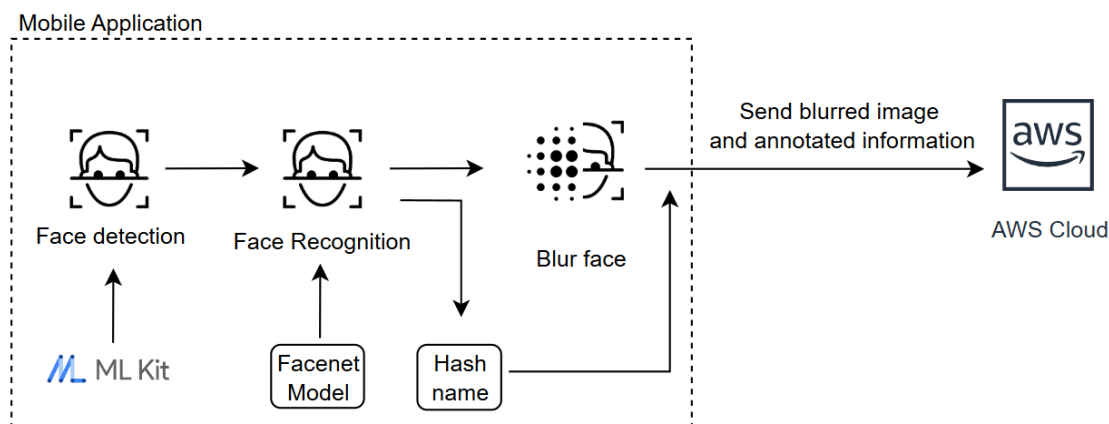
3.1.2.1 การส่งข้อมูลจากอุปกรณ์ไปยังโทรศัพท์เคลื่อนที่

อุปกรณ์บันทึกชีวิตที่ใช้คือ ESP32CAM ที่ตั้งเวลาไว้ให้เก็บข้อมูลตามเวลาที่กำหนดได้ และให้โทรศัพท์เคลื่อนที่ที่ตั้งเวลาให้ดึงข้อมูลจากอุปกรณ์ตามเวลาที่กำหนด โดยดึงข้อมูลผ่าน HTTP Protocol ผ่าน Endpoint ที่กำหนดไว้ในอุปกรณ์ ESP32CAM

หลังจากรับข้อมูลรูปภาพที่อุปกรณ์ปลายทางส่งมาเรียบร้อยแล้ว จะนำรูปภาพมาประมวลผลตรวจจับและเบลอบใบหน้า เพื่อปกป้องความเป็นส่วนตัวของข้อมูล จากนั้นจึงส่งภาพที่ประมวลผลแล้วไปยังคลาวด์ (Cloud) ผ่านโปรโตคอล HTTP เพื่อนำไปจัดเก็บหรือวิเคราะห์ต่อไป กระบวนการประมวลผลของแอปพลิเคชันมือถือมีรายละเอียดดังนี้

3.1.2.2 รายละเอียดของการการประมวลผลที่ขอบเครือข่าย (Edge Computing)

ในส่วนนี้จะพัฒนาแอปพลิเคชันมือถือขึ้นมาทำการการประมวลผลที่ขอบเครือข่าย (Edge Computing) เพื่อปกป้องความเป็นส่วนตัวของข้อมูลและเพิ่มประโยชน์ในการใช้งานอุปกรณ์ โดยการทำงานของแอปพลิเคชันมือถือมีรายละเอียดดังนี้



ภาพที่ 3.3 กระบวนการทำงานของการประมวลผลที่ขอบเครือข่าย (Edge Computing)

(1) การตรวจจับใบหน้า (Face detection) และเบลอใบหน้า

หลังจากอุปกรณ์มือถือรับข้อมูลรูปภาพมาแล้วจะทำการตรวจจับใบหน้าจากรูปภาพก่อนโดยใช้ไลบรารี ML Kit ที่มีโมเดลสำหรับตรวจจับใบหน้าจากรูปภาพมาช่วยทำงานในแอปพลิเคชันมือถือ ขั้นตอนการตรวจจับเริ่มจากการเรียกใช้ฟังก์ชันการตรวจจับใบหน้าของไลบรารี เมื่อพบใบหน้าแล้วจึงเบลอส่วนที่เป็นใบหน้านั้นผ่านการใช้ gaussian blur จากไลบรารี OpenCV หลังจากเบลอแล้วก็จะไปสู่ขั้นตอนถัดไป

(2) การจับคู่รูปภาพผ่านโมเดลจดจำใบหน้า

ในอุปกรณ์มือถือจะมีหน้าที่ให้ผู้ลงทะเบียนรูปภาพคนที่สนใจระบบจะตรวจจับใบหน้าจากภาพนั้นแล้วนำมาแปลงเป็นเวกเตอร์ของใบหน้าผ่านโมเดล FaceNet แล้วนำชื่อคนที่ผู้ลงทะเบียนและเวกเตอร์นี้ไปจัดเก็บไว้ในฐานข้อมูล

เมื่อมีรูปภาพถูกส่งมาจากอุปกรณ์และตรวจพบใบหน้าแล้วระบบจะนำใบหน้านั้นมาแปลงเป็นเวกเตอร์เช่นเดียวกับตอนลงทะเบียน แล้วจึงเอาเวกเตอร์นี้ไปเปรียบเทียบกับเวกเตอร์ที่อยู่ในฐานข้อมูลเพื่อจับคู่ใบหน้าที่ใกล้เคียงกัน หากพบว่าเป็นใบหน้าคนเดียวกันก็จะทำการแฮชชื่อคนที่ลงทะเบียนใบหน้านั้นไว้และแนบแฮชนั้นไปพร้อมกับชื่อรูปในขั้นตอนการส่งรูปภาพไปจัดเก็บบนคลาวด์

(3) การส่งรูปภาพไปจัดเก็บบนคลาวด์ (Cloud)

เมื่อเสร็จสิ้นกระบวนการตรวจจับใบหน้าและเบลอบใบหน้าเรียบร้อยแล้ว รูปภาพจะถูกส่งไปยังคลาวด์ (Cloud) เพื่อทำการจัดเก็บและนำไปวิเคราะห์ต่อผ่านโปรโตคอล HTTP แอปพลิเคชันมือถือจะใช้ยูอาร์แอล (URL) ของเซอร์วิสบนคลาวด์ (Cloud service) ซึ่งก็คือ API Gateway เพื่อส่งผ่านรูปภาพแลพไปกระตุ้นเซอร์วิสอีกตัวคือ AWS Lambda ใช้สำหรับนำรูปภาพเข้าไปเก็บในเซอร์วิสสำหรับจัดเก็บข้อมูล โดยแอปพลิเคชันมือถือจะใช้ HTTP POST Method ในการส่งรูปภาพ

3.1.3 รายละเอียดของสคริปต์อัตโนมัติ (Automate script)

การพัฒนาสคริปต์อัตโนมัติเพื่อสร้างทรัพยากรสำหรับจัดเก็บข้อมูลบนและวิเคราะห์ข้อมูลคลาวด์จะใช้บริการของ Amazon Web Service ที่ชื่อว่า AWS CloudFormation เป็นบริการสำหรับสร้างโมเดล จัดเตรียมและจัดการทรัพยากรโครงสร้างพื้นฐานในลักษณะอัตโนมัติและปลอดภัย โดยในโครงงานนี้จะสร้างเทมเพลตขึ้นมาสำหรับสร้างโครงสร้างพื้นฐานของระบบแบบอัตโนมัติซึ่งโครงสร้างพื้นฐานที่เทมเพลตสามารถสร้างได้มีดังนี้

3.1.3.1 การรับข้อมูลจากเซนเซอร์มาเก็บไว้ในฐานข้อมูล

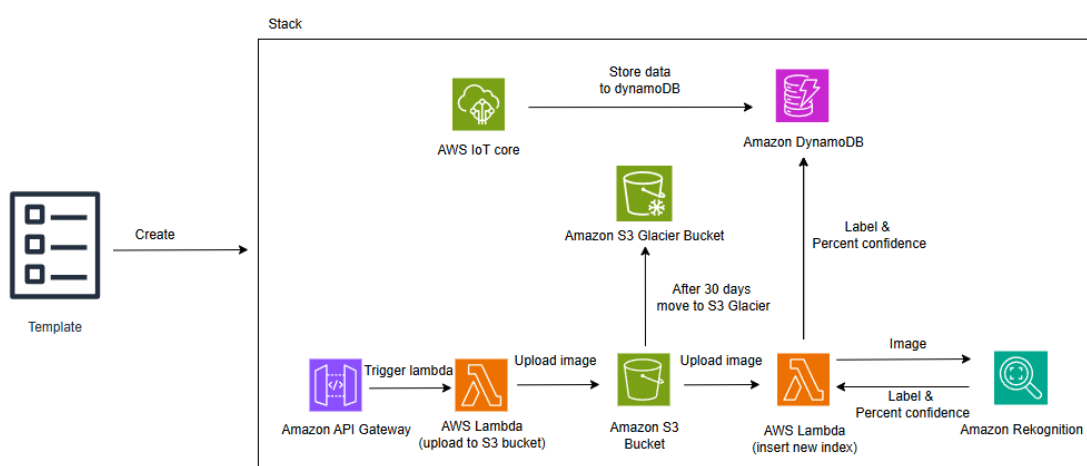
สร้างทรัพยากรสำหรับรับข้อมูลที่ได้จากเซนเซอร์ซึ่งก็คือบริการ AWS IoT Core และ สร้างฐานข้อมูลสำหรับจัดเก็บข้อมูลจากเซนเซอร์คือบริการ Amazon DynamoDB โดยตั้งค่าให้บริการ AWS IoT Core กำหนดกฎ (Rule) และหัวข้อ (Topic) สำหรับส่งข้อมูลไปเก็บที่บริการ Amazon DynamoDB

3.1.3.2 การรับข้อมูลรูปภาพจากอุปกรณ์เอดจ์ (Edge) มาจัดเก็บในที่เก็บข้อมูล

สร้างทรัพยากรสำหรับรับรูปภาพและนำไปจัดเก็บในที่จัดเก็บข้อมูลได้แก่ Amazon API Gateway, AWS Lambda และ Amazon S3 โดยตั้งค่าให้ฟังก์ชันภายในบริการ AWS Lambda นำรูปภาพที่ถูกส่งมาไปเก็บไว้ในถัง (Bucket) ของ Amazon S3 อย่างถูกต้อง

3.1.3.3 การวิเคราะห์รูปภาพและบันทึกผลลัพธ์ในฐานข้อมูล

สร้างทรัพยากรสำหรับการเรียกใช้งานบริการตรวจจับวัตถุได้แก่ สร้าง AWS Lambda และ Amazon Rekognition โดยตั้งค่าให้ฟังก์ชันภายในบริการ AWS Lambda เรียกใช้งานบริการ Amazon Rekognition เมื่อมีรูปภาพถูกเพิ่มเข้ามาในที่จัดเก็บข้อมูลซึ่งก็คือ Amazon S3 และนำผลลัพธ์ที่ได้จากโมเดลไปจัดเก็บไว้ใน Amazon DynamoDB อีกตารางหนึ่ง



ภาพที่ 3.4 รายละเอียดการสร้างโครงสร้างพื้นฐานผ่านเทมเพลต

3.2 การวิเคราะห์ขอบเขตและความต้องการของระบบ

โครงการการศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2 นี้มีหลายโมดูล (Module) ที่มีหน้าที่แตกต่างกันออกไปมาประกอบกันเป็นระบบที่สามารถบันทึกข้อมูลชีวิตประจำวัน (Lifelogging) ได้โดยที่ข้อมูลได้การปกป้องความเป็นส่วนตัวของข้อมูลเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล สามารถจัดเก็บข้อมูลที่บันทึกมาไว้บนระบบคลาวด์ (Cloud) ซึ่งมีเว็บแอปพลิเคชันที่สามารถเรียกดูข้อมูลได้ตลอดเวลา และมีการตรวจจับวัตถุในรูปภาพเพื่อนำมาเป็นฟีเจอร์การค้นหาในเว็บแอปพลิเคชัน โดยมีโมดูล (Module) ดังนี้

3.2.1 โมดูลอุปกรณ์การรวบรวมและบันทึกข้อมูลชีวิตประจำวัน

อุปกรณ์ที่ใช้สำหรับบันทึกข้อมูลยังใช้ฮาร์ดแวร์รุ่นเดียวกันเวอร์ชัน 1 อยู่

3.2.1.1 ส่วนประกอบสำคัญ

มีส่วนประกอบสำคัญคือกล้องและเซนเซอร์ต่าง ๆ ประกอบด้วย

(1) โมดูลกล้อง



ภาพที่ 3.5 โมดูลไมโครคอนโทรลเลอร์ ESP32-CAM

โมดูลไมโครคอนโทรลเลอร์ ESP32-CAM จากภาพที่ 3.5 เป็นโมดูลกล้องขนาดเล็กโดยใช้ชิป ESP32-S มี WiFi และบลูทูธเวอร์ชัน 4.2 ทำให้เหมาะสำหรับงานที่ต้องใช้งานอินเทอร์เน็ต ออกแบบมาสำหรับการเก็บข้อมูลภาพ มาพร้อมกับโมดูลกล้อง OV2640 ที่มีความละเอียด 2 ล้านพิกเซล (2MP) รองรับการบันทึกภาพ JPEG หรือ BMP ที่ความละเอียดสูงสุด 1632 x 1232 พิกเซล

(2) เซนเซอร์วัดอุณหภูมิและความชื้น



ภาพที่ 3.6 เซนเซอร์วัดอุณหภูมิและความชื้น SHT21

เซนเซอร์วัดอุณหภูมิและความชื้น SHT21 สามารถวัดอุณหภูมิได้ในช่วง -40 ถึง 125 องศาเซลเซียส และความชื้นที่ 0-100% อัตรารีเฟรชวัดความชื้น 8 วินาที

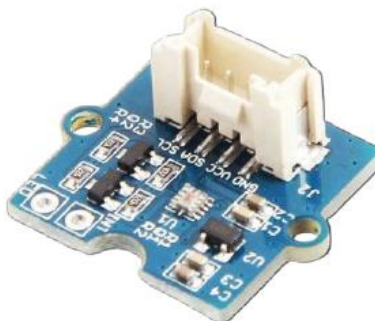
(3) เซนเซอร์เก็บข้อมูลตำแหน่งบนผิวโลก



ภาพที่ 3.7 โมดูลจีพีเอส (GPS) GY-NEO-6M Ublox

โมดูลจีพีเอส (GPS) GY-NEO-6M Ublox สามารถเชื่อมต่อกับไมโครคอนโทรลเลอร์ได้หลายประเภท ผ่านทาง Serial UART ความเร็วที่ 9600 สามารถเพิ่มได้ และตำแหน่งอัปเดตตลอดทุกๆ 1 วินาที สามารถตั้งค่าให้เร็วกว่านี้ได้ การทำงานเมื่อโมดูลจับสัญญาณได้จะขึ้นไฟกระพริบ

(4) เซนเซอร์วัดความเข้มของรังสีอัลตราไวโอเล็ต



ภาพที่ 3.8 เซนเซอร์วัดความเข้มของรังสีอัลตราไวโอเล็ต Grove – Sunlight Sensor

เซนเซอร์วัดความเข้มของรังสีอัลตราไวโอเลต Grove – Sunlight Sensor เป็นเซนเซอร์ที่สามารถตรวจจับแสงยูวี (UV) แสงที่ตามองเห็นได้ และแสงอินฟราเรดที่มีขนาดเล็ก

(5) โมดูลสำหรับชาร์จแบตเตอรี่



ภาพที่ 3.9 โมดูลสำหรับชาร์จแบตเตอรี่ TP4056 1A USB-C Charger

โมดูลชาร์จแบตเตอรี่แบบลิเทียม รับไฟชาร์จ 5 โวลต์ จากหัวต่อแบบยูเอสบีซี (USB TYPE-C) กระแสชาร์จสูงสุด 1A ตัดไฟเมื่อชาร์จเต็มที่ 4.2 โวลต์ พร้อมวงจรป้องกันแบตเตอรี่จ่ายไฟมากเกินไป มีไฟแจ้งสถานะการชาร์จ

(6) แบตเตอรี่



ภาพที่ 3.10 แบตเตอรี่ 3.7 โวลต์ 5000 มิลลิแอมป์ชั่วโมงโมโนลิเทียมโพลิเมอร์

แบตเตอรี่ 3.7 โวลต์ 5000 มิลลิแอมป์ชั่วโมงลิเทียมโพลิเมอร์ สามารถเก็บประจุไฟได้นานและคายประจุน้อย สามารถใช้พลังงานจนหมดได้ของเหลวด้านในเป็นเจล ไม่ติดไฟ

3.2.1.2 หน้าทีของโมดูล

โมดูลนี้มีหน้าที่สำคัญในการบันทึกข้อมูลชีวิตประจำวันของผู้ใช้พบเจอ จากกล้องและเซนเซอร์ต่างๆ ส่งข้อมูลรูปภาพไปยังอุปกรณ์เอดจ์ (Edge device) และส่งข้อมูลที่บันทึกได้จากเซนเซอร์ไปยังคลาวด์ (Cloud) เพื่อทำกระบวนการต่อไป

3.2.2 โมดูลเอดจ์

3.2.2.1 ส่วนประกอบสำคัญ

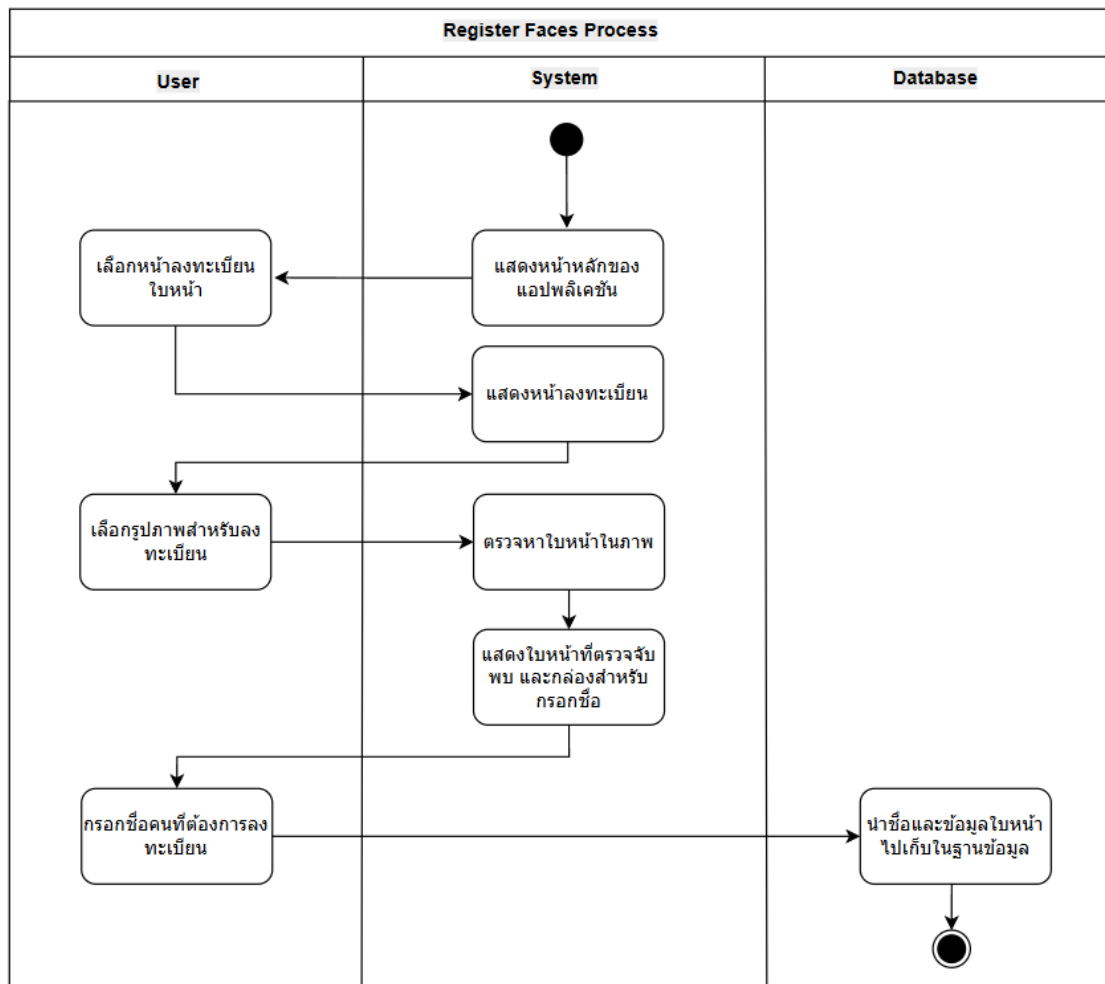
มีอุปกรณ์เอดจ์ (Edge device) ในที่นี้คือโทรศัพท์เคลื่อนที่สมาร์ทโฟน โดยประมวลผลผ่านแอปพลิเคชันมือถือมีฟังก์ชันการตรวจจับใบหน้าและเบลอใบหน้า หากตรวจพบ การจดจำใบหน้า และฟังก์ชันการส่งรูปภาพไปยังคลาวด์ (Cloud)

3.2.2.2 หน้าทีของโมดูล

โมดูลนี้มีหน้าที่รับรูปภาพที่ถ่ายได้จากอุปกรณ์บันทึก เพื่อนำรูปภาพมาวิเคราะห์ตรวจจับใบหน้าและเบลอใบหน้าในรูปภาพ จับคู่ใบหน้าผ่านการจดจำใบหน้า จากนั้นส่งรูปภาพที่เบลอแล้วไปยังคลาวด์ (Cloud) เพื่อทำกระบวนการต่อไป

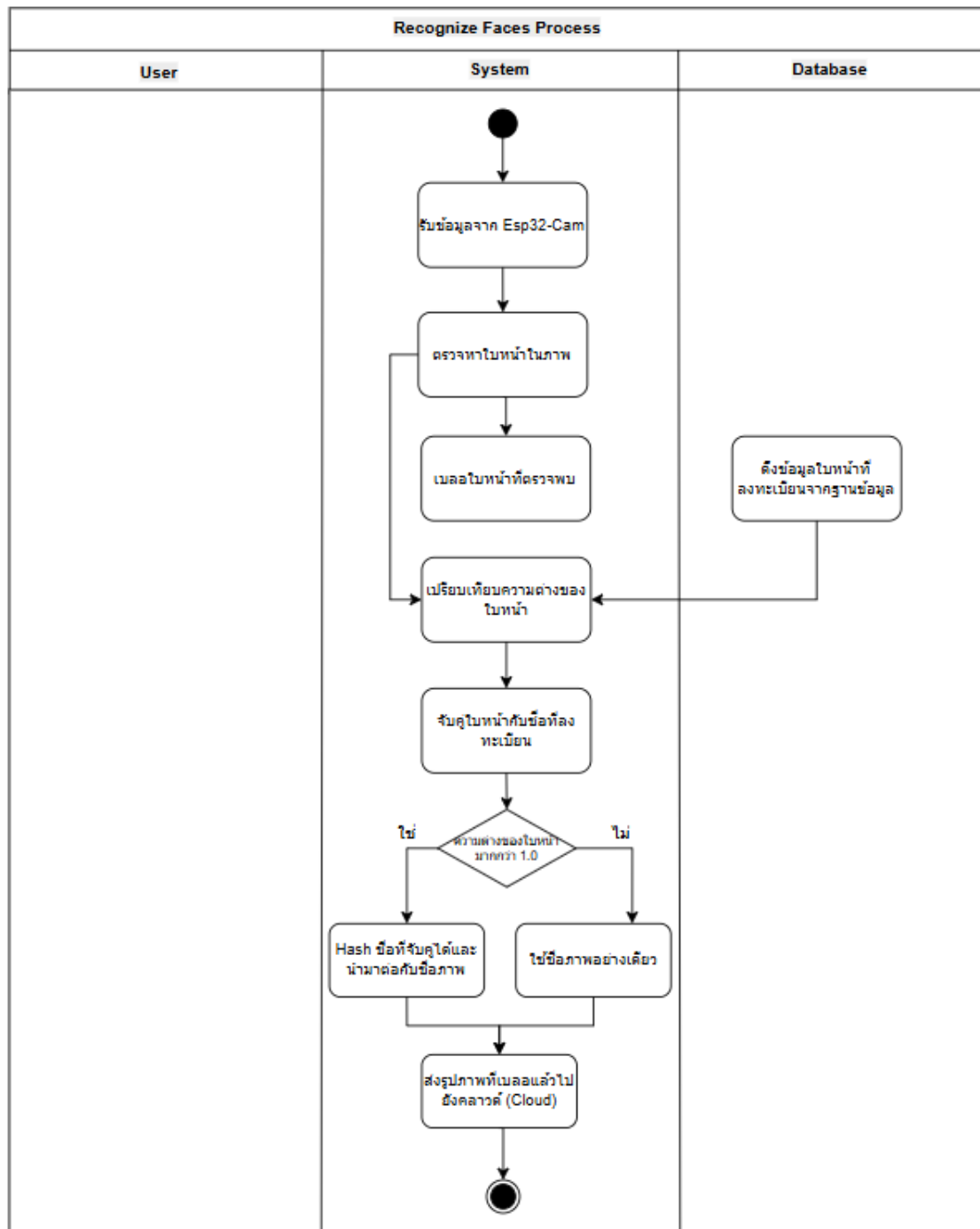
3.2.2.3 แผนภาพกิจกรรมของระบบ (Activity Diagram)

Activity Diagram ของฟังก์ชันลงทะเบียนใบหน้าในโทรศัพท์เคลื่อนที่



ภาพที่ 3.11 Activity Diagram ของฟังก์ชันลงทะเบียนใบหน้าในโทรศัพท์เคลื่อนที่

Activity Diagram ของฟังก์ชันการตรวจจับและจดจำใบหน้าในโทรศัพท์เคลื่อนที่



ภาพที่ 3.12 Activity Diagram ของฟังก์ชันการตรวจจับและจดจำใบหน้าในโทรศัพท์เคลื่อนที่

3.2.3 โมดูลสำหรับจัดเก็บข้อมูลที่เก็บได้จากเซนเซอร์บนคลาวด์

3.2.3.1 ส่วนประกอบสำคัญ

มีบริการบนคลาวด์ (Cloud) คือ AWS IoT Core สำหรับรับข้อมูลที่เก็บได้จากเซนเซอร์และกำหนดปลายทางของข้อมูลในการส่งไปเก็บยังฐานข้อมูล และบริการอีกตัวเป็นฐานข้อมูลสำหรับจัดเก็บข้อมูลคือ Amazon DynamoDB

3.2.3.2 หน้าที่ของโมดูล

โมดูลนี้มีหน้าที่รับข้อมูลที่ถูกส่งมาจากเซนเซอร์และนำข้อมูลไปเก็บไว้ยังฐานข้อมูล

3.2.4 โมดูลสำหรับจัดเก็บข้อมูลรูปภาพบนคลาวด์

3.2.4.1 ส่วนประกอบสำคัญ

มีบริการบนคลาวด์ (Cloud) คือ AWS Lambda สำหรับนำข้อมูลรูปภาพไปเก็บไว้ยังบริการจัดเก็บข้อมูลชื่อ Amazon S3

3.2.4.2 หน้าที่ของโมดูล

โมดูลนี้มีหน้าที่รับรูปภาพที่ถูกส่งมาจากอุปกรณ์เอดจ์ (Edge device) จากนั้นนำรูปภาพไปเก็บไว้ยังที่เก็บข้อมูลบนคลาวด์ (Cloud)

3.2.5 โมดูลการวิเคราะห์รูปภาพบนคลาวด์

3.2.5.1 ส่วนประกอบสำคัญ

มีบริการบนคลาวด์ (Cloud) คือ AWS Lambda สำหรับเรียกใช้งานบริการอีกตัวหนึ่งซึ่งใช้สำหรับวิเคราะห์ภาพคือ Amazon Rekognito

3.2.5.2 หน้าที่ของโมดูล

ใช้รูปภาพที่ถูกเพิ่มเข้ามาในบริการ Amazon S3 ไปวิเคราะห์ ตรวจสอบจับวัตถุ ในภาพและนำผลลัพธ์ที่ได้จากการตรวจจับไปเก็บไว้ในฐานข้อมูล

3.2.6 เว็บแอปพลิเคชัน (Web application)

3.2.6.1 ส่วนประกอบสำคัญ

เว็บแอปพลิเคชันมีส่วนประกอบที่สำคัญมากมายทั้งส่วนที่ใช้สำหรับดึง ข้อมูลรูปภาพมาแสดงผล ส่วนที่ใช้สำหรับดึงข้อมูลที่ได้จากเซนเซอร์และข้อมูลที่ได้ จากการตรวจจับวัตถุ ฟังก์ชันการค้นหา และส่วนที่ใช้สำหรับยืนยันตัวตนในการ เข้าใช้งานเว็บแอปพลิเคชัน

3.2.6.2 หน้าที่ของโมดูล

เว็บแอปพลิเคชันใช้ข้อมูลทั้งรูปภาพและข้อมูลจากเซนเซอร์รวมถึงผลลัพธ์ ของการตรวจจับวัตถุ จากฐานข้อมูลบนคลาวด์ (Cloud) มาแสดงผลให้ผู้ใช้งาน สามารถติดตามข้อมูลของตนเองได้อย่างสะดวก

3.3 ประเด็นที่น่าสนใจและสิ่งที่ท้าทาย

การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูลเวอร์ชัน 2 มี ประเด็นที่น่าสนใจและสิ่งที่ท้าทาย 3 ประเด็นดังนี้

- การดำเนินงานพัฒนาระบบซ้ำโดยการสร้างใหม่ (Rebuild) โดยตามรอยการ พัฒนาอุปกรณ์บันทึกชีวิตเวอร์ชัน 1 ด้วยความซับซ้อนของโครงสร้างระบบทำให้สร้างระบบใหม่ตามได้ยาก ใช้เวลานาน และอาจเกิดความผิดพลาด จึงได้นำ แนวคิดการพัฒนาโค้ดในการกำหนดค่าและจัดการโครงสร้างพื้นฐานของระบบ (Infrastructure as Code) มาใช้งาน แต่ก็อาจจะมีผลกระทบตรงที่ต้อง เรียนรู้และเข้าใจโครงสร้างของระบบเป็นอย่างดีรวมถึงแพลตฟอร์มและ เครื่องมือที่ใช้ที่มีความซับซ้อน จึงจะสามารถพัฒนาสคริปต์อัตโนมัติสำหรับ สร้างโครงสร้างระบบได้
- เรื่องของการปกป้องความเป็นส่วนตัวของข้อมูลด้วยการบล็อกใบหน้า การบล็อก ใบหน้าต้องใช้การตรวจจับใบหน้า ซึ่งการจะรันโมเดลอาจมีข้อจำกัดที่ตัว

อุปกรณ์ไมโครคอนโทรลเลอร์ที่มีทรัพยากรจำกัด ทำให้มีการนำการประมวลผลที่ขอบเครือข่าย (Edge computing) มาใช้ ซึ่งในกรณีนี้ใช้โทรศัพท์เคลื่อนที่มาใช้เป็นอุปกรณ์ (Edge device) เนื่องจากเป็นอุปกรณ์ที่อยู่ใกล้ตัวผู้ใช้อยู่แล้ว และมาพ่วงในการประมวลผล แต่ในขณะเดียวกันก็มีความท้าทายในเรื่องการพัฒนาแอปพลิเคชันมือถือ (Mobile application) เป็นเรื่องใหม่ทำให้ต้องใช้ความพยายามในการเรียนรู้สูง

- การเพิ่มรรถประโยชน์ที่ได้จากการใช้งานอุปกรณ์จากการใช้การจดจำใบหน้า ศึกษาผลกระทบระหว่างการเพิ่มจำนวนคนลงทะเบียนกับประสิทธิภาพในการจดจำใบหน้าซึ่งส่งผลต่อรรถประโยชน์ในการใช้งานอุปกรณ์

3.4 ผลลัพธ์ที่คาดหวัง

ผู้จัดทำคาดหวังว่าจะสามารถพัฒนาสคริปต์อัตโนมัติที่สามารถสร้างโครงสร้างพื้นฐานของระบบแบบอัตโนมัติได้ โดยที่ระบบที่ถูกสร้างโดยสคริปต์นี้สามารถทำงานทุกอย่างได้เหมือนเดิม ผู้ใช้สามารถนำสคริปต์นี้ไปใช้สร้างโครงสร้างพื้นฐานของตนเองได้อย่างสะดวก

และคาดหวังว่าจะสามารถพัฒนาอุปกรณ์บันทึกชีวิตที่สามารถส่งรูปภาพที่ถ่ายได้มายังโทรศัพท์เคลื่อนที่ที่เป็นอุปกรณ์เอดจ์ (Edge device) สำหรับสำหรับวิเคราะห์ใบหน้ามนุษย์จากรูปภาพและทำการเบลอใบหน้า เพื่อปกป้องความเป็นส่วนตัวของข้อมูลและป้องกันการละเมิดความเป็นส่วนตัว ส่วนตัว สามารถนำโมเดลการจดจำใบหน้ามาใช้ในการจับคู่ใบหน้าได้แม่นยำเพื่อเพิ่มประโยชน์ในการใช้อุปกรณ์ และอุปกรณ์มือถือสามารถส่งภาพที่ประมวลผลแล้วไปจัดเก็บยังคลาวด์ (Cloud) ได้ โดยที่ผู้ใช้ได้รับประโยชน์จากการใช้งานในการค้นหารูปภาพผ่านชื่อคนที่ลงทะเบียนไว้

3.5 การดำเนินงาน

3.5.1 ส่วนอุปกรณ์ฮาร์ดแวร์

อุปกรณ์ที่ใช้ยังคงเป็นอุปกรณ์ที่พัฒนาในเวอร์ชันที่ 1 ที่ผ่านมาได้มีการศึกษาการทำงานของอุปกรณ์จากเวอร์ชันที่ 1 เพื่อทำความเข้าใจการทำงานของฟังก์ชันต่างๆภายในอุปกรณ์ โดยใช้อุปกรณ์บันทึกชีวิตในส่วนของฮาร์ดแวร์ที่ถูกพัฒนาขึ้นในเวอร์ชันที่ 1 มาศึกษา



ภาพที่ 3.13 อุปกรณ์สำหรับการบันทึกชีวิตในเวอร์ชันที่ 1

3.5.2 การพัฒนาสคริปต์อัตโนมัติ (Automate script)

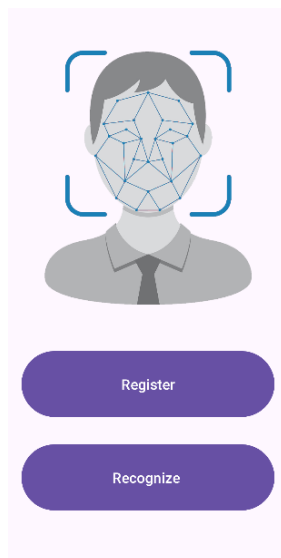
ได้ใช้บริการของ AWS ที่ชื่อว่า AWS CloudFormation ในการสร้างทรัพยากรสำหรับจัดเก็บรูปภาพ ข้อมูลจากเซนเซอร์ การประมวลผลรูปภาพบนคลาวด์ สำหรับใช้งานกับอุปกรณ์



ภาพที่ 3.14 แสดงเทมเพลตที่ถูกสร้างโดย AWS CloudFormation

3.5.3 ส่วนของซอฟต์แวร์ในโทรศัพท์เคลื่อนที่

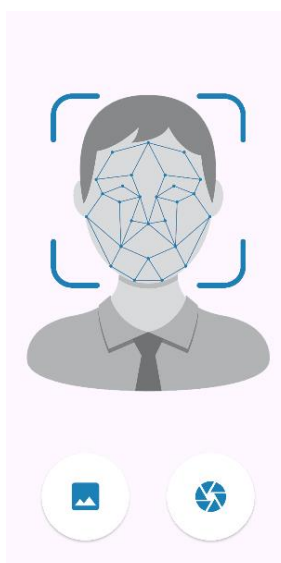
3.5.3.1 หน้าหลักของแอปพลิเคชัน



ภาพที่ 3.15 แสดงหน้าหลักของแอปพลิเคชัน

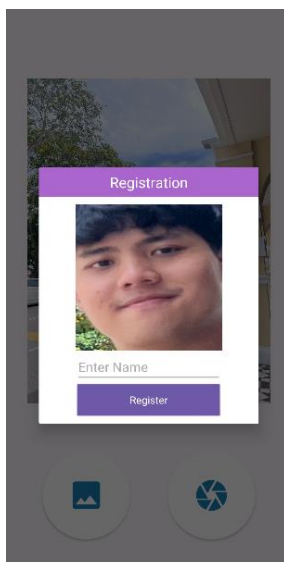
ภาพแสดงหน้าหลักของแอปพลิเคชันที่ผู้ใช้สามารถเลือกจะไปที่หน้าลงทะเบียนใบหน้าหรือหน้าการจดจำใบหน้าได้

3.5.3.2 หน้าลงทะเบียนใบหน้า



ภาพที่ 3.16 แสดงหน้าลงทะเบียนใบหน้าของแอปพลิเคชัน

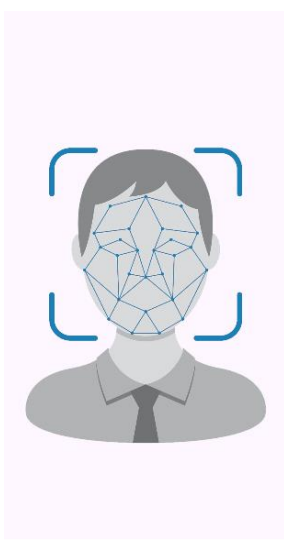
ในหน้าลงทะเบียนใบหน้าผู้ใช้สามารถเลือกใช้รูปที่ลงทะเบียนได้จากรูปภาพที่มีอยู่ในแกลลอรี่หรือถ่ายจากกล้อง



ภาพที่ 3.17 แสดงหน้าต่างให้ผู้ใช้กรอกชื่อคนที่ลงทะเบียน

เมื่อผู้ใช้เลือกรูปภาพที่ต้องการลงทะเบียนแล้วระบบจะแสดงหน้าต่างเพื่อแสดงถึงใบหน้าที่ตรวจจับได้ในภาพและกล้องให้ผู้ใช้กรอกชื่อของใบหน้าที่ลงทะเบียน

3.5.3.3 หน้าการทำงานหลักสำหรับดึงข้อมูลจากอุปกรณ์และจดจำใบหน้า



ภาพที่ 3.18 แสดงหน้าการทำงานหลักสำหรับดึงข้อมูลจากอุปกรณ์และจดจำใบหน้า

ภาพแสดงหน้าการทำงานหลักสำหรับดึงข้อมูลจากอุปกรณ์ เพื่อนำมาตรวจจับใบหน้าและเบลอ และจับคู่ใบหน้าและแฮชชื่อคนที่ลงทะเบียน ในหน้านี้ หากยังไม่รู้ภาพในเซิร์ฟเวอร์ของอุปกรณ์ แอปพลิเคชันก็จะไม่แสดงรูปอะไร



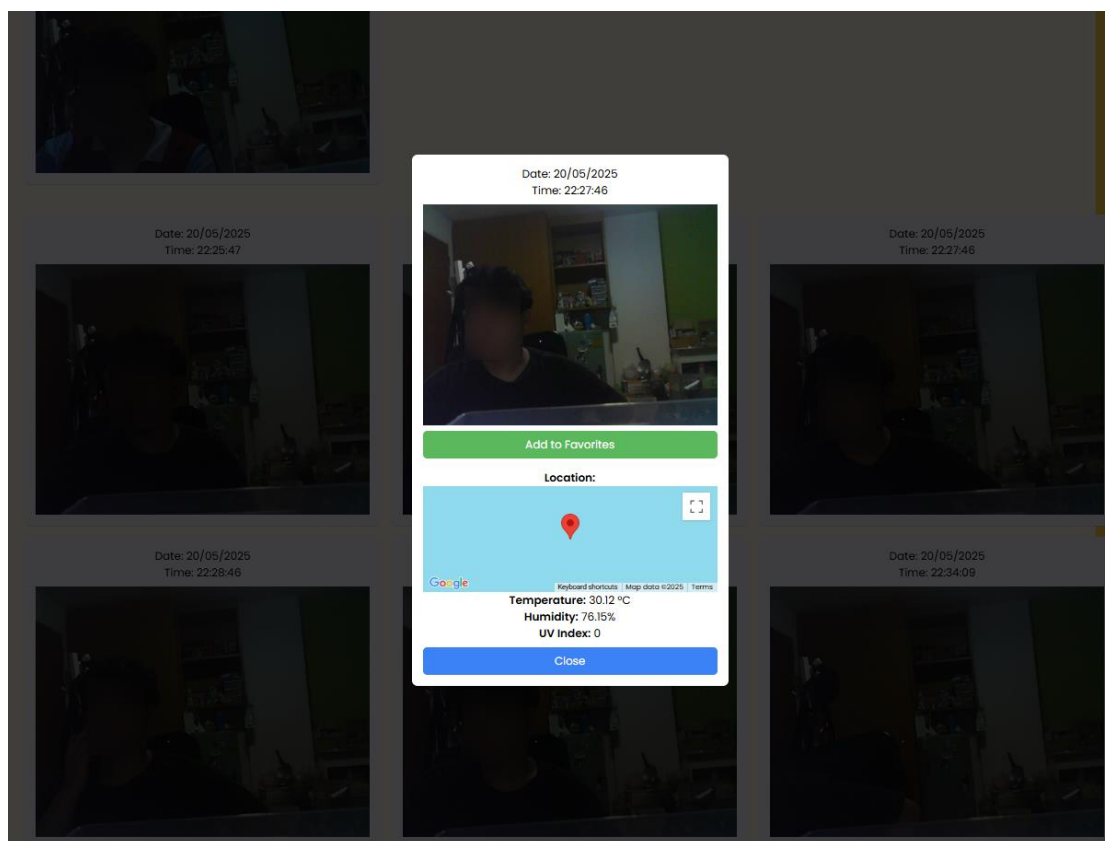
ภาพที่ 3.19 แสดงภาพที่ดึงมาจากเซิร์ฟเวอร์ของอุปกรณ์

เมื่อถึงเวลาที่ตั้งไว้ และหากมีรูปภาพอยู่ในเซิร์ฟเวอร์ของอุปกรณ์ระบบจะดึงรูปภาพนั้นมาและตรวจหาใบหน้า หากพบใบหน้าก็จะนำใบหน้าไปเข้าโมเดลเพื่อเปรียบเทียบจับคู่กับใบหน้าที่ลงทะเบียนในระบบหากพบว่าเป็นคนที่ลงทะเบียนไว้ก็จะนำชื่อที่ลงทะเบียนมาแฮชแล้วรวมกับชื่อภาพ จากนั้นเบลอใบหน้าในรูปภาพและส่งรูปภาพนั้นไปยังคลาวด์

3.5.4 ส่วนของซอฟต์แวร์ในเว็บแอปพลิเคชัน

ในส่วนนี้มีส่วนที่ปรับปรุงเพิ่มจากเวอร์ชัน 1 คือการค้นหารูปภาพที่มีคนที่ลงทะเบียนด้วยชื่อของคนที่ยลงทะเบียน

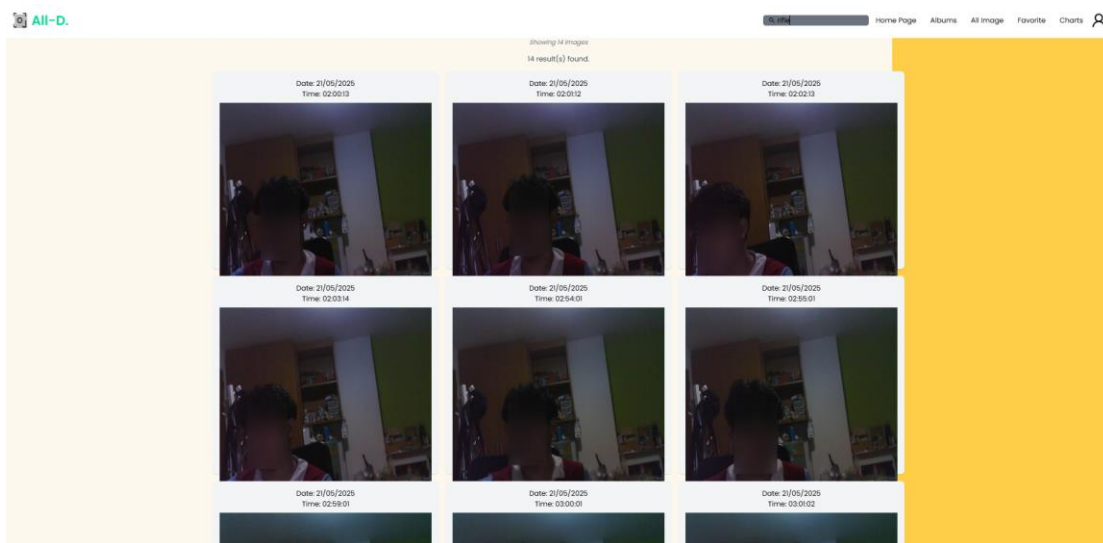
3.5.4.1 หน้าการแสดงรูปภาพที่ผ่านกระบวนการปกป้องความเป็นส่วนตัวแล้ว



ภาพที่ 3.20 แสดงรูปภาพที่ผ่านกระบวนการปกป้องความเป็นส่วนตัวแล้ว

หน้านี้แสดงรูปภาพที่ถูกส่งอุปกรณ์ไปตรวจจับและเบอลไบหน้าในโทรศัพท์เคลื่อนที่ และส่งไปจัดเก็บยังคลาวด์ แล้วเว็บแอปพลิเคชันจึงค่อยไปดึงภาพนั้นมาแสดงอีกทีโดยที่ข้อมูลจากเซนเซอร์ที่บันทึกได้จากอุปกรณ์จะถูกจับคู่กับรูปภาพและนำมาแสดงด้วย

3.5.4.2 หน้าการค้นหาด้วยชื่อของคนทีลงทะเบียน



ภาพที่ 3.21 แสดงหน้าการค้นหาด้วยชื่อของคนทีลงทะเบียน

ในหน้านี้ผู้ใช้สามารถค้นหารูปภาพจากชื่อของคนทีลงทะเบียนได้ รูปภาพที่นำมาแสดงจะเป็นรูปภาพที่ผ่านการเบลอใบหน้าแล้ว และมีค่าแฮชตรงกับค่าแฮชของชื่อที่ผู้ใช้ค้นหาจึงจับคู่ภาพมาได้ตรงกัน

3.5.5 การทดลองเพื่อหาค่าเกณฑ์ (Threshold) ในการจับคู่ใบหน้าในระบบจดจำใบหน้าที่เหมาะสมกับระบบ

ทดลองหาค่า Threshold สำหรับบ่งบอกว่าใบหน้าที่ทดลองเป็นใบหน้าเดียวกับใบหน้าที่ลงทะเบียนหรือไม่หากนำผลการแปลงใบหน้าจากโมเดลมาเปรียบเทียบกับกันแล้วมีค่าต่ำกว่า Threshold จะถือว่าเป็นคนเดียวกัน แต่ถ้าหากผลการเปรียบเทียบมีค่าสูงกว่า Threshold จะถือว่าเป็นคนละคน ทำการทดลองนี้ในระหว่างการพัฒนาเพื่อหาค่า Threshold ที่เหมาะสมและนำมาปรับใช้กับแอปพลิเคชันที่ใช้โมเดลนี้ในการจดจำใบหน้า

โดยมีการออกแบบการทดลองคือ มีชุดข้อมูลสำหรับการทดลองเป็นดังนี้

- ใบหน้าคนที่ลงทะเบียน 1 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

- รูปภาพที่มีคนอยู่ในภาพ 2 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 3 คน จำนวน 5 รูป

- รูปภาพที่มีคนอยู่ในภาพ 4 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 5 คน จำนวน 5 รูป

ดังที่แสดงในตารางนี้

ตารางที่ 3.1 ตารางแสดงชุดข้อมูลสำหรับการทดลองหาค่า Threshold ที่เหมาะสม

จำนวนใบหน้าทีลงทะเบียน	จำนวนคนในรูปที่ใช้ทดลอง	รูปที่ใช้ทดสอบ
1 ใบหน้า	2 คน	รูปที่ 1
		รูปที่ 2
		รูปที่ 3
		รูปที่ 4
		รูปที่ 5
1 ใบหน้า	3 คน	รูปที่ 1
		รูปที่ 2
		รูปที่ 3
		รูปที่ 4
		รูปที่ 5
1 ใบหน้า	4 คน	รูปที่ 1
		รูปที่ 2
		รูปที่ 3
		รูปที่ 4
		รูปที่ 5
1 ใบหน้า	5 คน	รูปที่ 1
		รูปที่ 2
		รูปที่ 3
		รูปที่ 4
		รูปที่ 5

ซึ่งรูปภาพที่นำมาทดลองมีทั้งรูปภาพที่มีคนที่ลงทะเบียนอยู่ภายในรูปและรูปภาพที่ไม่มีคนที่ลงทะเบียนอยู่ในรูป

ทำการทดลองโดยการนำรูปภาพไปเข้าโมเดลและนำผลที่พบว่าจับคู่ถูกต้องทั้ง True Positive และ True Negative มาคำนวณหาค่าความแม่นยำ (Accuracy) ของแต่ละรูปและนำ Accuracy มาเฉลี่ยเพื่อดูค่า Accuracy ของแต่ละเงื่อนไข โดยมีการทดลอง 2 กรณีคือกรณีที่ Threshold เป็น 1.1 และกรณีที่ Threshold เป็น 1.0 และนำค่าเฉลี่ยของ Accuracy ของ 2 กรณีนี้มาเปรียบเทียบกัน

3.5.6 การทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า

ทดลองเพื่อศึกษาว่ามุมของใบหน้าและความสว่างของภาพที่นำมาเข้าโมเดลการจดจำใบหน้ามีผลกับผลลัพธ์ของโมเดลอย่างไร

โดยมีชุดการทดลองประกอบด้วย

- ใบหน้าที่ลงทะเบียน 1 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

- รูปที่มีใบหน้าตรงและเป็นภาพที่สว่าง 5 รูป
- รูปที่มีใบหน้าตรงและเป็นภาพที่มืด 5 รูป
- รูปที่มีใบหน้าเป็นมุมก้มและเป็นภาพที่สว่าง 5 รูป
- รูปที่มีใบหน้าเป็นมุมก้มและเป็นภาพที่มืด 5 รูป
- รูปที่มีใบหน้าเป็นมุมเงยและเป็นภาพที่สว่าง 5 รูป
- รูปที่มีใบหน้าเป็นมุมเงยและเป็นภาพที่มืด 5 รูป
- รูปที่มีใบหน้าเป็นมุมหันซ้ายและเป็นภาพที่สว่าง 5 รูป
- รูปที่มีใบหน้าเป็นมุมหันซ้ายและเป็นภาพที่มืด 5 รูป
- รูปที่มีใบหน้าเป็นมุมหันขวาและเป็นภาพที่สว่าง 5 รูป
- รูปที่มีใบหน้าเป็นมุมหันขวาและเป็นภาพที่มืด 5 รูป

โดยใบหน้าที่อยู่ในรูปที่ใช้ทดลองเป็นใบหน้าคนเดียวกันกับใบหน้าที่ลงทะเบียน

ตารางที่ 3.2 ตารางแสดงชุดข้อมูลสำหรับการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า

มุมของใบหน้าที่ใช้ทดลอง	ใบหน้าที่ใช้ทดลอง แสงสว่าง	ใบหน้าที่ใช้ทดลอง แสงค่อนข้างมืด
หน้าตรง	5 รูป	5 รูป
มุมก้ม	5 รูป	5 รูป
มุมเงย	5 รูป	5 รูป
มุมหันซ้าย	5 รูป	5 รูป
มุมหันขวา	5 รูป	5 รูป

ทำการทดลองโดยนำรูปภาพไปเข้าโมเดลที่ละเอียดและบันทึกผลลัพธ์ที่ได้จากโมเดลที่เป็นค่าของการเปรียบเทียบเวกเตอร์ของ 2 ใบหน้าออกมาโดยค่ายิ่งใกล้ 0.0 หมายความว่ายิ่งเป็นใบหน้าที่ใกล้เคียงกันมาก จากนั้นนำผลลัพธ์มาสร้างเป็นตารางและเปรียบเทียบกัน

3.5.7 การทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น

ทดลองเพื่อศึกษาผลกระทบกับความแม่นยำของโมเดลที่เกิดขึ้นเมื่อมีจำนวนใบหน้าที่ลงทะเบียนเพิ่มขึ้นและจำนวนคนในภาพทดลองเพิ่มขึ้นโดยมีการออกแบบการทดลองดังนี้

- ชุดข้อมูลของการทดลองชุดที่ 1
 - ใบหน้าที่ลงทะเบียน 1 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

 - รูปภาพที่มีคนอยู่ในภาพ 2 คน จำนวน 5 รูป
 - รูปภาพที่มีคนอยู่ในภาพ 3 คน จำนวน 5 รูป
 - รูปภาพที่มีคนอยู่ในภาพ 4 คน จำนวน 5 รูป
 - รูปภาพที่มีคนอยู่ในภาพ 5 คน จำนวน 5 รูป

ตารางที่ 3.3 ตารางแสดงชุดการทดลองชุดที่ 1

จำนวนใบหน้าที่ลงทะเบียน	จำนวนคนในรูปที่ใช้ทดลอง
1 ใบหน้า	2 คน
1 ใบหน้า	3 คน
1 ใบหน้า	4 คน
1 ใบหน้า	5 คน

ทำการทดลองโดยการนำรูปภาพไปเข้าโมเดลจดจำใบหน้าทีละชุดโดยเริ่มจากชุดที่ 1 ที่มีจำนวนใบหน้าทีลงทะเบียนคือ 1 คน กำหนดให้เป็น A จากนั้นสร้างตาราง Confusion Matrix ขนาด 2x2 กำหนดคลาสคือ A และ Not A เริ่มโดยนำรูปภาพที่มีจำนวน 2 คนในภาพไปเข้าโมเดลทีละภาพ แล้วจดผลว่าที่โมเดลจับคู่ได้เป็นคนที่ลงทะเบียนหรือไม่ใช้แล้วนำค่ามาใส่ในตาราง Confusion Matrix แล้วเพิ่มจำนวนคนในภาพและบันทึกผลแบบนี้ไปเรื่อย ๆ

- ชุดข้อมูลของการทดลองชุดที่ 2
 - ใบหน้าที่ลงทะเบียน 2 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

- รูปภาพที่มีคนอยู่ในภาพ 2 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 3 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 4 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 5 คน จำนวน 5 รูป

ตารางที่ 3.4 ตารางแสดงชุดการทดลองชุดที่ 2

จำนวนใบหน้าที่ลงทะเบียน	จำนวนคนในรูปที่ใช้ทดลอง
2 ใบหน้า	2 คน
2 ใบหน้า	3 คน
2 ใบหน้า	4 คน
2 ใบหน้า	5 คน

ชุดทดลองที่ 2 มีจำนวนใบหน้าที่ลงทะเบียนคือ 2 คน กำหนดให้เป็น A และ B จากนั้นสร้างตาราง Confusion Matrix ขนาด 3x3 กำหนดคลาสคือ A B และ Not A B เริ่มโดยนำรูปภาพที่มีจำนวน 2 คนในภาพไปเข้าโมเดลทีละภาพ แล้วจดผลว่าใบหน้าที่โมเดล

จับคู่ได้เป็น A B หรือ Not A B แล้วนำค่ามาใส่ในตาราง Confusion Matrix แล้วเพิ่มจำนวนคนในภาพและบันทึกผลแบบนี้ไปเรื่อย ๆ

- ชุดข้อมูลของการทดลองชุดที่ 3
 - ใบหน้าที่ลงทะเบียน 3 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

- รูปภาพที่มีคนอยู่ในภาพ 2 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 3 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 4 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 5 คน จำนวน 5 รูป

ตารางที่ 3.5 ตารางแสดงชุดการทดลองชุดที่ 3

จำนวนใบหน้าที่ลงทะเบียน	จำนวนคนในรูปที่ใช้ทดลอง
3 ใบหน้า	2 คน
3 ใบหน้า	3 คน
3 ใบหน้า	4 คน
3 ใบหน้า	5 คน

ชุดทดลองที่ 3 มีจำนวนใบหน้าที่ลงทะเบียนคือ 3 คน กำหนดให้เป็น A B และ C จากนั้นสร้างตาราง Confusion Matrix ขนาด 4x4 กำหนดคลาสคือ A B C และ Not A B C เริ่มโดยนำรูปภาพที่มีจำนวน 2 คนในภาพไปเข้าโมเดลที่ละภาพ แล้วจดผลว่าใบหน้าที่โมเดลจับคู่ได้เป็น A B C หรือ Not A B C แล้วนำค่ามาใส่ในตาราง Confusion Matrix แล้วเพิ่มจำนวนคนในภาพและบันทึกผลแบบนี้ไปเรื่อย ๆ

- ชุดข้อมูลของการทดลองชุดที่ 4
 - ใบหน้าที่ลงทะเบียน 4 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

- รูปภาพที่มีคนอยู่ในภาพ 2 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 3 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 4 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 5 คน จำนวน 5 รูป

ตารางที่ 3.6 ตารางแสดงชุดการทดลองชุดที่ 4

จำนวนใบหน้าที่ลงทะเบียน	จำนวนคนในรูปที่ใช้ทดลอง
4 ใบหน้า	2 คน
4 ใบหน้า	3 คน
4 ใบหน้า	4 คน
4 ใบหน้า	5 คน

ชุดทดลองที่ 4 มีจำนวนใบหน้าที่ลงทะเบียนคือ 4 คน กำหนดให้เป็น A B C และ D จากนั้นสร้างตาราง Confusion Matrix ขนาด 5x5 กำหนดคลาสคือ A B C D และ Not A B C D เริ่มโดยนำรูปภาพที่มีจำนวน 2 คนในภาพไปเข้าโมเดลทีละภาพ แล้วจดผลว่าใบหน้าที่โมเดลจับคู่ได้เป็น A B C D หรือ Not A B C D แล้วนำค่ามาใส่ในตาราง Confusion Matrix แล้วเพิ่มจำนวนคนในภาพและบันทึกผลแบบนี้ไปเรื่อย ๆ

- ชุดข้อมูลของการทดลองชุดที่ 5
 - ใบหน้าที่ลงทะเบียน 5 ใบหน้า

รูปภาพสำหรับนำไปทดสอบมี

- รูปภาพที่มีคนอยู่ในภาพ 2 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 3 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 4 คน จำนวน 5 รูป
- รูปภาพที่มีคนอยู่ในภาพ 5 คน จำนวน 5 รูป

ตารางที่ 3.7 ตารางแสดงชุดการทดลองชุดที่ 5

จำนวนใบหน้าที่ลงทะเบียน	จำนวนคนในรูปที่ใช้ทดลอง
5 ใบหน้า	2 คน
5 ใบหน้า	3 คน
5 ใบหน้า	4 คน
5 ใบหน้า	5 คน

ชุดทดลองที่ 5 มีจำนวนใบหน้าที่ลงทะเบียนคือ 5 คน กำหนดให้เป็น A B C D และ E จากนั้นสร้างตาราง Confusion Matrix ขนาด 6x6 กำหนดคลาสคือ A B C D E และ Not A B C D E เริ่มโดยนำรูปภาพที่มีจำนวน 2 คนในภาพไปเข้าโมเดลที่ละภาพ แล้วจดผลว่าใบหน้าที่โมเดลจับคู่ได้เป็น A B C D E หรือ Not A B C D E แล้วนำค่ามาใส่ในตาราง Confusion Matrix แล้วเพิ่มจำนวนคนในภาพและบันทึกผลแบบนี้ไปเรื่อย ๆ

เมื่อทำการทดลองครบทุกเงื่อนไขแล้วจะได้ Confusion Matrix ของแต่ละเงื่อนไข การดำเนินการขั้นต่อไปคือหาค่า True Positive (TP), False Positive (FP), False Negative (FN) และ True Negative (TN) จากแต่ละตาราง

การหาค่า TP, FP, FN และ TN ของตาราง Confusion Matrix แบบ Multi-Class Classification หาได้จากการคำนวณต่อไปนี้

- TP หาได้จากช่องตารางที่ค่าจริงและค่าที่ทำนายได้เป็นค่าเดียวกัน
- FN หาได้จากผลรวมค่าของแถวที่เกี่ยวข้องยกเว้นค่า TP
- FP หาได้จากผลรวมค่าของคอลัมน์ที่เกี่ยวข้องยกเว้นค่า TP
- TN หาได้จากผลรวมของค่าของคอลัมน์และแถวทั้งหมด ยกเว้นค่าของคลาสที่เรากำลังคำนวณ

เมื่อเราหาค่า TP, FP, FN และ TN ของแต่ละคลาสได้แล้วขั้นตอนต่อไปคือการหา Micro Precision และ Micro Recall ของแต่ละเงื่อนไขเพื่อนำมาพล็อตเป็นกราฟแสดงตารางให้เห็นถึงการเปรียบเทียบ โดยค่า Precision และ Recall คำนวณได้จากสูตร

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP})$$

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN})$$

และ Micro Precision และ Micro Recall คำนวณได้จากสูตร

$$\text{Micro Precision} = \text{ผลรวมของ TP} / (\text{ผลรวมของ TP} + \text{ผลรวมของ FP})$$

$$\text{Micro Recall} = \text{ผลรวมของ TP} / (\text{ผลรวมของ TP} + \text{ผลรวมของ FN})$$

เมื่อหาค่า Micro Precision และ Micro Recall ของแต่ละเงื่อนไขได้แล้วก็นำมาพล็อตกราฟเพื่อเปรียบเทียบผลการทดลองที่ได้

บทที่ 4

ผลการดำเนินงาน

4.1 การจัดเตรียมฮาร์ดแวร์และซอฟต์แวร์

4.1.1 ฮาร์ดแวร์ที่ใช้ในการพัฒนาอุปกรณ์ IoT

1. โมดูลไมโครคอนโทรลเลอร์ ESP32-CAM พร้อมกล้อง OV2640
2. โมดูล SHT21 วัดค่าอุณหภูมิและความชื้น
3. โมดูล Ublox NEO-6M (GPS) ระบุตำแหน่งค่าละติจูดและลองจิจูด
4. โมดูล Grove-Sunlight Sensor วัดค่าความเข้มแสงอัลตราไวโอเล็ต (UV)
5. โมดูลสำหรับชาร์จแบตเตอรี่ TP4056 1A USB-C Charger
6. แบตเตอรี่ 3.7 โวลต์ 5000 มิลลิแอมป์ชั่วโมงลิเทียมโพลิเมอร์

4.1.2 ภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนา

4.1.2.1 กลุ่มของภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนาอุปกรณ์ IoT

ภาษาโปรแกรมที่ใช้ : ภาษาซี (C) และ ซีพลัสพลัส (C++)

เครื่องมือที่ใช้ : โปรแกรม Arduino IDE เวอร์ชัน 2.0.2

4.1.2.2 กลุ่มของภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนาแอปพลิเคชันในโทรศัพท์เคลื่อนที่

ภาษาโปรแกรมที่ใช้ : ภาษาจาวา (Java)

เครื่องมือที่ใช้ : โปรแกรม Android Studio เวอร์ชัน Ladybug | 2024.2.1

4.1.2.3 กลุ่มของภาษาโปรแกรมและเครื่องมือที่ใช้ในการพัฒนาแอปพลิเคชัน บันทึกและสืบค้นความทรงจำของผู้ใช้

ภาษาโปรแกรมที่ใช้ : HTML (HyperText Markup Language) CSS (Cascading Style Sheets) และภาษาจาวาสคริปต์ (JavaScript)

เครื่องมือที่ใช้ : โปรแกรม Visual Studio Code

4.1.2.4 บริการบนคลาวด์ (Cloud service) Amazon Web Services

1. Amazon API Gateway : ใช้สำหรับสร้าง Endpoint ในการส่งรูปภาพไปจัดเก็บยังคลาวด์
2. AWS Lambda : ใช้สำหรับสั่งการบนคลาวด์ให้นำรูปภาพไปจัดเก็บในเซิร์ฟเวอร์สำหรับจัดเก็บรูปภาพ หรือส่งรูปภาพไปประมวลผลที่เซิร์ฟเวอร์สำหรับประมวลผลรูปภาพบนคลาวด์
3. AWS Rekognition : ใช้สำหรับประมวลผลรูปภาพในการทำ Object detection เพื่อนำผลลัพธ์ที่ได้ไปใช้ประโยชน์ต่อไป
4. AWS IoT Core : ใช้สำหรับเชื่อมต่อเซิร์ฟเวอร์กับอุปกรณ์ IoT และสร้าง Rule และ Topic สำหรับรับข้อมูลที่บันทึกได้จากเซนเซอร์จากอุปกรณ์แล้วส่งไปจัดเก็บยังที่จัดเก็บบนคลาวด์
5. AWS S3 : ใช้สำหรับจัดเก็บรูปภาพบนคลาวด์
6. Amazon DynamoDB : ใช้สำหรับจัดเก็บข้อมูลที่บันทึกจากเซนเซอร์ไว้บนคลาวด์
7. AWS User : ใช้สำหรับสร้าง Credential เพื่อใช้ดึงข้อมูลจากคลาวด์ไปใช้ในแอปพลิเคชันบันทึกและสืบค้นความทรงจำของผู้ใช้
8. Amazon EC2 : ใช้สำหรับ Deploy แอปพลิเคชัน

4.1.3 คอมพิวเตอร์ที่ใช้ในการพัฒนา

ตารางที่ 4.1 คอมพิวเตอร์ที่ใช้ในการพัฒนา

คอมพิวเตอร์	คอมพิวเตอร์เครื่องที่ 1	คอมพิวเตอร์เครื่องที่ 2
ชื่อรุ่น (Name)	DESKTOP-1TTK4GC	DESKTOP-31L61O8
ระบบประมวลผล (Processor)	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 3.60 GHz	Intel(R) Core(TM) i7- 7700HQ CPU @ 2.80GHz 2.81 GHz
หน่วยความจำ (Memory)	16.0 GB	8.00 GB
ส่วนประมวลผลภาพ (Graphic)	NVIDIA GeForce RTX 2070	NVIDIA GeForce GTX 1050
ส่วนเก็บข้อมูล (Storage)	WD Blue SN580 500GB	WDS500G3X0C-00SJG0 500GB
ระบบปฏิบัติการ (Operating System)	Windows 11 Pro	Windows 10 Home Single Language

4.2 การทดสอบระบบ

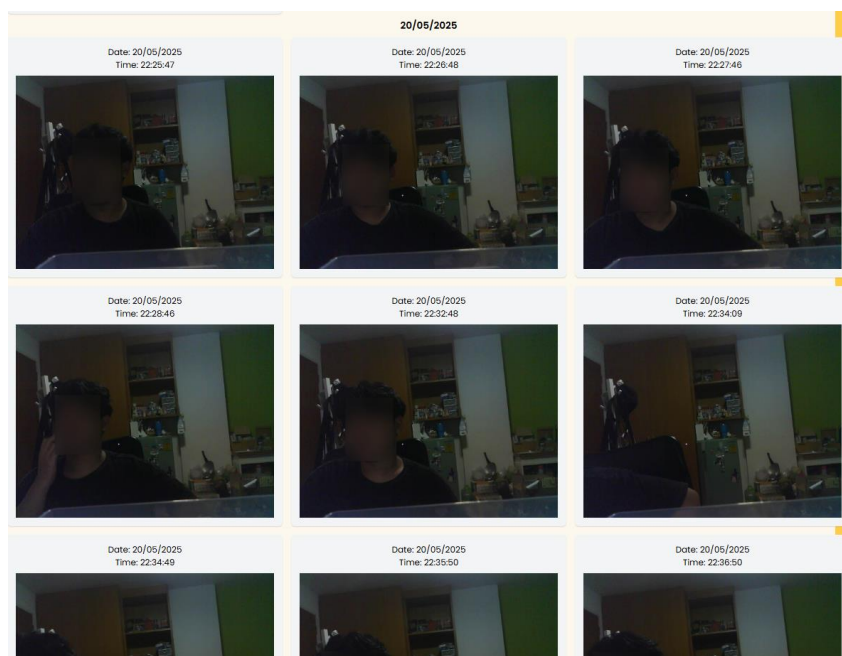
4.2.1 การสร้างทรัพยากรด้วยสคริปต์อัตโนมัติ

สามารถสร้างทรัพยากรจากสคริปต์ได้โดยมีการทดลองส่งข้อมูลผ่านเซอร์วิสที่สร้างด้วยสคริปต์สามารถส่งข้อมูลและนำข้อมูลไปจัดเก็บได้

โดยการสร้างทรัพยากรด้วยสคริปต์จะใช้เวลาเพียง 5 – 10 นาที ในขณะที่การสร้างด้วยมือแบบปกติจะใช้เวลา 2 – 3 ชั่วโมง และอาจมากกว่านั้นขึ้นอยู่กับความชำนาญของแต่ละบุคคล

4.2.2 การทดสอบการเบลอใบหน้าที่ตรวจจับได้ในรูปภาพ

การทดสอบนี้ทำเพื่อทดสอบว่ารูปภาพที่ถูกส่งมาในโทรศัพท์เคลื่อนที่สามารถเบลอใบหน้าที่ตรวจพบได้ วัตถุประสงค์คือเพื่อดูว่าการปกป้องความเป็นส่วนตัวซึ่งเป็นวัตถุประสงค์หลักของโครงการสามารถทำได้จริง

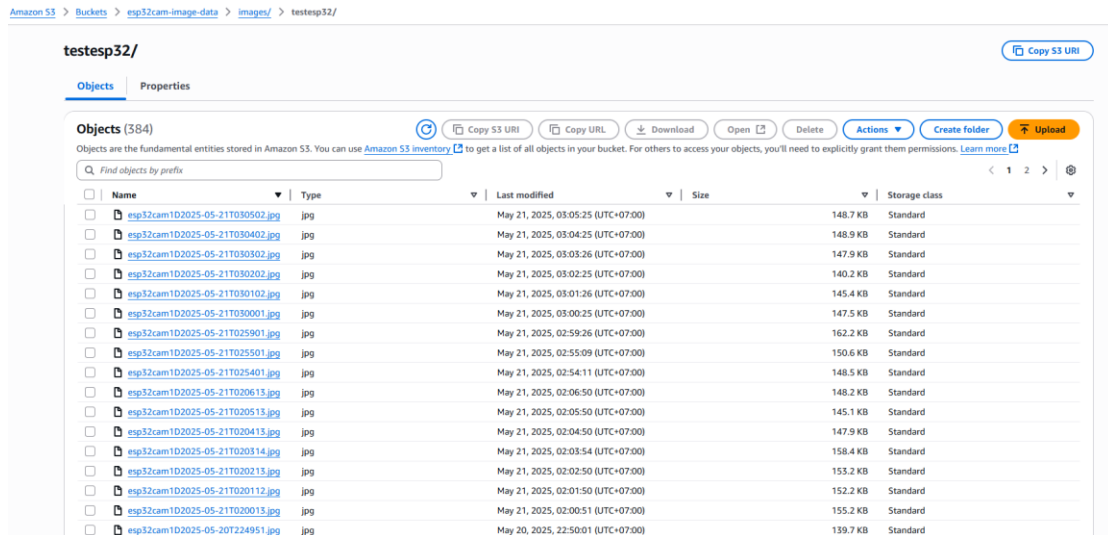


ภาพที่ 4.1 แสดงรูปภาพที่แสดงผลในเว็บและมีการเบลอใบหน้า

จากภาพ 4.1 แสดงรูปภาพที่แสดงอยู่ในเว็บแอปพลิเคชัน ซึ่งทุกรูปเป็นรูปภาพที่มีการเบลอใบหน้าเพื่อปกป้องความเป็นส่วนตัวแล้ว

4.2.3 การทดสอบกระบวนการส่งรูปภาพ

ทดสอบกระบวนการของการส่งรูปภาพจากอุปกรณ์มายังโทรศัพท์เคลื่อนที่ หลังจากผ่านการประมวลผลรูปภาพแล้วจึงส่งต่อไปยังคลาวด์เพื่อจัดเก็บ

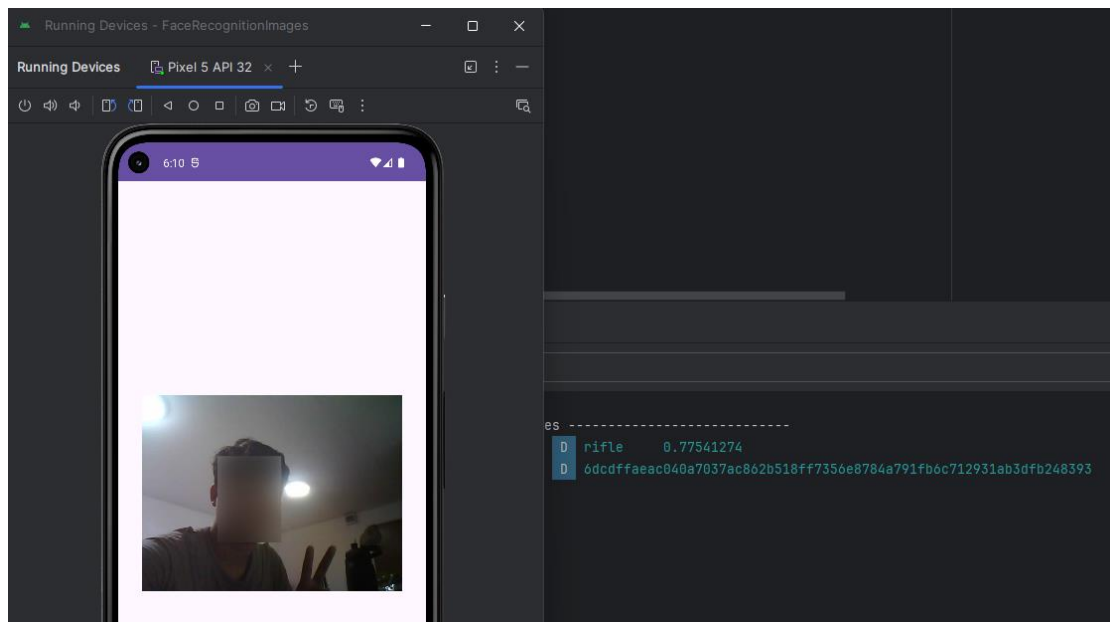


ภาพที่ 4.2 ตัวอย่างของรูปภาพที่ถูกส่งมาเก็บใน Amazon S3

ภาพที่ 4.2 แสดงผลว่ารูปภาพที่บันทึกจากอุปกรณ์สามารถส่งไปประมวลผลรูปภาพและส่งมาจัดเก็บในเซอร์วิส Amazon S3 ได้สำเร็จ

4.2.4 การทดสอบการแฮชชื่อและจัดเก็บค่าแฮชบนคลาวด์

การทดสอบนี้ทำเพื่อดูว่าใบหน้าที่ระบบจดจำใบหน้าเปรียบเทียบแล้วได้ผลว่าตรงกับใบหน้าที่ลงทะเบียนจะสามารถแฮชชื่อที่ลงทะเบียนนั้นและส่งค่าแฮชมาจัดเก็บบนคลาวด์ได้



ภาพที่ 4.3 ตัวอย่างของรูปภาพที่จับคู่ตรงกับใบหน้าทีลงทะเบียนและแฮชชื่อนั้น

imagename(String)	Hashes	Labels	Timestamp
esp32cam1D2025-05-...	[{"S": "6e35c2cd3b6641bb0e2050b78932cbb..."}]	[{"M": {"C": ...}}]	2025-05-20T19:59:27.400Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T19:03:54.605Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T19:55:10.233Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T19:01:51.147Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T19:00:52.584Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T20:05:25.678Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T19:54:13.278Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T20:00:25.765Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T20:02:25.929Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T20:03:26.361Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T20:04:26.021Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T19:02:51.271Z
esp32cam1D2025-05-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T20:01:26.378Z
null	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-23T11:10:00.291Z
esp32cam1D0000-00-...	[{"S": "6dc0ffaeac040a7037ac862b518f7356e8..."}]	[{"M": {"C": ...}}]	2025-05-20T17:54:05.966Z

ภาพที่ 4.4 ตัวอย่างค่าแฮชที่ถูกจัดเก็บใน Amazon DynamoDB

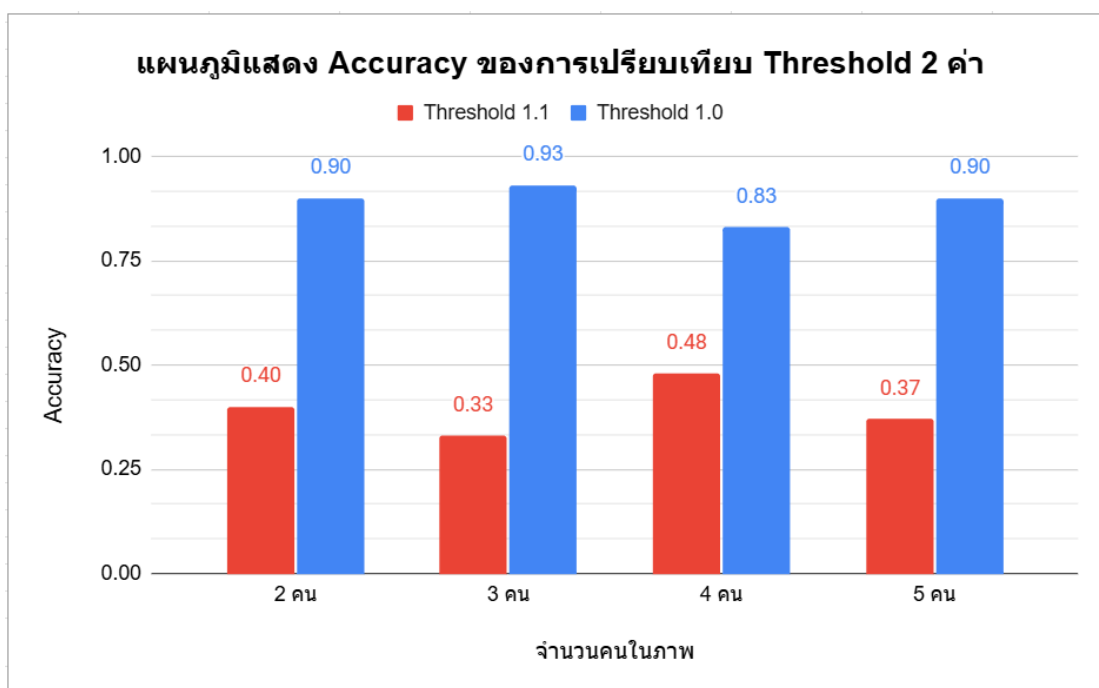
จากภาพที่ 4.3 และภาพที่ 4.4 แสดงให้เห็นว่าเมื่อระบบจับคู่ใบหน้าที่ได้รับมากับ ใบหน้าที่ลงทะเบียนโดยใช้เกณฑ์วัดตาม Threshold แล้วจะแปลงชื่อที่ลงทะเบียนไว้เป็นค่าแฮช และค่าแฮชที่เป็นชื่อของคนทีลงทะเบียนได้ถูกส่งมาจัดเก็บไว้ใน Amazon DynamoDB ได้ สำเร็จ

4.2.5 ผลการทดลองเพื่อหาค่าเกณฑ์ (Threshold) ในการจับคู่ใบหน้าในระบบจดจำใบหน้าที่เหมาะสมกับระบบ

ตารางที่ 4.2 ตารางแสดงผลจากการทดลองหาค่า Threshold ที่เหมาะสม

จำนวนคนในภาพ Threshold	2 คน	3 คน	4 คน	5 คน
1.1	0.40	0.33	0.48	0.37
1.0	0.90	0.93	0.83	0.90

และนำผลการทดลองมาแสดงในรูปแบบแผนภูมิแท่งได้ดังนี้



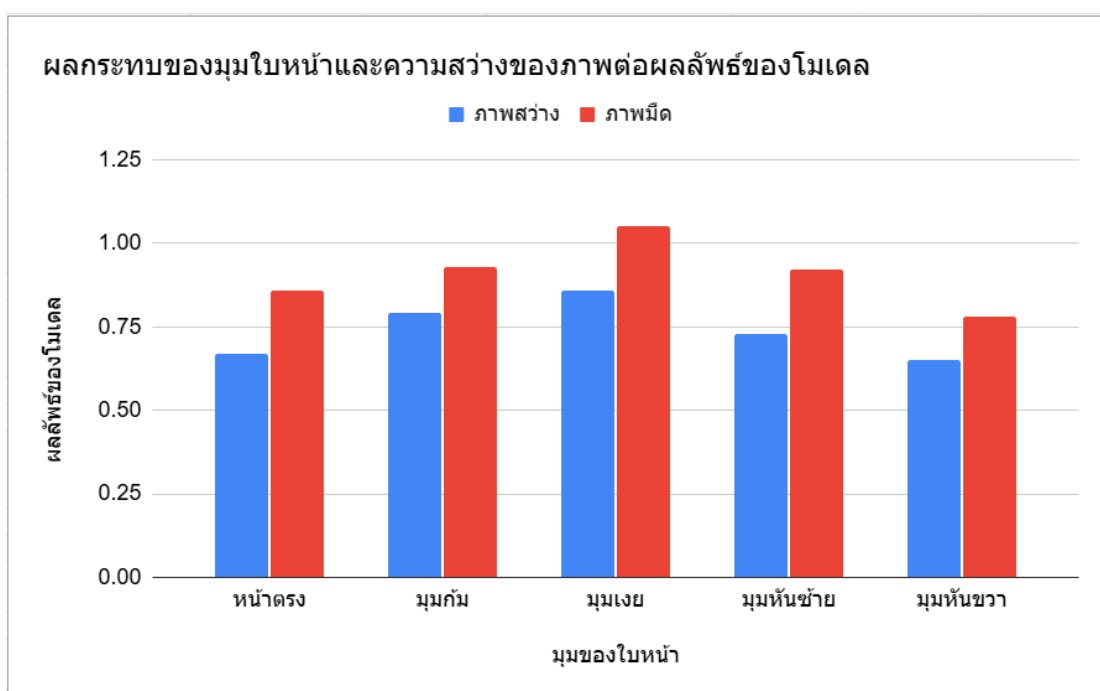
ภาพที่ 4.5 แผนภูมิแสดงผลการทดลองหาค่า Threshold ที่เหมาะสม

จากผลการทดลองพบว่าค่า Accuracy ของในกรณีที่มีการใช้ Threshold เป็น 1.1 ต่ำกว่ากรณีที่มีการใช้ Threshold เป็น 1.0 อย่างมากจึงสามารถสรุปได้ว่าควรใช้ Threshold 1.0 กับระบบในปัจจุบัน

4.2.6 ผลการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า

ตารางที่ 4.3 ตารางแสดงผลจากการทดลองทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า

ความสว่างของภาพ มุมของใบหน้า	ภาพสว่าง	ภาพมืด
หน้าตรง	0.67	0.86
มุมก้ม	0.79	0.93
มุมเงย	0.86	1.05
มุมหันซ้าย	0.73	0.92
มุมหันขวา	0.65	0.78



ภาพที่ 4.6 แผนภูมิแสดงผลการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า

จากผลการทดลองจะเห็นได้ว่าผลลัพธ์ของโมเดลที่ได้จากรูปภาพที่มีแสงสว่าง มีค่าเฉลี่ย 0.0 มากกว่าผลลัพธ์จากรูปภาพที่มีภาพมืด สรุปได้ว่าภาพที่สว่างให้ผลลัพธ์ของโมเดลดีกว่าภาพที่มืด และมุมที่ได้ผลลัพธ์ดีที่สุดคือมุมหน้าตรงและมุมหันขวา ซึ่งได้ผลลัพธ์จากโมเดลเฉลี่ย 0.0 ที่สุด

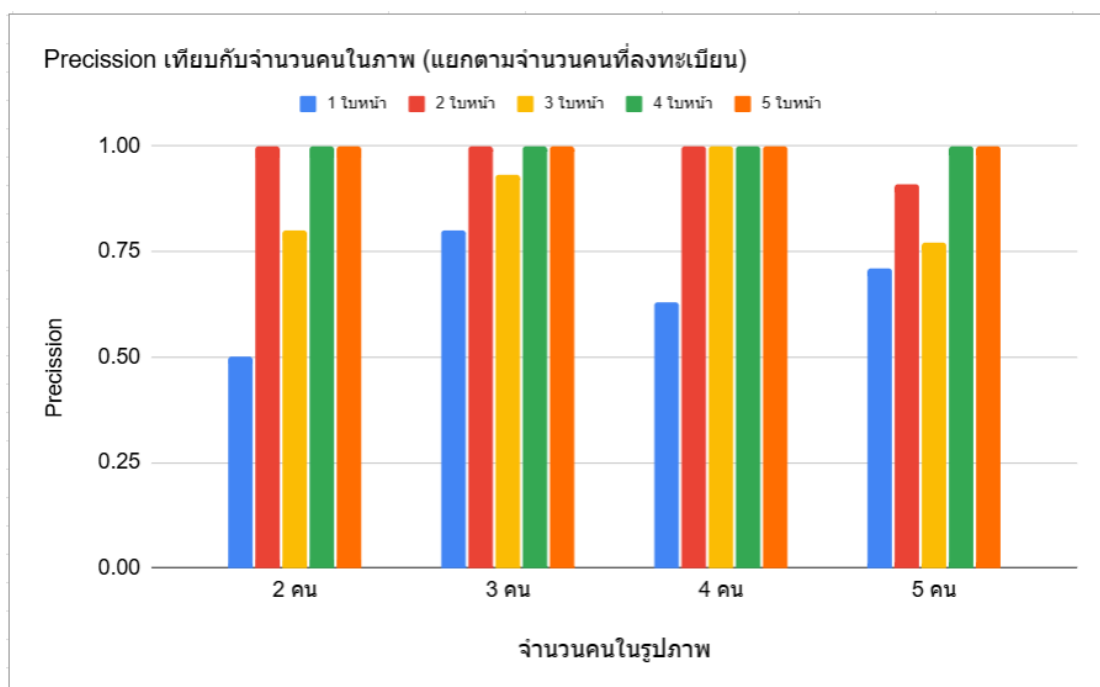
4.2.7 ผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น

เมื่อคำนวณค่า Micro Precision ได้แล้วนำมาใส่ตารางจะได้ตารางลักษณะนี้

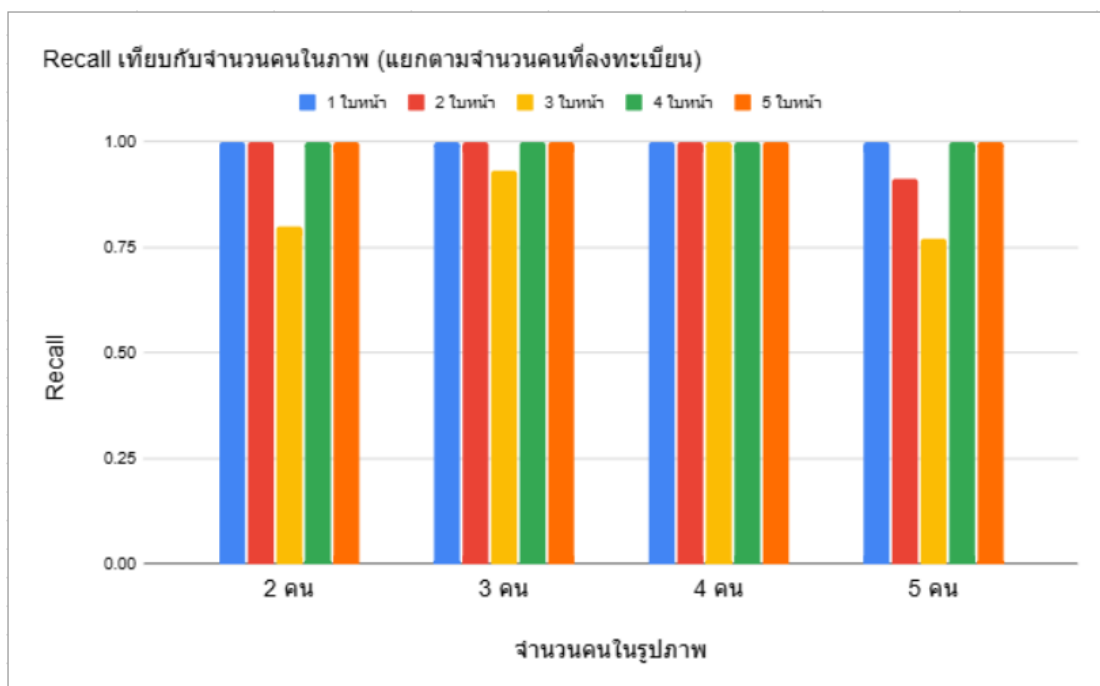
ตารางที่ 4.4 ตารางแสดง Precision ของโมเดล

จำนวนใบหน้าทีลงทะเบียน จำนวนคนในรูปภาพ	1 ใบหน้า	2 ใบหน้า	3 ใบหน้า	4 ใบหน้า	5 ใบหน้า
2 คน	0.5	1	0.8	1	1
3 คน	0.8	1	0.93	1	1
4 คน	0.63	1	1	1	1
5 คน	0.71	0.91	0.77	1	1

สามารถพล็อตกราฟได้จากตารางดังนี้



ภาพที่ 4.7 แผนภูมิแสดงผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น (Precision)



ภาพที่ 4.8 แผนภูมิแสดงผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น (Recall)

จากผลของการทดลองสามารถอธิบายได้ยากกว่าผลที่แท้จริงเป็นอย่างไรเนื่องจากชุดการทดลองที่นำมาทดลองไม่สมดุลกันระหว่าง Positive กับ Negative ทำให้เกิดการลำเอียงไปฝ่ายใดฝ่ายหนึ่งได้ เป็นเหตุผลที่ทำให้เห็นว่าบางค่ามี Precision และ Recall สูงกว่าปกติ แต่จากการทดลองนี้ทำให้สามารถสรุปได้ว่าโมเดลนี้ให้ Precision ไม่ต่ำกว่า 0.5

บทที่ 5

สรุป

5.1 อภิปรายผลการทดลอง

จากการพัฒนาอุปกรณ์บันทึกชีวิตเวอร์ชัน 2 และการทำการทดสอบระบบตามหัวข้อ 4.3.1 การทดสอบการเบลอใบหน้าที่ตรวจจับได้ในรูปภาพ พบว่าระบบสามารถเบลอใบหน้าที่ตรวจจับได้จริง ดังที่ได้แสดงในภาพ 4.1 ซึ่งการทดสอบในส่วนนี้สามารถยืนยันได้ว่ารูปภาพได้รับการปกป้องความเป็นส่วนตัวแล้วตามวัตถุประสงค์

จากหัวข้อ 4.3.2 การทดสอบกระบวนการส่งรูปภาพ จากภาพที่ 4.2 แสดงให้เห็นว่ารูปภาพที่ถูกบันทึกจากอุปกรณ์และถูกส่งไปประมวลผลรูปภาพที่โทรศัพท์ เมื่อเสร็จกระบวนการแล้ว ก็ถูกส่งมาจัดเก็บไว้ใน Amazon S3

จากหัวข้อ 4.3.3 การทดสอบการแฮชชื่อและจัดเก็บค่าแฮชบนคลาวด์ จากภาพที่ 4.3 และภาพที่ 4.4 แสดงให้เห็นว่าเมื่อรูปภาพถูกจับคู่ใบหน้าแล้วระบบจะแฮชชื่อของใบหน้าที่ลงทะเบียนที่จับคู่ได้นั้นแล้วส่งมาจัดเก็บยัง Amazon DynamoDB

จากผลการทดลองในหัวข้อ 4.3.4 การทดลองเพื่อหาค่าเกณฑ์ (Threshold) ในการจับคู่ใบหน้าในระบบจดจำใบหน้าที่เหมาะสมกับระบบ จากภาพที่ 4.5 ดูจาก Accuracy ของโมเดลในแต่ละกรณีสามารถบอกได้ว่าค่า Threshold ที่เหมาะสมในการใช้กับระบบในปัจจุบันคือ 1.0 แม้ว่าในงานวิจัยของ FaceNet model จะใช้ค่า 1.1 ในการทดสอบ

จากผลการทดลองในหัวข้อ 4.3.5 ผลการทดลองเปรียบเทียบคุณลักษณะของรูปภาพที่นำไปเข้าโมเดลจดจำใบหน้า ค่าที่นำมาเปรียบเทียบกันในการทดลองนี้คือผลลัพธ์ที่ได้จากโมเดลซึ่งเป็นค่าระยะห่างระหว่างเวกเตอร์ของ 2 ใบหน้า จากภาพที่ 4.6 สามารถบอกได้ว่าภาพที่สว่างให้ผลลัพธ์ของโมเดลดีกว่าภาพที่มีมืด และมุมที่ได้ผลลัพธ์ที่ดีที่สุดคือมุมหน้าตรงและมุมหันขวา ซึ่งได้ผลลัพธ์จากโมเดลใกล้เคียง 0.0 ที่สุด

จากผลการทดลองในหัวข้อ 4.3.6 ผลการทดลองศึกษาผลกระทบของการจดจำใบหน้าเมื่อมีจำนวนคนลงทะเบียนและจำนวนคนในภาพเพิ่มขึ้น อาจเป็นเพราะว่าชุดข้อมูลที่นำมาทดสอบไม่ได้มีการปรับสมดุลระหว่าง Positive และ Negative ให้เท่ากัน จึงทำให้ผลการคำนวณความลำเอียงไปทางใดทางหนึ่งจากในภาพที่ 4.7 แต่จากการทดลองและผลของการทดลองยังสามารถสรุปจากผลได้ว่าโมเดลมี Precision ไม่ต่ำกว่า 0.5

5.2 สรุปผลการดำเนินงาน

โครงการนี้มีเป้าหมายเพื่อยกระดับระบบบันทึกชีวิตให้สามารถใช้งานได้จริงภายใต้ข้อจำกัดด้านความเป็นส่วนตัว โดยมุ่งเน้นการพัฒนาระบบใน 3 ด้านหลัก ได้แก่

ความสะดวกในการใช้งานและขยายระบบ โดยได้พัฒนา สคริปต์อัตโนมัติ เพื่อสร้างและจัดการทรัพยากรคลาวด์ เช่น Amazon S3, DynamoDB และบริการอื่น ๆ ซึ่งช่วยลดความซับซ้อนและเวลาในการตั้งค่าระบบสำหรับผู้ใช้งานใหม่

การปกป้องความเป็นส่วนตัวของข้อมูล โดยนำภาพจากอุปกรณ์บันทึกชีวิตมาประมวลผลบนสมาร์ตโฟนก่อนจัดเก็บบนคลาวด์ เพื่อให้มั่นใจว่าใบหน้าที่ปรากฏในภาพได้รับการเบลอเรียบร้อยแล้วตามนโยบายความเป็นส่วนตัวที่กำหนดไว้

การรักษาอรรถประโยชน์ในการใช้งาน (data utility retention) โดยผสมโมเดลจดจำใบหน้าบนสมาร์ตโฟนเพื่อตรวจจับบุคคลที่ผู้ใช้ลงทะเบียนไว้ และจัดเก็บผลลัพธ์เป็นค่าแฮชของชื่อเท่านั้น ซึ่งสามารถใช้ในการสืบค้นภาพในภายหลังได้ โดยไม่ลดทอนระดับความเป็นส่วนตัวของระบบ

5.3 แนวทางการพัฒนาต่อ

เพื่อให้โครงการมีศักยภาพในการใช้งานจริงและตอบโจทย์ผู้ใช้ในวงกว้างมากขึ้น แนวทางการพัฒนาต่อในอนาคตมีดังนี้

1. ปรับปรุงฮาร์ดแวร์ของอุปกรณ์บันทึกชีวิต เช่น ลดขนาด เพิ่มความสบายในการสวมใส่ หรือพัฒนาเวอร์ชันที่ใช้เซ็นเซอร์ชนิดใหม่
2. ขยายการประมวลผลภาพไปยังอุปกรณ์อื่น เช่น สมาร์ตวอตช์ หรืออุปกรณ์ IoT อื่น ๆ เพื่อรองรับบริบทการใช้งานที่หลากหลาย
3. ขยายแอปพลิเคชันให้รองรับหลายระบบปฏิบัติการ เช่น iOS (iPhone, iPad) นอกเหนือจาก Android (แอนดรอยด์)
4. เพิ่มความยืดหยุ่นในการเบลอใบหน้า โดยเปิดให้ผู้ใช้สามารถเลือกที่จะเบลอเฉพาะบุคคลที่ไม่อนุญาตหรือไม่
5. เพิ่มทางเลือกในการสืบค้นภาพ โดยรองรับการสืบค้นด้วยคำอธิบายภาพหรือภาษาธรรมชาติมากกว่าการระบุชื่อเพียงอย่างเดียว
6. ปรับปรุงการตั้งค่า threshold ของโมเดลรู้จำใบหน้า โดยศึกษาค่าที่หลากหลายและเหมาะสมกับลักษณะของภาพจริงในระบบให้มากขึ้น

รายการอ้างอิง

- [1] ปราณต์สกล เส้งรอด และ นฤพร บุญยวง, "การศึกษาอุปกรณ์บันทึกชีวิตและแพลตฟอร์มสำหรับจัดเก็บข้อมูล." [Accessed: August 2024].
- [2] L.-D. Tran, C. Gurrin, and A. F. Smeaton, "Lifelogging As An Extreme Form of Personal Information Management - What Lessons To Learn," arXiv, [Online]. Available: <https://arxiv.org/html/2401.05767v1>. [Accessed: Dec. 2024].
- [3] M. Harvey, M. Langheinrich, and G. Ward, "Remembering through lifelogging: A survey of human memory augmentation," *Pervasive and Mobile Computing*, vol. 27, pp. 14–26, 2016.
- [4] G. Wilson, D. Jones, P. Schofield, and D. J. Martin, "The use of a wearable camera to explore daily functioning of older adults living with persistent pain: Methodological reflections and recommendations," *Journal of Rehabilitation and Assistive Technologies Engineering*, vol. 5, pp. 2055668318765411, 2018.
- [5] B. Everson, K. A. Mackintosh, M. A. McNarry, C. Todd, and G. Stratton, "Can wearable cameras be used to validate school-aged children's lifestyle behaviours?" *Children*, vol. 6, no. 2, p. 20, 2019.
- [6] Q. Zhou, D. Wang, C. Ni Mhurchu, C. Gurrin, J. Zhou, Y. Cheng, and H. Wang, "The use of wearable cameras in assessing children's dietary intake and behaviours in China," *Appetite*, vol. 139, pp. 1–7, 2019.
- [7] นายวันพิชิต ชินตระกูลชัย, "ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว คืออะไร มีกี่ประเภท มีอะไรบ้าง ?," [Online]. Available: <https://openpdpa.org/personal-data-type/>. [Accessed: Dec. 2024].
- [8] "Data security and Data privacy," PDPAPlus, [Online]. Available: <https://www.pdpaplus.com/Article/Detail/173856/Data-security-%E0%B9%81%E0%B8%A5%E0%B8%B0-Data-privacy-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3>. [Accessed: Dec. 2024].

- [9] C. Liu, T. Zhu, and W. Zhou, "Privacy Intelligence: A Survey on Image Privacy in Online Social Networks," *ACM Digital Library*, [Online]. Available: <https://dl.acm.org/doi/full/10.1145/3547299#sec-2>. [Accessed: Dec. 2024].
- [10] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Xplore*, [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/7488250>. [Accessed: Dec. 2024].
- [11] Deepak, M. K. Upadhyay, and M. Alam, "Edge Computing: Architecture, Application, Opportunities, and Challenges," *IEEE Xplore*, [Online]. Available: <https://ieeexplore.ieee.org/document/10390171>. [Accessed: Dec. 2024].
- [12] Amazon Web Services, "What is Cloud Computing," AWS, [Online]. Available: <https://aws.amazon.com/th/what-is-cloud-computing/>. [Accessed: Dec. 2024].
- [13] T. Torcheewee, "AI, Machine Learning (ML) คืออะไร? ทำความรู้จักกับบริการ AI และ ML จาก Google Cloud," *Cloud Ace*, [Online]. Available: <https://cloud-ace.co.th/blogs/o0v9a6-ai-machine-learning-ml-ai-ml-goog>. [Accessed: Dec. 2024].
- [14] "Face detection," *Papers with Code*, [Online]. Available: <https://paperswithcode.com/task/face-detection>. [Accessed: Nov. 2024].
- [15] B. Anaya, "Face detection using Haar Cascade," *Medium*, [Online]. Available: <https://medium.com/@baselanaya/faces-detection-using-haar-cascade-3e175aef84f5>. [Accessed: Dec. 2024].
- [16] AWS, "Infrastructure as Code," [Online]. Available: <https://aws.amazon.com/th/what-is/iac/>. [Accessed: Nov. 2024].
- [17] S. Cawley, "How does an OTA firmware update work?" *Mender*, [Online]. Available: <https://mender.io/blog/how-does-an-ota-firmware-update-work>. [Accessed: Dec. 2024].
- [18] K. T. Hanna and I. Wigmore, "Mobile app," *TechTarget*, [Online]. Available: <https://www.techtarget.com/whatis/definition/mobile-app>. [Accessed: Dec. 2024].

- [19] "Mobile app," UDS, [Online]. Available: <https://www.uds.co.th/article/2020/04/27/mobile-application/>. [Accessed: Dec. 2024].
- [20] TP-Link, "Wi-Fi คืออะไร?," [Online]. Available: <https://www.tp-link.com/th/wifi/>. [Accessed: Dec. 2024].
- [21] Sony (Thailand), "เทคโนโลยีไร้สาย Bluetooth คืออะไร?," [Online]. Available: <https://www.sony.co.th/th/electronics/support/articles/00030769>. [Accessed: Dec. 2024].
- [22] Intel Corporation, "What is Bluetooth® Technology?" [Online]. Available: <https://www.thailand.intel.com/content/www/th/th/products/docs/wireless/what-is-bluetooth.html>. [Accessed: Dec. 2024].
- [23] Amazon Web Services, Inc., "The Difference Between HTTP and HTTPS," [Online]. Available: <https://aws.amazon.com/th/compare/the-difference-between-https-and-http/>. [Accessed: Dec. 2024].
- [24] S. Sinkaseam, "มารู้จัก HTTP กันดีกว่าคืออะไรและมีอะไรบ้าง," [Online]. Available: <https://www.borntodev.com/2024/06/17/%E0%B8%A1%E0%B8%B2%E0%B8%A3%E0%B8%B9%E0%B9%89%E0%B8%88%E0%B8%B1%E0%B8%81-http-%E0%B8%81%E0%B8%B1%E0%B8%99%E0%B8%94%E0%B8%B5%E0%B8%81%E0%B8%A7%E0%B9%88%E0%B8%B2/>. [Accessed: Dec. 2024].
- [25] S. Boonklang, "ตรวจจับใบหน้าน้องเหมียวด้วย OpenCV," Born to Dev, [Online]. Available: <https://www.borntodev.com/2021/09/10/%E0%B8%95%E0%B8%A3%E0%B8%A7%E0%B8%88%E0%B8%88%E0%B8%B1%E0%B8%9A%E0%B9%83%E0%B8%9A%E0%B8%AB%E0%B8%99%E0%B9%89%E0%B8%B2%E0%B8%99%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B9%81%E0%B8%A1%E0%B8%A7/>. [Accessed: Nov. 2024].
- [26] OpenCV, "About OpenCV," OpenCV, [Online]. Available: <https://opencv.org/about/>. [Accessed: Nov. 2024].

- [27] M. Bangash, "Smartphone as an Edge for Context-Aware Real-Time Processing for Personal e-Health," ResearchGate, [Online]. Available: https://www.researchgate.net/publication/367636224_Smartphone_as_an_Edge_for_Context-Aware_Real-Time_Processing_for_Personal_e-Health. [Accessed: Dec. 2024].
- [28] Y. Xie, P. Li, N. Nedjah, B. B. Gupta, D. Taniar, and J. Zhang, "Privacy protection framework for face recognition in edge-based Internet of Things," Springer, [Online]. Available: <https://link.springer.com/article/10.1007/s10586-022-03808-8>. [Accessed: Dec. 2024].
- [29] Y. Sun, "iRPy," ACM Digital Library, [Online]. Available: <https://dl.acm.org/doi/abs/10.1145/3395351.3399341>. [Accessed: Dec. 2024].
- [30] Google. (2023). ML Kit for Firebase. [Online]. Available: <https://developers.google.com/ml-kit> [Accessed : Dec. 2025].
- [31] Google Developers. (2023). ML Kit Face Detection on Android. [Online]. Available: <https://developers.google.com/ml-kit/vision/face-detection/android>
- [32] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR), 815–823. [Online]. Available: <https://arxiv.org/abs/1503.03832> [Accessed : May. 2025].
- [33] Liu, Y., Song, Y., & Xu, Y. (2020). Deep Learning Face Recognition System: A Survey. IEEE Access, 8, 179685–179706.
- [34] HumanSoft. (2566). ระบบจดจำใบหน้า (Face Recognition) คืออะไร? พร้อมตัวอย่างการใช้งานจริง. [Online]. เข้าถึงได้จาก: <https://www.humansoft.co.th/th/blog/face-recognition> [Accessed : May. 2025].
- [35] TechTarget. *Hashing คืออะไร*. [Online]. Available: <https://www.techtarget.com/searchdatamanagement/definition/hashing> [Accessed : May. 2025].
- [36] Google Developers, "Face detection with ML Kit," Google, [Online]. Available: <https://developers.google.com/ml-kit/vision/face-detection>. [Accessed: Jun. 2025].

- [37] P. Viola and M. Jones, "Rapid Object Detection using a Boosted Cascade of Simple Features," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Kauai, HI, USA, 2001.
- [38] T. N. Nguyen, T. T. Nguyen, et al., "Real-time Face Detection on Mobile Devices using Google ML Kit," *J. Mobile Vision Syst.*, vol. 9, no. 2, pp. 87–95, 2023.
- [39] Schroff, F., Kalenichenko, D., & Philbin, J., "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proc. CVPR*, 2015. [Online]. Available: <https://arxiv.org/abs/1503.03832>. [Accessed: Jun. 2025].
- [40] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L., "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," in *Proc. CVPR*, 2014. [Online]. Available: <https://www.cs.tau.ac.il/~wolf/DeepFace.pdf>. [Accessed: Jun. 2025].

