

การพัฒนาระบบสแกนลายนิ้วมือและจับภาพใบหน้าด้วยเทคโนโลยีอินเทอร์เน็ตทุก สรรพสิ่งสำหรับห้องแม่ข่าย

FINGERPRINT SCAN AND FACE CAPTURE WITH INTERNET OF THINGS TECHNOLOGY FOR THE HOST ROOM

เอกรัตน์ สุขสุคนธ์*, สมชิต พวกสันเทียะ, บัณฑิต วัชรธรรม, ศักดิ์เจริญชัยกุล และ พิชชากร ขอบใจ
Aekkarat Suksukont*, Somchit Puaksantier, Buawan Sakcharoenchaiyakun
and Pichakorn Khobjai

สาขาวิชาเทคโนโลยีคอมพิวเตอร์และนวัตกรรม คณะวิทยาศาสตร์และเทคโนโลยี วิทยาลัยเซาธ์อีสท์บางกอก
Department of Computer Technology and Innovation Faculty of Science and Technology,
Southeast Bangkok College

บทคัดย่อ

งานวิจัยนี้นำเสนอเกี่ยวกับการพัฒนาระบบสแกนลายนิ้วมือและจับภาพใบหน้าด้วยเทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่งสำหรับห้องแม่ข่าย การออกแบบระบบได้พิจารณาจากการใช้งานของบุคลากรภายในห้องแม่ข่าย ในระบบสแกนลายนิ้วมือเพื่อปลดล็อกประตูจะนำบอร์ด Arduino Uno R3 สั่งการให้บอร์ด Raspberry Pi เปิดกล้องและทำการบันทึกภาพใบหน้าของผู้ที่ทำการสแกนลายนิ้วมือ โดยบันทึกภาพของผู้สแกนลายนิ้วมือลงในฐานข้อมูลพร้อมกับบันทึกวันที่และเวลาไว้ จากนั้นระบบจะแยกลายนิ้วมือที่ข้อมูลถูกต้องและทำการปลดล็อกประตู หากผู้ที่สแกนลายนิ้วมือไม่ผ่านระบบจะบันทึกวันที่และเวลาไว้พร้อมภาพถ่ายของผู้เข้าห้องแม่ข่ายผ่านทางแอปพลิเคชันไลน์ให้แก่ผู้ที่มีหน้าที่ในการรับผิดชอบตามที่กำหนดไว้ จากการทดลอง พบว่า ในส่วนที่มีฐานข้อมูลของบุคลากรที่ทำการลงทะเบียนไว้แล้วนั้น ระบบสามารถยืนยันบุคคลที่มีสิทธิ์ใช้งานห้องแม่ข่ายได้อย่างถูกต้องแม่นยำ คิดเป็น 90 เปอร์เซ็นต์ ผลการถ่ายภาพใบหน้า คิดเป็น 95 เปอร์เซ็นต์ ผลการบันทึกข้อมูล คิดเป็น 100 เปอร์เซ็นต์ และผลการแจ้งเตือนผ่านทางแอปพลิเคชันไลน์ คิดเป็น 100 เปอร์เซ็นต์

คำสำคัญ: ระบบสแกนลายนิ้วมือ, ระบบถ่ายภาพใบหน้า, อินเทอร์เน็ตทุกสรรพสิ่ง

* ผู้ประสานงาน: เอกรัตน์ สุขสุคนธ์

อีเมล: aekkarat2331@gmail.com

Abstract

This research aimed to present the fingerprint scan and face capture with Internet of Things (IoT) technology for the host room. The system design was based on the accessibility of personnel within the server host room. In the fingerprint scanning system, to unlock the door, the Arduino Uno R3 would order the Raspberry Pi board to turn on the camera and capture the face of the person who was scanning the fingerprints by recording the fingerprint and the picture of that person into the database with the date and time of scanning. After that, the system would extract the fingerprint with the correct information and unlock the door. If the information of that person was not correct, the system would record the date and time, including capturing the picture of that person who wanted to enter the server room and sending the information through the Line application to the person in charge. The research found that, according to the database of registered personnel, the system accurately verified the personnel with permission to access the server room at 90%. The accuracy of face capture was at 95%, data recording was at 100% and line application notification was at 100%.

Keywords: Fingerprint system, face capture system, Internet of Things

บทนำ

ในปัจจุบันเทคโนโลยีที่เกี่ยวข้องกับความปลอดภัยในการเข้าหรือออกในห้องต่าง ๆ โดยส่วนมากระบบรักษาความปลอดภัยที่ติดตั้งไว้นั้นจะอยู่ในรูปแบบของการสแกนลายนิ้วมือหรือระบบคีย์การ์ด ซึ่งอาจจะยังมีความปลอดภัยที่ไม่เพียงพอ ด้วยเหตุนี้จึงเป็นที่มาของแนวคิดในการเพิ่มความปลอดภัยในการเข้าหรือออกในห้องต่าง ๆ ด้วยระบบถ่ายภาพใบหน้าควบคู่กับระบบสแกนลายนิ้วมือ เพื่อเพิ่มความปลอดภัยให้มากยิ่งขึ้นจากผู้ที่ไม่เกี่ยวข้องในสำนักงานนั้น ๆ หลายองค์กรได้นำเทคโนโลยีเข้ามาประยุกต์ใช้อย่างแพร่หลาย และการระบุบุคคลมีความสำคัญและเกี่ยวข้องกับงานหลากหลายสาขา เช่น การแพทย์และอาชญากรรม

รวมถึงการสำรวจประชากรเพื่อให้มีประสิทธิภาพในด้านความสะดวกรวดเร็วและความถูกต้อง เช่น โรงแรม เป็นองค์กรที่มีการนำเทคโนโลยีสมัยใหม่มาใช้ สำหรับเทคโนโลยีระบบสแกนลายนิ้วมือหรือแม้กระทั่งเทคโนโลยีการรู้จำใบหน้า (Face recognition) เป็นกระบวนการที่นำภาพไปตรวจจับในกระบวนการประมวลผลภาพ แล้วนำมาเปรียบเทียบกับฐานข้อมูลของใบหน้า เพื่อระบุว่าใบหน้านั้น ๆ ตรงกับบุคคลใดหรือไม่ ซึ่งการระบุใบหน้าที่มีหลากหลายวิธี เช่น Principal component analysis (PCA), Linear discriminant analysis (LDA), Elastic bunch graph matching (EBGM) เป็นต้น

จากงานวิจัยของ (Adulkasem et al., 2007) ได้นำเสนอแบบจำลองการควบคุมเข้าใช้งานระบบโดยการพิสูจน์ลายนิ้วมือ โดยแบบจำลองทำงานในลักษณะไคลเอนต์-เซิร์ฟเวอร์ แบบจำลองสามารถทำการยืนยันบุคคลที่มีสิทธิ์เข้าใช้พื้นที่/ระบบ สามารถพิสูจน์บุคคลด้วยลายนิ้วมือ ความถูกต้องแม่นยำในการพิสูจน์บุคคลด้วยลายนิ้วมือ คิดเป็น 80.56 เปอร์เซ็นต์ และแบบจำลองสามารถตรวจสอบการเข้าใช้ระบบ โดยมีความถูกต้องแม่นยำ คิดเป็น 98.12 เปอร์เซ็นต์ จากงานวิจัยของ (Sillapakitkosol et al., 2010) ได้นำเสนอเครื่องสแกนลายนิ้วมือเพื่อเปิด-ปิดประตู เกิดจากการศึกษาความเป็นไปได้ของระบบทำให้เกิดแนวคิดในการใช้อุปกรณ์ควบคุมแบบอัตโนมัติ ซึ่งใช้ไมโครคอนโทรลเลอร์ ตระกูล AVR เป็นตัวควบคุมหลักของระบบ โดยประโยชน์ของระบบเครื่องสแกนลายนิ้วมือนี้ สามารถใช้เครื่องรับ-ส่งสัญญาณผ่านพอร์ต RS-232 แบบไร้สาย ในการส่งสัญญาณรับและส่งข้อมูลมาที่หน่วยประมวลผลกลาง เพื่อลดจำนวนอุปกรณ์ จากงานวิจัยของ (Pongkan & Boonto, 2018) ได้นำเสนอระบบตรวจสอบการเข้าเรียนแบบทันกาลด้วยลายนิ้วมือ เพื่อช่วยให้ผู้สอนไม่ต้องเสียเวลาไปกับการขานชื่อผู้เรียนในชั้นเรียน เริ่มต้นจากผู้เรียนทำการลงทะเบียนลายนิ้วมือไปเก็บไว้ในชุดเซนเซอร์ตรวจสอบลายนิ้วมือ จากนั้นในการตรวจสอบการเข้าเรียน บอร์ด Arduino จะอ่านค่าลายนิ้วมือจากเซนเซอร์ตรวจสอบลายนิ้วมือไปยัง Node MCU เพื่อทำการส่งค่าลายนิ้วมือไปเก็บยังฐานข้อมูลในคอมพิวเตอร์ของผู้สอนผ่านการสื่อสารข้อมูลแบบไร้สายผ่านสัญญาณ WiFi ระบบนี้จะมีการแสดงผลการเข้าเรียนแบบทันกาลผ่านทางเว็บแอปพลิเคชัน จากการทดสอบการใช้งาน พบว่า อุปกรณ์ต้นแบบที่ได้พัฒนาขึ้นสามารถส่งค่าลายนิ้วมือแบบไร้สายในอัตราเฉลี่ย 3.62 วินาทีต่อคน และสามารถบันทึกผลการเข้าเรียนของผู้เรียนไว้ในฐานข้อมูลพร้อมทั้งแสดงผลการเข้าเรียนผ่านหน้าเว็บแอปพลิเคชันได้อย่างถูกต้องแม่นยำ คิดเป็น 100 เปอร์เซ็นต์ และจากงานวิจัยของ (Triprapin et al., 2018) ได้นำเสนอระบบ

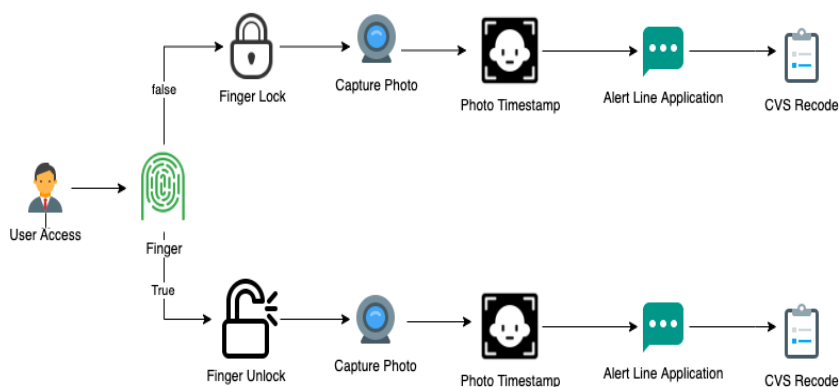
ตรวจสอบนักศึกษาเข้าเรียนโดยใช้เทคนิคการรู้จำใบหน้า โดยใช้การเปรียบเทียบ 3 วิธี คือ วิธี Eigen face recognition วิธี Fisher face recognition และวิธี Local binary pattern histograms (LBPH) recognition เพื่อนำไปใช้ในระบบที่พัฒนา จากการทดลอง พบว่า วิธี LBPH recognition มีความถูกต้องแม่นยำในการระบุตัวตนของนักศึกษา คิดเป็น 94.21 เปอร์เซ็นต์

จากงานวิจัยที่กล่าวมาข้างต้น ในการตรวจสอบลายนิ้วมียังมีความผิดพลาดพอสมควร ดังนั้น ผู้วิจัยจึงได้มีแนวคิดออกแบบระบบให้สามารถจัดเก็บข้อมูลภาพถ่ายบันทึกเวลาและแยกลายนิ้วมือที่ผ่านและไม่ผ่านการตรวจสอบ โดยสามารถแจ้งข้อมูลให้ผู้เกี่ยวข้องทราบผ่านแอปพลิเคชันไลน์พร้อมสามารถภาพถ่ายได้ทันที

วิธีการดำเนินการวิจัย

การออกแบบระบบ

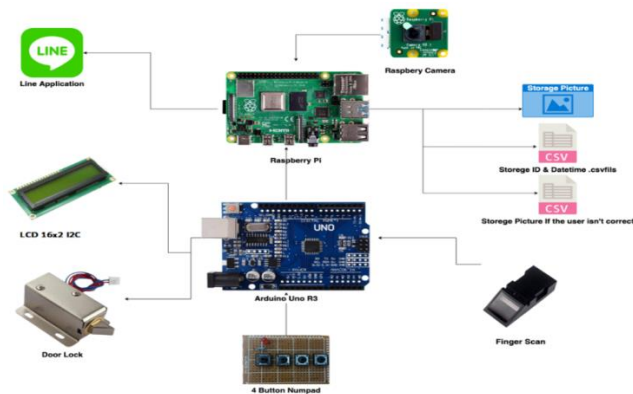
ในการออกแบบระบบได้พิจารณาจากเข้าใช้งานของห้องแม่ข่ายโดยหลังจากการสแกนลายนิ้วมือเพื่อปลดล็อกประตูแล้ว ระบบได้สั่งการให้เปิดกล้องและบันทึกใบหน้าของผู้สแกนลายนิ้วมือ โดยบันทึกภาพผู้สแกนลายนิ้วมือลงในฐานข้อมูลพร้อมวันที่และเวลา โดยแยกลายนิ้วมือที่ข้อมูลถูกต้องและระบบปลดล็อกประตูให้ และแยกผู้ที่สแกนลายนิ้วมือไม่ผ่านพร้อมบันทึกวันที่เวลา โดยจะส่งข้อมูลทั้งผู้ที่สแกนลายนิ้วมือผ่านและไม่ผ่านพร้อมภาพถ่ายของผู้เข้าห้องแม่ข่ายผ่านทางแอปพลิเคชันไลน์



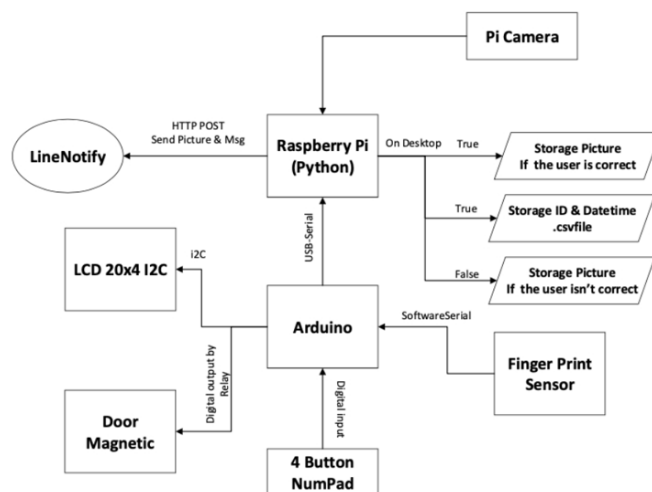
รูปที่ 1 การออกแบบการทำงานของระบบ

การออกแบบอุปกรณ์

ในส่วนของฮาร์ดแวร์ คือ ชุดอุปกรณ์สำหรับระบบสแกนลายนิ้วมือและจับภาพใบหน้าด้วยเทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่งสำหรับห้องแม่ข่าย เพื่อตรวจสอบการเข้าใช้งานห้องแม่ข่ายซึ่งจะประกอบไปด้วย เซนเซอร์ตรวจจับลายนิ้วมือ (Fingerprint sensor), Arduino Uno R3, 16x2 LCD I2C, Door lock, Raspberry Pi, 4 Button numpad, Camera และในส่วนของซอฟต์แวร์ประกอบไปด้วย แอปพลิเคชันไลน์ (Line application) และฐานข้อมูลที่ใช้คือ CSV (Comma separated value) ดังรูปที่ 2 และรูปที่ 3



รูปที่ 2 อุปกรณ์และฐานข้อมูลของระบบ

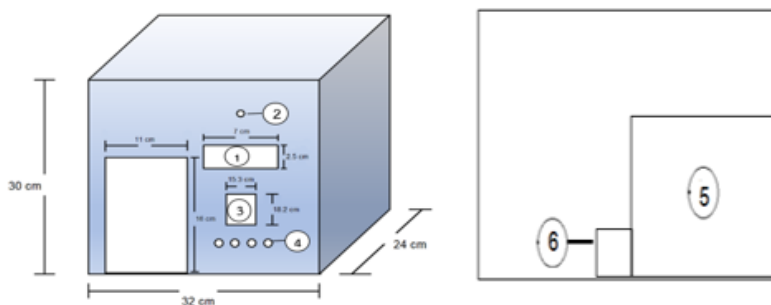


รูปที่ 3 การเชื่อมต่อระบบ

การศึกษาการเข้าออกห้องแม่ข่ายจากผู้เกี่ยวข้อง โดยส่วนใหญ่นอกจากแผนกไอทีผู้เป็นเจ้าของพื้นที่แล้ว ยังมีแผนกรักษาความปลอดภัยและแผนกซ่อมบำรุงที่สามารถเข้า-ออกห้องแม่ข่ายได้ ดังนั้นในกระบวนการศึกษาและการดำเนินการวิจัยจึงเริ่มออกแบบในภาพรวมและพิจารณาเลือกอุปกรณ์ให้เหมาะสมกับการใช้งาน ในการออกแบบระบบมีวัตถุประสงค์ให้การเข้า-ออกห้องแม่ข่ายมีการป้องกันและสามารถบันทึกข้อมูลต่าง ๆ โดยคำนึงถึงการเข้า-ออกใช้งานของผู้ที่เกี่ยวข้องเป็นสำคัญ

การออกแบบชิ้นงาน

การออกแบบเพื่อใช้สำหรับป้องกันส่วนของชิ้นงานที่ใช้ในการประมวลผลจากสภาพแวดล้อมภายนอกและออกแบบมาเพื่อลดพื้นที่ของชิ้นงานทั้งหมด โดยวัสดุที่ใช้ห่อหุ้มชิ้นงานจะเลือกใช้เป็นพลาสติกชนิดอะคริลิก (Acrylic plastic) เนื่องจากมีความคงทนแข็งแรง และคุณลักษณะภายนอกที่คล้ายคลึงกับกระจกแต่ดูแลรักษาง่ายและเบากว่าอีกทั้งยังนิยมใช้งานอย่างมาก ดังรูปที่ 4



รูปที่ 4 การออกแบบชิ้นงาน

การออกแบบชิ้นงานนั้น ภายนอกเป็นวัสดุอุปกรณ์ที่ใช้ห่อหุ้มชิ้นงาน โดยที่หมายเลข 1 เป็นตำแหน่ง ของหน้าจอ LCD หมายเลข 2 เป็นตำแหน่งของ Raspberry Pi Camera V2 และหมายเลข 3 เป็นตำแหน่งของ Fingerprint sensor หมายเลข 4 เป็นตำแหน่งของ 4 Button numpad การออกแบบภายในนั้น ส่วนของวงจรควบคุมจะอยู่ภายในวัสดุห่อหุ้มโดยที่หมายเลข 5 เป็นตำแหน่งของวงจรควบคุมทั้งหมด และหมายเลข 6 เป็นตำแหน่งของ Door lock และในส่วนของการเชื่อมต่อบอร์ด Arduino Uno R3 กับ Raspberry Pi เข้าด้วยกัน เพื่อใช้ในการติดต่อและรับ-ส่งข้อมูลให้กันและกัน

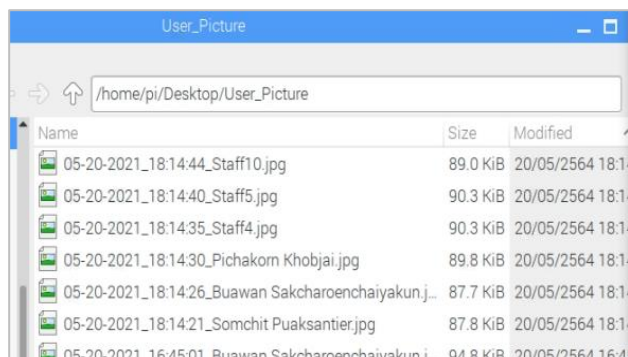
การสร้างโปรแกรม

ขั้นตอนการสร้างโปรแกรม ใช้การเขียนภาษาไพธอน ผ่านโปรแกรม Visual studio code (VS Code) ส่วนของโปรแกรมบันทึกข้อมูลและส่งข้อมูลไปยัง Raspberry Pi รวมทั้งส่วนที่ใช้แสดงลายนิ้วมือและการปลดล็อคประตู ดังรูปที่ 5

```
1 name0 = 'No ID'
2 name1 = 'Somchit Puaksantier'
3 name2 = 'Buawan Sakcharoenchaiyakun'
4 name3 = 'Pichakorn Khobjai'
5 #import cv2
6 import time
7 import serial
8 import csv
9 import requests
10 import datetime
11 import cv2
12 import numpy as np
13 arduino = serial.Serial('/dev/ttyACM0',9600)
14 path = '/home/pi/Desktop/datalogger.csv'
15 path_pic = '/home/pi/Desktop/capture.jpg'
16 path_UserPic = '/home/pi/Desktop/User_Picture/'
17 path_NoUserPic = '/home/pi/Desktop/Stranger_Picture/'
18 count=0
19 is0
20 cap = cv2.VideoCapture(0) #camera1
21 def write_csv(data):
22     with open(path, 'a') as outfile:
23         writer = csv.writer(outfile)
24         writer.writerow(data)
25
26 while True:
27     ret, frame = cap.read()
28     gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
29
30     # Display the resulting frame
31     font = cv2.FONT_HERSHEY_SIMPLEX
32     bottomLeftCornerOfText = (10,450)
33     fontScale = 1
34     fontColor = (255,255,255)
35     lineType = 2
36     x=datetime.datetime.now()
37     ddx=strftime("%x")
38     tt=x.strftime("%H")+":"+x.strftime("%M")+":"+x.strftime("%S")
39     cv2.putText(frame,dd+' '+tt,
40                 bottomLeftCornerOfText,
41                 font,
42                 fontScale,
43                 fontColor,
44                 lineType)
45
```

รูปที่ 5 ขั้นตอนการสร้างโปรแกรม

ในการทดสอบประสิทธิภาพของโปรแกรมในส่วนของรูปแบบการบันทึกข้อมูล และการแจ้งเตือนต่าง ๆ ดังรูปที่ 6 และรูปที่ 7



รูปที่ 6 หน้าต่างแสดงรายชื่อผู้ใช้งานห้องแม่ข่าย



รูปที่ 7 ข้อความและรูปภาพผ่านแอปพลิเคชันไลน์

ผลการวิจัยและอภิปรายผล

งานวิจัยชิ้นนี้ได้พัฒนาระบบสแกนลายนิ้วมือและจับภาพใบหน้าด้วยเทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่งสำหรับห้องแม่ข่าย ซึ่งจุดเด่นของงานวิจัยนี้คือการสแกนลายนิ้วมือและถ่ายภาพบุคคลที่ผ่านเข้าห้องแม่ข่าย ระบบสามารถแจ้งเตือนไปยังผู้ดูแลระบบได้ หากพบบุคคลที่ไม่พึงประสงค์ก็สามารถระบุได้ว่าบุคคลคนนั้นคือใคร จากผลการทดสอบระบบสแกนลายนิ้วมือและจับภาพใบหน้าด้วยเทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่งสำหรับห้องแม่ข่าย ผลการทดสอบตารางที่ 1 คือการทดสอบกับผู้ที่มีฐานข้อมูลอยู่ในระบบ จำนวน 20 คน และผลการทดสอบตารางที่ 2 คือการทดสอบกับผู้ที่ไม่ได้บันทึกฐานข้อมูลไว้ในระบบ จำนวน 20 คน กลุ่มประชากรที่ใช้ในการทดสอบระบบทั้งสิ้น จำนวน 40 คน

ตารางที่ 1 การทดสอบประสิทธิภาพความแม่นยำของระบบ โดยทดสอบกับผู้ที่มีฐานข้อมูลอยู่ในระบบ จำนวน 20 คน

การทดสอบ	ผ่าน	ไม่ผ่าน	ประสิทธิภาพ
ผลการสแกนลายนิ้วมือ	18	2	90 %
ผลการถ่ายภาพใบหน้า	19	1	95 %
ผลการบันทึกข้อมูล	20	0	100 %
ผลการแจ้งเตือนผ่านไลน์	20	0	100 %

จากตารางที่ 1 การทดสอบประสิทธิภาพของผู้ที่มีข้อมูลอยู่ในฐานข้อมูล ซึ่งผลการสแกนลายนิ้วมือ คิดเป็น 90 เปอร์เซ็นต์ ผลการถ่ายภาพใบหน้า คิดเป็น 95 เปอร์เซ็นต์ ผลการบันทึกข้อมูล คิดเป็น 100 เปอร์เซ็นต์ และผลการแจ้งเตือนผ่านทางแอปพลิเคชันไลน์ คิดเป็น 100 เปอร์เซ็นต์ ซึ่งผลการทดสอบโดยรวมอยู่ในระดับที่ดีมาก

ตารางที่ 2 การทดสอบประสิทธิภาพความแม่นยำของระบบ โดยทดสอบกับผู้ที่ไม่ได้บันทึกฐานข้อมูลไว้ในระบบ จำนวน 20 คน

การทดสอบ	ผ่าน	ไม่ผ่าน	ประสิทธิภาพ
ผลการสแกนลายนิ้วมือ	0	20	100 %
ผลการถ่ายภาพใบหน้า	19	1	95 %
ผลการบันทึกข้อมูล	20	0	100 %
ผลการแจ้งเตือนผ่านไลน์	20	0	100 %

จากตารางที่ 2 การทดสอบประสิทธิภาพของผู้ที่ไม่มีข้อมูลอยู่ในฐานข้อมูล ซึ่งผลการสแกนลายนิ้วมือ คิดเป็น 100 เปอร์เซ็นต์ ผลการถ่ายภาพใบหน้าคิดเป็น 95 เปอร์เซ็นต์ ผลการบันทึกข้อมูล คิดเป็น 100 เปอร์เซ็นต์ และผลการแจ้งเตือนผ่านทางแอปพลิเคชันไลน์ คิดเป็น 100 เปอร์เซ็นต์ ซึ่งผลการทดสอบโดยรวมอยู่ในระดับที่ดีมาก ซึ่งค่าความผิดพลาดเกิดจากการสแกนลายนิ้วมือของผู้ที่ทำงาน บางครั้งการสแกนนิ้วเร็วหรือช้าเกินไป ทำให้การอ่านข้อมูลของเครื่องสแกนลายนิ้วมือและถ่ายภาพใบหน้าอาจเกิดการอ่านที่ผิดพลาดหรือกรณีที่ลายนิ้วมือที่มีการลอกหรือกรณีอื่น ๆ ก็อาจมีผลทำให้ระบบตรวจสอบผิดพลาดได้

สรุปผลการวิจัย

จากผลการวิจัยพบว่า ระบบสแกนลายนิ้วมือและจับภาพใบหน้าด้วยเทคโนโลยีอินเทอร์เน็ตทุกสรรพสิ่งสำหรับห้องแม่ข่ายสามารถทำการยืนยันตัวตนบุคคลที่มีสิทธิ์เข้าใช้พื้นที่ระบบโดยการแยกรายละเอียดตามแต่ละส่วน คือ ส่วนที่มีข้อมูลของบุคคลอยู่ในฐานข้อมูลแล้ว ผลการสแกนลายนิ้วมือมีความแม่นยำ คิดเป็น 90 เปอร์เซ็นต์ ผลการถ่ายภาพใบหน้า คิดเป็น 95 เปอร์เซ็นต์ ผลการบันทึกข้อมูลคิดเป็น 100 เปอร์เซ็นต์ และผลการแจ้งเตือนผ่านทางแอปพลิเคชันไลน์ คิดเป็น 100 เปอร์เซ็นต์ โดยหากเปรียบเทียบกับงานวิจัยที่ผ่านมา

ค่าความแม่นยำในการตรวจสอบลายนิ้วมือมีค่าความแม่นยำที่สูงกว่า ซึ่งในการพัฒนาค่าความแม่นยำในการตรวจสอบลายนิ้วมืออาจใช้เซ็นเซอร์ที่มีคุณภาพมากกว่านี้ก็จะทำให้ระบบมีความแม่นยำในการตรวจสอบมากขึ้น

เอกสารอ้างอิง

- Adulkasem, S., Preechasuk, J., Rongrat, J., & Tangsirimongkol, W. (2007). System Access Control Model using Fingerprint verification. *Information Technology Journal*, 3(1), 24-28.
- Sillapakitkosol, A., Prakobdee, C., & Suthamma, P. (2010). *Fingerprint Scanner to Open and Close The Door*. Faculty of Engineering. Suranaree University Technology.
- Pongkan, P., & Boonto, W. (2018). *Real Time Class Roll Call System by Fingerprint*. Faculty of Engineering. Burapha University.
- Triprapin, K., Naudom, P., & Kongchai, P. (2018). Attendance Monitoring System with Face Recognition Technologies. *Science and Technology Journal*, 20(2), 92-105.