ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

ชนิดา รูปเลิศ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

มหาวิทยาลัยธุรกิจบัณฑิตย์

พ.ศ. 2563

Identity Authentication System for Confidential Digital Document

Chanida Rooblert

A Thematic Paper Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering

Department of Computer and Telecommunication Engineering

College of Innovative Technology And Engineering,

Dhurakij Pundit University

2020

ใบรับรองสารนิพนธ์

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

หัวข้อสารนิพนธ์ ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

เสนอโดย ร้อยโทหญิงชนิดา รูปเลิศ

สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม

อาจารย์ที่ปรึกษาสารนิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.ณรงค์เดช กีรติพรานนท์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบสารนิพนธ์แล้ว

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร.ลัญฉกร วุฒิสิทธิกุลกิจ)

.....กรรมการและอาจารย์ที่ปรึกษาสารนิพนธ์

(ผู้ช่วยศาสตราจารย์ ดร.ณรงค์เดช กีรติพรานนท์)

.....กรรมการ

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์รับรองแล้ว

.....คณบดีวิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

(ผู้ช่วยศาสตราจารย์ ดร.ณรงค์เดช กีรติพรานนท์)

วันที่ 11 เดือน ก.ค. พ.ศ. 2563

หัวข้อสารนิพนธ์ ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ
ชื่อผู้เขียน ชนิดา รูปเลิศ
อาจารย์ที่ปรึกษา ผศ.ดร.ณรงค์เดช กีรติพรานนท์
สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม
ปีการศึกษา 2561

บทคัดย่อ

ปัจจุบันระบบการรับ-ส่ง หนังสือราชการของสำนักงานปลัดกระทรวงกลาโหมนั้น ได้พัฒนาเป็นการรับ-ส่ง รูปแบบออนไลน์ในระบบงานสารบรรณอิเล็กทรอนิกส์ โดยไม่รวมการรับ-ส่ง หนังสือราชการชั้นความลับ ซึ่งแยกการปฏิบัติโดยควบคุมการรับ-ส่ง แบบสมุดทะเบียนของทางราชการ ดำเนินการผ่านสายงานธุรการเพื่อจัดส่งเอกสารให้ผู้รับปลายทาง บางครั้งผู้บังคับบัญชาไม่ต้องการเปิดเผยข้อมูลชั้นความลับให้ผู้ใดได้รับทราบนอกจากผู้รับปลายทางเท่านั้น เนื่องจากอาจจะมีการสำเนาเอกสารข้อมูลระหว่างทางการเดินของเอกสาร ทำให้ข้อมูลรั่วไหลอาจถูกเปิดเผยไปสู่บุคคลที่ไม่ประสงค์ดีต่อองค์กร และส่งผลกระทบต่อความมั่นคงต่อประเทศได้ เพื่อแก้ปัญหานี้จึงมีแนวคิดในการพัฒนาระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับขึ้น

ระบบการรับ-ส่ง หนังสือราชการชั้นความลับของเหล่าทัพอื่นนั้น ซึ่งอยู่ในรูปแบบออนไลน์ ในส่วนการเข้าถึงชั้นความลับนั้น โดยใช้ User และ Password ที่แตกต่างกันเพื่อยืนยันตัวบุคคล จำนวน 2 ครั้ง ซึ่งผู้วิจัยเห็นว่ายังคงมีช่องโหว่ในการยืนยันตัวบุคคล จึงได้พัฒนาระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ ซึ่งเป็นการพัฒนาต่อยอดจากระบบการจัดการเนื้อหาของเว็บไซต์ (Content Management System) บนแพลทฟอร์มของ ดรูพอล (Drupal) ภายในหน่วยงานของสำนักงานปลัดกระทรวงกลาโหมเดิมที่มีอยู่แล้ว โดยนำอุปกรณ์สแกนลายนิ้วมือ (Fingerprint Sensor) เพื่อยืนยันตัวบุคคลผู้ที่มีสิทธิ์ในการเข้าถึงข้อมูลเอกสารชั้นความลับ โดยการเขียนโปรแกรมภาษาไพธอน (Python) เพื่อบริหารจัดการลายนิ้วมือและส่งข้อมูลลายนิ้วมือไปยังระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

จากการทดสอบการทำงาน ระบบสามารถเชื่อมต่อกับอุปกรณ์สแกนลายนิ้วมือ (Fingerprint Sensor) และยืนยันตัวบุคคลผู้ที่มีสิทธิ์ในการเข้าถึงข้อมูลชั้นความลับได้ดี โดยให้บุคคลที่ปฏิบัติงานเกี่ยวข้องในระบบงานทำการทดสอบและประเมินผลความพึงพออยู่ในระดับความพึงพอใจมากที่สุด คิดเป็นร้อยละ 93.96 บรรลุวัตถุประสงค์และขอบเขตของสารนิพนธ์ที่ตั้งไว้

Thematic Paper Title	Identity Authentication System for Confidential Digital Document
Author	Chanida Rooblert
Thematic Paper Advisor	Asst.Prof.Dr. Narongdech Keeratipranon
Department	Computer and Telecommunication Engineering
Academic Year	2019

ABSTRACT

Nowadays official documents within Office of the Permanent Secretary for Defence (OPSD) are transferred through the Electronic Office Automation (E-Office), however E-Office confidential office documents are not transferred through this process. The process of sending-receiving confidential office documents is done manually by administrators who control the official registration book. Sometimes, the commander does not want to disclose confidential information to anyone other than the recipient leading to information leakage, which may affect the stability of the country. To solve this problem, I propose to develop an identity verification system for sending and receiving secret government documents.

E-Authentication for confidential documents in the Army, Air Force and Navy are accessed through the system using various username and password to verify their identity. However, this method of identification is flawed, as anyone knowing the password can access the system. The proposed solution is to develop an Identity Authentication System for Confidential Document by using Drupal, a Content Management System (CMS) to manage the confidential documents, and the use of a fingerprint scanner which will be used to verify the identity of the user. Python is used to send the fingerprint information to the Identity Authentication System for Confidential Documents.

It can be concluded that the test run of E-Authentication for confidential documents can connect with a Fingerprint scanner and work perfectly to verify the identity of those whom have access to the confidential document. The test involves personnel involved with this process to use and evaluate the satisfaction which results to 93.96% satisfaction, which achieves the objective and scope of the thesis.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จลุล่วง และบรรลุวัตถุประสงค์ โดยได้รับความอนุเคราะห์อย่างสูงยิ่งจากอาจารย์ ผศ.ดร.ณรงค์เดช กีรติพรานนท์ อาจารย์ที่ปรึกษาสารนิพนธ์ซึ่งท่านได้สละเวลาให้คำปรึกษา ให้แนวคิด คำแนะนำและข้อคิดเห็นต่างๆ พร้อมทั้งให้ความเมตตา และกำลังใจแก่ผู้วิจัยมาโดยเสมอมา ทำให้สารนิพนธ์ฉบับนี้เสร็จเรียบร้อย จึงขอกราบขอบพระคุณเป็นอย่างยิ่งมา ณ โอกาสนี้

ขอกราบขอบพระคุณ อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ รศ.ดร.ลัญฉกร วุฒิสิทธิกุล คณะกรรมการสอบสารนิพนธ์ที่สละเวลามาเป็นกรรมการสอบสารนิพนธ์ กรุณาให้คำแนะนำที่เป็นประโยชน์ต่องานวิจัย ขอกราบขอบพระคุณอาจารย์ทุกท่านในสาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมานาคม เจ้าหน้าที่ทุกท่าน ที่ช่วยดำเนินเรื่องต่างๆให้เป็นอย่างดี ขอขอบคุณเพื่อนๆ ร่วมรุ่นทุกท่านที่คอยช่วยเหลือกันตลอดมา

สุดท้ายนี้ ผู้วิจัยขอขอบพระคุณบิดามารดา และสมาชิกในครอบครัวทุกคน ซึ่งเปิดโอกาสให้ได้รับการศึกษาเล่าเรียนแก่ผู้วิจัยตั้งแต่วัยเยาว์ ให้ความรัก ความเข้าใจ คอยช่วยเหลือและเป็นกำลังใจสำคัญผู้วิจัยเสมอมาจนสำเร็จการศึกษา

ชนิดา รูปเลิศ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

สำนักงานปลัดกระทรวงกลาโหมได้ดำเนินการใช้ระบบงานสารบรรณอิเล็กทรอนิกส์ในการควบคุมการ รับ - ส่ง หนังสือราชการ แบบออนไลน์ โดยได้รับการสนับสนุนระบบงานสารบรรณอิเล็กทรอนิกส์จาก สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ซึ่งเป็นระบบที่รัฐบาลส่งเสริมให้ส่วนราชการนำไปใช้ประโยชน์และสามารถแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ ที่มีมาตราฐาน เพื่อให้เป็นไปตามนโยบายของรัฐบาล และเพิ่มประสิทธิภาพการปฏิบัติราชการของสำนักงานปลัดกระทรวงกลาโหม รวมถึงเกิดผลสัมฤทธิ์การลดการใช้กระดาษอย่างเป็นรูปธรรม

ปัจจุบันระบบการรับ-ส่ง หนังสือชั้นความลับของสำนักงานปลัดกระทรวงกลาโหมนั้นต้องดำเนินการผ่านสายงานธุรการ เพื่อจัดส่งเอกสารฉบับจริงให้ผู้รับปลายทาง บางครั้งผู้บังคับบัญชาไม่ต้องการเปิดเผยข้อมูลชั้นความลับให้ผู้ใดได้รับทราบนอกจากผู้รับปลายทางเท่านั้น เนื่องจากอาจจะมีการสำเนาเอกสารข้อมูลระหว่างทางการเดินของเอกสาร ทำให้ข้อมูลรั่วไหลอาจถูกเปิดเผยไปสู่บุคคลที่ไม่ประสงค์ดีต่อองค์กร อาจส่งผลกระทบต่อความมั่นคงต่อประเทศได้ ซึ่งระบบการ รับ-ส่ง เอกสารชั้นความลับจำเป็นต้องมีกระบวนการที่รัดกุม เข้มงวด สามารถยืนยันตัวบุคคลได้ว่าบุคคลนั้น มีสิทธิ์เข้าถึงหนังสือชั้นความลับได้หรือไม่

ผู้บังคับบัญชามีนโยบายให้ข้าราชการทุกระดับชั้น จะต้องรักษา ปกป้อง และปกปิดความลับทางราชการไม่ให้เผยแพร่สู่บุคคลที่ไม่เกี่ยวข้อง โดยปัจจุบันมีมาตราการการควบคุมหนังสือชั้นความลับอยู่ในการกำกับดูแลของนายทหารชั้นความลับ ซึ่งการนำสารนั้นจะใช้วิธีการปกปิดข้อมูลโดยการใส่ซองซ้อนกันสองชั้น เพื่อเป็นการปกปิดข้อมูล โดยเป็นการปฏิบัติกันมาแต่ดั้งเดิมจนถึงปัจจุบัน

ดังนั้นจึงมีแนวความคิดพัฒนาและออกแบบระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ ระหว่างผู้บังคับบัญชากับผู้บังคับบัญชาโดยตรง ไม่ผ่านสายงานธุรการ ซึ่งการใช้งานนั้นจะเป็นการรับ-ส่ง จากต้นทาง และปลายทางเท่านั้น ผ่านการสแกนลายนิ้วมือเพื่อ

ยืนยันตัวบุคคลผู้ที่มีสิทธิ์ในการเข้าถึงข้อมูลเอกสารชั้นความลับได้อย่างถูกต้อง และเป็นการปกปิดข้อมูลของเอกสารชั้นความลับที่รัดกุมและปลอดภัย

1.2 วัตถุประสงค์

1.2.1 เพื่อสร้างระบบบริหารจัดการสแกนลายนิ้วมือเพื่อยืนยันตัวบุคคล

1.2.2 พัฒนาระบบ รับ-ส่ง หนังสือราชการชั้นความลับให้มีการเชื่อมต่อกับ Finger Print

1.2.3 เพื่อทดสอบระบบ รับ-ส่ง หนังสือราชการชั้นความลับ สำหรับสรุปผลให้ผู้บังคับบัญชาระดับสูงของสำนักงานปลัดกระทรวงกลาโหม พิจารณาต่อไป

1.3 ขอบเขต

1.3.1 สร้างระบบบริหารจัดการลายนิ้วมือ โดยมีรายละเอียดดังนี้

1.3.1.1 ศึกษาการทำงานของ Finger Print

1.3.1.2 ศึกษาการเขียนโค้ดโดยใช้ภาษา Phyton ในการสร้างระบบบริหารจัดการลายนิ้วมือ

1.3.1.3 ออกแบบระบบบริหารจัดการลายนิ้วมือให้สามารถ เพิ่ม, ลบ และ ค้นหาลายนิ้วมือ พร้อมทั้งส่งข้อมูลไปยังเว็บไซต์

1.3.1.4 ศึกษาการส่งข้อมูลของ Finger Print ไปยังเว็บไซต์

1.3.2 พัฒนาและออกแบบระบบ รับ-ส่ง หนังสือราชการชั้นความลับ ให้มีการเชื่อมต่อกับ Finger Print โดยมีรายละเอียดดังนี้

1.3.2.1 ศึกษาระบบงานเดิมที่ใช้สมุดทะเบียน รับ-ส่ง ในการคุมหนังสือ และระบบงานสารบรรณอิเล็กทรอนิกส์เดิมที่เคยใช้ภายในหน่วยงานสำนักงานปลัดกระทรวงกลาโหม

1.3.2.2 ศึกษาทำความเข้าใจ Finger Print ในการเชื่อมต่อผ่านสาย USB

1.3.2.3 พัฒนาระบบงานสารบรรณอิเล็กทรอนิกส์เดิมให้สามารถเชื่อมต่อ Finger Print โดยมีรายละเอียดดังนี้

1.3.2.3(1) เพิ่มหน้าต่างเว็บไซต์ในส่วนของการตรวจสอบลายนิ้วมือผู้มีสิทธิ์ในการเปิดไฟล์เอกสาร

1.3.2.3(2) การแนบไฟล์นั้นอยู่ในรูปแบบไฟล์นามสกุล .pdf เท่านั้น

1.3.2.3(3) แบ่งสิทธิ์การใช้ระบบงานเป็น 2 ระดับ คือเลขาประจำผู้บังคับบัญชา(นายทหารคนสนิท) สามารถเข้าถึงชื่อหัวข้อเท่านั้น ไม่สามารถเข้าถึงรายละเอียดข้อมูลได้และผู้บังคับบัญชา สามารถเข้าถึงรายละเอียดข้อมูลได้

1.3.3 เพื่อทดสอบระบบ รับ-ส่ง หนังสือราชการชั้นความลับ สำหรับสรุปผลให้ผู้บังคับบัญชาระดับสูงของสำนักงานปลัดกระทรวงกลาโหม โดยมีรายละเอียดดังนี้

1.3.3.1 ทำการติดตั้งเว็บไซต์บน localhost ภายในหน่วยงานของสำนักงานปลัดกระทรวงกลาโหม

1.3.3.2 ให้ผู้ปฏิบัติงานทางด้านงานสารบรรณและผู้เกี่ยวข้องทำการทดสอบระบบงาน

1.3.3.3 ทำแบบสอบถามแสดงความคิดเห็น หลังจากการทำการทดสอบระบบงาน

1.3.3.4 สรุปผลนำเรียนผู้บังคับบัญชาเพื่อประกอบการพิจารณาต่อไป

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่จะได้รับจะแบ่งออกเป็น 2 ส่วน ดังนี้

1.4.1 ส่วนของผู้ใช้งาน

1.4.1.1 ป้องปรามไม่ให้ข้าราชการ รับ-ส่งหนังสือราชการ ปฏิบัติงานหละหลวม

1.4.1.2 ข้อมูลชั้นความลับถึงมือผู้รับผิดชอบโดยตรง

1.4.1.3 ลดขั้นตอนการทำงาน ทำให้รวดเร็วในการปฏิบัติงาน

1.4.2 ส่วนของหน่วยงาน

1.4.2.1 ป้องกันความลับทางราชการรั่วไหล

1.4.2.2 การดำเนินงานเพื่อสั่งการรวดเร็ว

1.4.2.3 สร้างความเชื่อมั่นในขบวนการทำงานของระบบงานราชการไทย

1.5 วัสดุอุปกรณ์

1.5.1 Hardware

1.5.1.1 Notebook

1.5.1.2 Fingerprint Sensor Module

1.5.1.3 สาย USB Port

1.5.2 Software

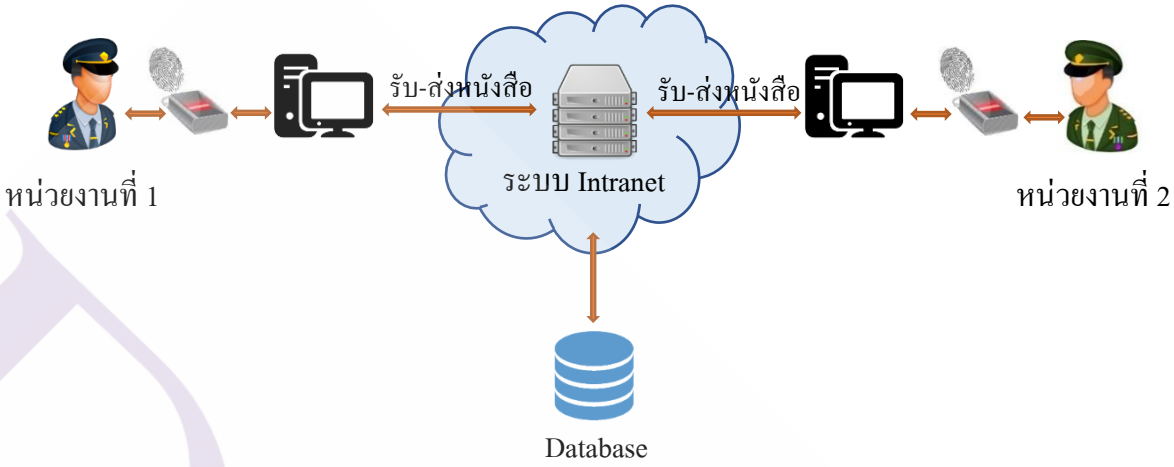
1.5.2.1 Content Management System ของ Drupal

1.5.2.2 โปรแกรม Python สำหรับเขียนคำสั่งบริหารจัดการลายนิ้วมือและส่งข้อมูลลายนิ้วมือไปยังระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

1.5.2.3 โปรแกรม Mysql เป็นฐานข้อมูล

1.5.2.4 โปรแกรม Xampp ไว้จำลอง web serve

1.6 ภาพรวมของระบบงาน



ภาพที่ 1.1 ภาพรวม ระบบการรับ-ส่ง หนังสือราชการชั้นความลับ

จากภาพที่ 1 สามารถอธิบายภาพรวมของระบบการรับ-ส่ง หนังสือราชการชั้นความลับได้ว่า เมื่อหนังสือราชการชั้นความลับได้รับการอนุมัติให้ส่งหนังสือไปยังผู้รับ หน่วยงานต้นทางจะทำการแนบไฟล์เอกสารส่งผ่านระบบงาน และเมื่อผู้รับปลายทางต้องการรับหนังสือ จะต้องสแกนลายนิ้วมือเพื่อตรวจสอบสิทธิ์ในการเข้าถึงข้อมูลชั้นความลับ

1.7 แผนการดำเนินงาน

ผู้วิจัยได้วางแผนการและระยะเวลาดำเนินงาน โดยแบ่งขั้นตอนดำเนินงานเป็น 7 ขั้นตอน และใช้ระยะเวลาในการดำเนินงานทั้งสิ้นเป็นเวลา 11 เดือน โดยเริ่มต้นตั้งแต่เดือนพฤษภาคม พ.ศ.2562 จนถึงเดือนมีนาคม พ.ศ.2563 โดยรายละเอียดของแผนการดำเนินงานดูได้จากตารางที่ 3.1

ตารางที่ 1.1 แผนการดำเนินงาน

เดือน / รายละเอียด	2562						2563				
	ก.ค.	ส.ค	ก.ย	ต.ค	พ.ย	ธ.ค	ม.ค	ก.พ	มี.ค	เม.ย.	พ.ค.
1. เลือกปัญหาที่สนใจและนำเสนอหัวข้อโครงการ	←	→									
2. ศึกษาระบบงานในปัจจุบันและแนวทางการแก้ไขปัญหา		←	→								
3. ออกแบบระบบฐานข้อมูล				←	→						
4. พัฒนาระบบ						←	→				
5. ทดสอบการใช้งานและปรับปรุงระบบ							←	→			
6. สรุปผลการดำเนินงาน								←	→		
7. เขียนรายงานฉบับสมบูรณ์และนำเสนอ										←	→

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

2.1 ระเบียบว่าด้วยการรักษาความลับของราชการ พ.ศ.2544

2.1.1 ความหมายของข้อมูลข่าวสารลับ

ข้อมูลข่าวสารลับ หมายความว่า ข้อมูลข่าวสารตามมาตรา 14 หรือมาตรา 15 ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด ตามระเบียบนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐ

2.1.2 ความหมายของชั้นความลับของข้อมูลข่าวสารลับ

แบ่งออกเป็น 3 ชั้น คือ

2.1.2.1 ลับที่สุด (TOP SECRET) หมายถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

2.1.2.2 ลับมาก (SECRET) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

2.1.2.3 ลับ (CONFIDENTIAL) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

2.1.3 หน้าที่ของเจ้าหน้าที่นำสารและผู้อารักขาการนำสาร

2.1.3.1 รักษาความปลอดภัยของข้อมูลข่าวสารลับตลอดเวลาที่นำออกนอกบริเวณหน่วยงานและเก็บรักษาข้อมูลข่าวสารลับที่อยู่ในความดูแลให้ความปลอดภัย

2.1.3.2 จัดส่งข้อมูลข่าวสารลับแก่นายทะเบียนข้อมูลข่าวสารลับ ถ้านายทะเบียนข้อมูลข่าวสารลับหรือผู้ปฏิบัติการแทนไม่อยู่หรือไม่อาจปฏิบัติหน้าที่ได้ให้ส่งข้อมูลข่าวสารลับนั้นแก่ผู้รับตามจ่าหน้า ถ้าผู้รับตามจ่าหน้าไม่อยู่หรือไม่อาจปฏิบัติหน้าที่ได้ ให้นำข้อมูลข่าวสารลับกลับมาเก็บรักษาที่หน่วยงานของตน และแจ้งให้นายทะเบียนข้อมูลข่าวสารลับบันทึกไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับหรือในกรณีที่สถานที่นำส่งอยู่ห่างจากหน่วยงานของรัฐที่ส่งและ

ไม่สามารถเดินทางกลับภายในวันเดียวกันได้ ให้เก็บรักษาไว้ในที่ปลอดภัยจนกว่าจะส่งมอบแก่นายทะเบียนข้อมูลข่าวสารลับหรือผู้รับตามจ่าหน้าแล้วแต่กรณี

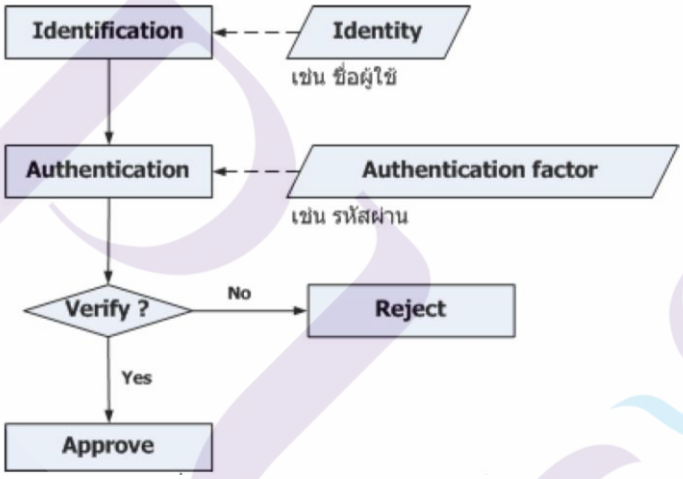
ในกรณีที่เจ้าหน้าที่นำสารไม่สามารถปฏิบัติหน้าที่ได้ ให้ผู้อารักขาการนำสารปฏิบัติหน้าที่แทนและให้รายงานนายทะเบียนข้อมูลข่าวสารลับทราบโดยเร็ว

2.2 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

2.2.1 การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)

2.2.2 การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง



ภาพที่ 2.1 แสดงแผนผังแสดงการพิสูจน์ตัวตน

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบซึ่งในขั้นตอนนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ

หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

- Actual identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

- Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

- สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น

- สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs) เป็นต้น

- สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

เปรียบเทียบข้อดีข้อเสียของการพิสูจน์ตัวตนแต่ละชนิด

ตารางที่ 2.1 การเปรียบเทียบข้อดีข้อเสียของการพิสูจน์ตัวตนแต่ละชนิด

การพิสูจน์ตัวตน	**ข้อดี**	**ข้อเสีย**
ไม่มีการพิสูจน์ตัวตนตน	ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ	ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่
การพิสูจน์ตัวตนโดยใช้รหัสผ่าน	สามารถใช้ได้กับทุกระบบ	จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็น

		สาธารณะหรือไม่มีการเข้ารหัสข้อมูล
การพิสูจน์ตัวตนโดยใช้ PIN	- ง่ายต่อการจำและความปลอดภัยค่อนข้างดี (บัตร ATM) - สามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่างปลอดภัย	- ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN - ไม่สามารถใช้กับต่างระบบกันได้ - ราคาแพง
การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens แบบซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - ผู้ที่ละเมิดเข้ามาไม่สามารถจะเข้ามาจู่โจมได้	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - authenticator เป็นวัตถุจึงง่ายต่อการสูญหายและการถูกขโมยได้
การพิสูจน์ตัวตนตนโดยใช้ password authenticators หรือ tokens แบบอะซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่าน แบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - เป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับ วิธีการใช้การพิสูจน์ตัวตนโดยใช้ password authenticators หรือ tokens	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - authenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้ไม่สามารถป้องกันผู้ที่ละเมิดเข้ามาในระบบได้ - การใช้งานค่อนข้างยุ่งยากกว่าวิธีการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" วิธีอื่น ๆ
การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล	มีความปลอดภัยสูงเพราะเลียนแบบกันได้ยาก	- ระบบมีความซับซ้อนสูง - ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย - ค่าใช้จ่ายสูง
การพิสูจน์ตัวตนโดยวิธี One-Time Password	ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก	- ไม่สะดวกต่อการใช้งานเพราะผู้ใช้ต้องจำรหัสผ่านหลายตัว

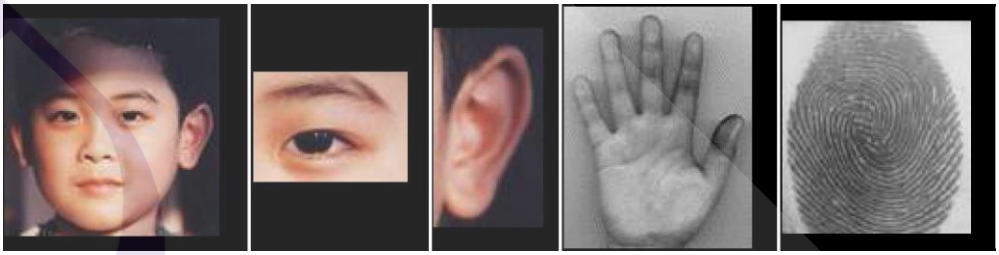
		- ถ้าผู้ใช้จำรหัสผ่านไม่ได้ หรือ ทำรหัสผ่านสูญหาย ก็ไม่สามารถเข้าใช้ระบบได้
การพิสูจน์ตัวตนโดยการเข้ารหัสแบบคู่รหัสกุญแจ	- การจัดการกุญแจทำได้ปลอดภัย เพราะ ใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน - สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์	- ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก - ต้องใช้ระบบท่สนับสนุนการทำงาน
การพิสูจน์ตัวตนโดยการใช้ลายเซ็นดิจิตอล	- สามารถระบุตัวผู้ส่งได้ชัดเจน - ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามาถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่	ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
การพิสูจน์ตัวตนโดยวิธี zeroknowledge proofs	ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้ และเซิร์ฟเวอร์เท่านั้นที่ทราบ	ความซับซ้อนของระบบเพิ่มขึ้นตามความฉลาดของระบบ

2.3 ไบโอเมตริกซ์

2.3.1 นิยามและความหมายของไบโอเมตริกซ์

คำว่า Biometrics (ไบโอเมตริกซ์) หรือ Biometry โดยเป็นศาสตร์ด้านหนึ่งในการนำเอาวิธีการทางคณิตศาสตร์ หรือวิธีการทางสถิติ มาใช้ในการวิเคราะห์แก้ไขปญหาทางด้านชีววิทยาต่าง ๆ เช่น การใช้วิธีทางสถิติวิเคราะห์ผลกระทบของ มลพิษที่มีผลต่อสุขภาพของบุคคล, การวิเคราะห์ข้อมูลสภาพอากาศที่มีผลต่อการเพาะปลูกเป็นต้น แต่ความหมายของ Biometrics ด้านนี้ไม่ใช่วัตถุประสงค์หลักของกลุ่มวิจัยนี้ แต่เป็นอีก ความหมายหนึ่งของ Biometrics ซึ่งเป็น

ศาสตร์ที่เกี่ยวข้องกับการใช้กระบวนการ ในการระบุด้วยบุคคลหรือ ตรวจสอบตัวบุคคลโดยอัตโนมัติ โดยใช้ลักษณะทางกายภาพ ที่แตกต่างกันแต่ละ บุคคล เช่น รูปแบบของลายนิ้วมือ (Fingerprint) , รูปลักษณ์ของมือ (Hand Geometry), ลักษณะของเรตินา (Retina Pattern), ลักษณะของม่านตา (Iris Pattern) รูปลักษณ์ใบหน้า (Facial) เป็นต้น หรือใช้ลักษณะทางพฤติกรรมของแต่ละบุคคล เช่น เสียง (Voice) , เอกลักษณ์ ในการพิมพ์ (Keystroke Dynamics), ลักษณะท่าทางในการเดิน (Gait recognition) เป็นต้น



ภาพที่ 2.2 แสดงลักษณะต่างๆ ทางชีวภาพของคน

กระบวนการที่ท่าให้ระบบคอมพิวเตอร์สามารถระบุบุคคลได้โดยอัตโนมัติ นั้น เป็นการเลียนแบบพฤติกรรมของมนุษย์ประเภทหนึ่ง มนุษย์เราใช้วิธีการทางไบโอเมตริกซ์ในการระบุตัวบุคคลอยู่ตลอดเวลา เราใช้ลักษณะจำเพาะทางรูปร่าง ใบหน้า น้ำเสียง หรือ แม้กระทั้งกลิ่นของแต่ละบุคคลในการระบุว่าคนที่เราพบเป็นคนที่เรารู้จักหรือไม่ ดังนั้นจึงถือได้ ว่าไบโอเมตริกซ์ เป็นรูปแบบหนึ่งของปัญญาประดิษฐ์ (Artificial Intelligence) นั้นเอง

เทคโนโลยีด้านนี้เริ่มมีการนำมาประยุกติใช้งานมานับสิบปีแล้ว ทั้งในภาครัฐบาลและภาคเอกชน แต่ประสิทธิภาพและความน่าเชื่อถือได้เป็นที่น่าสงสัยอยู่ อย่างไรก็ตามการที่บุคคลโดยทั่วไป เริ่มมีการใช้งานระบบคอมพิวเตอร์เพิ่มมากขึ้น ความจำเป็นและความสำคัญในการใช้ Biometric ในการตรวจสอบตัวบุคคลก็มีความสำคัญและจำเป็นเพิ่มขึ้นไปด้วย

การระบุตัวบุคคลโดยใช้ไบโอเมตริกซ์สามารถนำมาประยุกค์ใช้งาน ได้ทั้งในภาครัฐบาลและภาคเอกชน เช่น งานทางด้านรักษาความปลอดภัย, ช่วยผู้รักษากฎหมายในการจับตัวผู้กระทำผิด, ช่วยในการตรวจสอบผู้ใช้งานของระบบเครือข่ายคอมพิวเตอร์, การวัดการระบบบริหารงานบุคคล (เช่น งานตรวจสอบเวลาการทำงาน), ช่วยในการตรวจสอบตัวบุคคลใน การซื้อขายสินค้าผ่านทางอินเทอร์เน็ต, การวัดการเรื่องการพิสูจน์ตัวบุคคลของสถาบันการเงิน เป็นต้น

2.3.2 ข้อดีของไบโอเมตริกซ์

2.3.2.1 การใช้ไบโอเมตริกซ์ ทำให้ผู้ใช้ ไม่จำเป็นต้องใช้ความจำ หรือจำเป็นต้องถือบัตรใดๆ ทำให้สะดวกและรวดเร็ว ผู้ใช้ไม่จำเป็นต้องพกบัตร และจำรหัสผ่าน อีกทั้งยังเป็นการช่วยเพิ่มความปลอดภัย และป้องกันการสูญหายของบัตรผ่าน หรือการลักลอบนำเอารหัสผ่านไปใช้

2.3.2.2 ไบโอตริกซ์ ยากต่อการปลอมแปลง และยากต่อการลักลอบนำไปใช้

2.3.2.3 การใช้ไบโอตริกซ์ ทำให้ผู้ใช้ไม่สามารถปฏิเสธความรับผิดชอบได้ เช่นในกรณีของการใช้รหัสผ่าน หรือบัตรผ่าน เจ้าของบัตรอาจอ้างได้ว่ารหัสผ่านหรือบัตรถูกผู้อื่นลักลอบนำไปใช้ แต่ถ้าใช้ การใช้การตรวจสอบหรือระบุตัวบุคคลด้วยไบโอเมตริกซ์ ทำให้ผู้ใช้ไม่สามารถปฏิเสธความรับผิดชอบได้

2.3.2.4 ช่วยลดค่าใช้จ่าย เช่น ช่วยในการป้องกันพนักงานลงเวลาแทนกัน (Buddy Punching)

2.3.2.5 ระบบจะไม่อนุญาตให้เข้าถึงข้อมูลได้ง่ายเพราะอวัยวะของร่างกายไม่ใช่สิ่งที่จะทำเลียนแบบกันได้

2.3.2.6 เทคโนโลยีการจดจำอวัยวะแบบสามมิติจะช่วยเพิ่มความปลอดภัยในระดับที่ยอดเยี่ยม

2.3.3 ข้อเสียของไบโอเมตริกซ์

ปัญหาที่สำคัญของ ไบโอเมตริกซ์ ที่ทำให้ไม่ได้ใช้กันอย่างแพร่หลายมีอยู่ 3 ประการหลัก คือ

2.3.3.1 ความเชื่อถือได้ของเทคโนโลยี ไบโอเมตริกซ์ บางประเภทยังมีความเชื่อถือได้ไม่ดีเท่าที่ควร ยังต้องการพัฒนาทั้งทางด้านทฤษฎี และทางด้านอุปกรณ์เครื่องมือ

2.3.3.2 ราคาของอุปกรณ์ที่จำเป็นเช่น เครื่องแสกนลายนิ้วมือ เครื่องแสกนเรตินา/ไอริสในดวงตา เป็นต้น ยังมีราคาค่อนข้างสูง

2.3.3.3 การยอมรับของสังคม เพราะเรื่องของความเป็นส่วนตัวของแต่ละบุคคล (Privacy) ซึ่งเรื่องนี้เป็นเรื่องที่สำคัญมากในสังคมตะวันตกแต่มีปัญหาน้อยในสังคมตะวันออก อย่างไรก็ตามทุกปัญหาที่กล่าวมาก็มีการแก้ไขและพัฒนาอย่างต่อเนื่องทั้งในด้านความรู้ความเข้าใจและราคาของอุปกรณ์ที่มีราคาถูกมากในแต่ละปี จะเป็นแรงผลักดันให้มีความนิยมใช้เทคโนโลยีไบโอเมตริกซ์กันมากขึ้น

- ไม่สามารถใช้ได้หากไม่มีอุปกรณ์เฉพาะทาง
- เนื่องจากใช้อวัยวะของร่างกายเป็นรหัสผ่าน จึงมีโอกาสโดนทำร้ายร่างกายได้ง่าย ซึ่งต่างจากรหัสผ่านและชิปโทเคน
- รหัสผ่านที่ใช้กับระบบนี่ไม่สามารถเปลี่ยนแปลงได้

2.3.4 ประเภทของไบโอเมตริกซ์

ไบโอเมตริกซ์สามารถแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือ การใช้ลักษณะทางกายภาพ (Physiological Biometrics) และการใช้ลักษณะทางพฤติกรรม (Behavioural Biometrics) ในการระบุตัวบุคคล

2.3.4.1 ลักษณะทางกายภาพ (Physiological Biometrics)

2.3.4.1 (1) ลายนิ้วมือ Fingerprint

2.3.4.1 (2) ลักษณะใบหน้า Facial Recognition

2.3.4.1 (3) ลักษณะของมือ Hand Geometry

2.3.4.1 (4) ลักษณะของนิ้วมือ Finger Geometry

2.3.4.1 (5) ลักษณะใบหู Ear Shape

2.3.4.1 (6) Iris และ Retina ภายในดวงตา

2.3.4.1 (7) กลิ่น Human Scent

2.3.4.2 ลักษณะทางพฤติกรรม (Behavioral Biometrics)

2.3.4.2 (1) การพิมพ์ Keystroke Dynamics

2.3.4.2 (2) การเดิน Gait Recognition

2.3.4.2 (3) เสียง Voice Recognition

2.3.4.2 (4) การเซ็นชื่อ Signature

2.3.5 กระบวนการในการตรวจสอบ หรือระบุตัวบุคคลด้วย Biometrics

กระบวนการในการตรวจสอบจะเป็นการใช้ลักษณะเฉพาะแบบใดก็ตามจะมีขั้นตอนเหมือนกันดังต่อไปนี้

2.3.5.1 ผู้ใช้ระบบต้องทำการให้ตัวอย่าง (Samples) ของลักษณะทางไบโอเมตริกซ์ที่จะใช้ หรือเป็นการลงทะเบียนเริ่มต้นก่อนที่จะทำการใช้ระบบ

2.3.5.2 ตัวอย่างทางไบโอเมตริกซ์ที่ถูกเก็บมาในขั้นตอนแรก จะถูกทำการแปลงและจัดเก็บ ให้เป็นแม่แบบ (Template) ที่จะใช้ในการเปรียบเทียบ

2.3.5.3 เมื่อผู้ใช้ต้องการที่จะใช้ระบบ ก็จะถูกตรวจสอบหรือระบุผู้ใช้ โดยทำการเก็บตัวอย่างไบโอเมตริกซ์ของผู้ใช้และทำการเปรียบเทียบกับแม่แบบ (Template) ที่เก็บไว้ แล้วทำการตรวจสอบความเหมือนของตัวอย่างกับแม่แบบ จากนั้นก็จะทำการอนุญาต หรือปฏิเสธการเข้ามาใช้งานระบบของผู้ใช้

เราเรียกขั้นตอนที่ 1 และ 2 ว่าเป็นขั้นตอนของการลงทะเบียน (Emrolment) ซึ่งจะเป็นการทำเพียงครั้งเดียว ก่อนการที่จะเริ่มใช้งาน ส่วนขั้นตอนที่ 3 เป็นกระบวนการตรวจสอบ (Authentication) หรือ ระบุตัวผู้ใช้ (Identification) ซึ่งผลของการตรวจสอบหรือระบุตัวผู้ใช้นี้มีผลออกมาได้ 4 กรณีคือ Correct Accept: อนุญาตให้ผู้ใช้ที่มีสิทธิใช้ระบบ เข้าใช้ระบบ, Correct Accept: ปฏิเสธผู้ที่ไม่มีสิทธิใช้ระบบ, False Accept: อนุญาตให้ผู้ที่ไม่มีสิทธิ์ เข้าใช้ระบบ จำนวนของ False Accept ถ้าคำนวณออกมาเป็นเปอร์เซ็นต์ จะเรียกว่า อัตราการอนุญาตผิดพลาด (Fase Accept Rate หรือ FAR), False Reject: ปฏิเสธผู้ใช้ที่มีสิทธิใช้ระบบ ไม่ให้เข้าระบบ จำนวนของ False Reject ถ้าคำนวณออกมาเป็นเปอร์เซ็นต์ จะเรียกว่า อัตราการปฏิเสธผิดพลาด (False Reject Rate หรือ FRR)

2.4 จำแนกลายนิ้วมือ

2.4.1 ความรู้ทั่วไปเกี่ยวกับลายนิ้วมือ ฝ่ามือ ฝ่าเท้า

2.4.1.1 เส้นนูน – เส้นร่อง (Ridges-furrows) ผิวหนังตรงบริเวณลายนิ้วมือ ฝ่ามือ นิ้วเท้า ฝ่าเท้า ของมนุษย์ประกอบด้วยลายเส้น 2 ชนิด คือ เส้นนูนและเส้นร่อง

2.4.1.1 (1) เส้นนูน คือรอยนูนที่อยู่สูงกว่าผิวหนังส่วนนอก

2.4.1.1 (2) เส้นร่อง คือรอยลึกที่อยู่ต่ำกว่าระดับของเส้นนูน

2.4.1.2 จุดสำคัญพิเศษหรือจุดตำหนิ (Special Characteristic of minutia) ลายเส้นที่อยู่บนลายนิ้วมือ ฝ่ามือ ฝ่าเท้า จะประกอบด้วยลายเส้นที่มีลักษณะเฉพาะเรียกว่าจุดลักษณะสำคัญพิเศษหรือจุดตำหนิหรือมินูเชีย ดังต่อไปนี้

2.4.1.2 (1) เส้นแตก (Ridge bifurcation หรือ fork) เป็นลายเส้นจากเส้นเดี่ยวที่แยกออกจากกันเป็นสองเส้นหรือมากกว่า หรือในทางกลับกันอาจเรียกว่าลายเส้นสองเส้นมารวมกันเป็นเส้นเดียว

ภาพที่ 2.3 เส้นแตก

2.4.1.2 (2) เส้นสั้น ๆ (short ridge) เป็นลายเส้นที่สั้นแต่ไม่สั้นมากถึงกับเป็นจุดเล็กๆ

ภาพที่ 2.4 เส้นสั้น ๆ

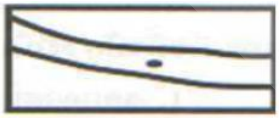
2.4.1.2 (3) เส้นทะเลสาบ (enclosure หรื lake) เป็นลายเส้นที่แยกออกเป็นสองเส้นแล้วกลับมารวมกันใหม่ จึงมีพื้นที่ปิดเกิดขึ้น

ภาพที่ 2.5 เส้นทะเลสาบ

2.4.1.2 (4) เส้นขาด (ridge beginning หรือ ending suddenly) เป็นลายเส้นจากเส้นเดี่ยวที่ขาดออกจากเส้นเดิม

ภาพที่ 2.6 เส้นขาด

2.4.1.2 (5) จุด (dot หรือ island) เป็นเส้นที่สั้นมากจนดูเหมือนเป็นจุดเล็กๆ



ภาพที่ 2.7 จุด

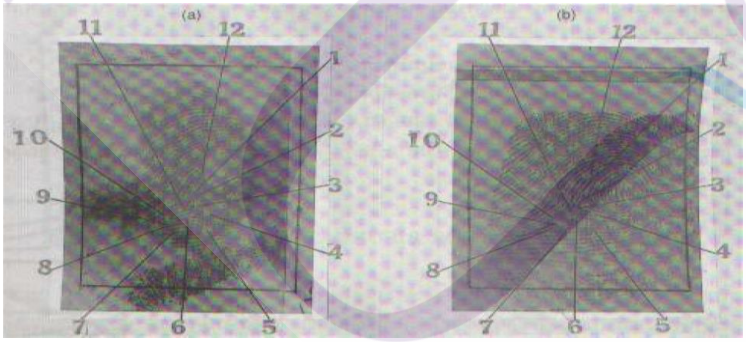
2.4.1.2 (6) ตะขอ (hook) เป็นลายเส้นของเส้นเดี่ยวแต่แยกออกเป็น 2 เส้น โดยที่เส้นหนึ่งสั้นอีกเส้นหนึ่งยาวดูคล้ายตะขอ

ภาพที่ 2.8 ตะขอ

2.4.1.2 (7) อื่นๆ (miscellaneous) เป็นลายเส้นที่มีลักษณะไม่ตรงกับแบบที่กล่าวมาแล้วเช่น เป็นลายเส้นที่แยกจากหนึ่งเส้นเป็นสามเส้นเรียก trifurcation

ภาพที่ 2.9 miscellaneous

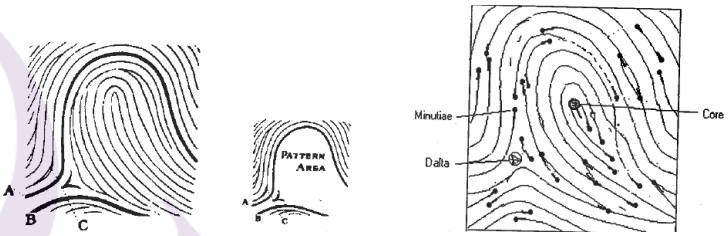
ในการตรวจพิสูจน์ จะใช้จุดตำหนิต่างๆ ดังกล่าว ยืนยันตัวบุคคล โดยปกติจะใช้จุดตำหนิตั้งแต่ 10 จุดขึ้นไป ในการยืนยันว่าเป็นลายนิ้วมือของบุคคลคนเดียวกัน



ภาพที่ 2.10 ลายนิ้วมือแฝงที่เก็บจากสถานที่เกิดเหตุกับลายพิมพ์นิ้วมือของผู้ต้องหาที่มีจุดตำหนิตรงกัน

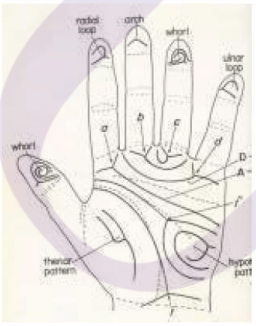
2.4.2 แบบแผนพื้นฐานของลายนิ้วมือ (finger pattern)

ลักษณะลายนิ้วมือที่ใช้ในการพิสูจน์บุคคล ดูได้จาก 2 ลักษณะใหญ่ๆ ได้แก่ลักษณะโดยรวม (global feature) และลักษณะเฉพาะที่ (local feature) ลักษณะโดยรวมคือลักษณะลายนิ้วมือที่มองเห็นได้ด้วยตาเปล่า ประกอบด้วย (1)แบบแผนลายเส้นพื้นฐาน (basic ridge pattern) (2) พื้นที่ทั้งหมดของแบบแผนลายเส้น (patten area) (3)จุดใจกลาง (core area) (4) สามเหลี่ยมเดลต้าหรือสันตอน (delta, tritadius) (5)ชนิดของเส้น (typelines) และ (6)จำนวนเส้นลายนิ้วมือ (ridge count)



ภาพที่ 2.1.1 แบบแผนลายเส้นพื้นฐาน (2)พื้นที่ทั้งหมดของแบบแผนลายเส้น (3) จุดใจกลาง (4) สามเหลี่ยมเดลต้าหรือสันตอนและ (5) จุดตำหนิ

การจำแนกแบบแผนลายเส้นพื้นฐานอาจแบ่งได้หลากหลาย แต่ที่นิยมใช้กันมากที่สุดแบ่งได้เป็น 3 แบบหลักๆได้แก่ โค้ง (arch) มัดหวาย (loop) และก้นหอย (whorl)

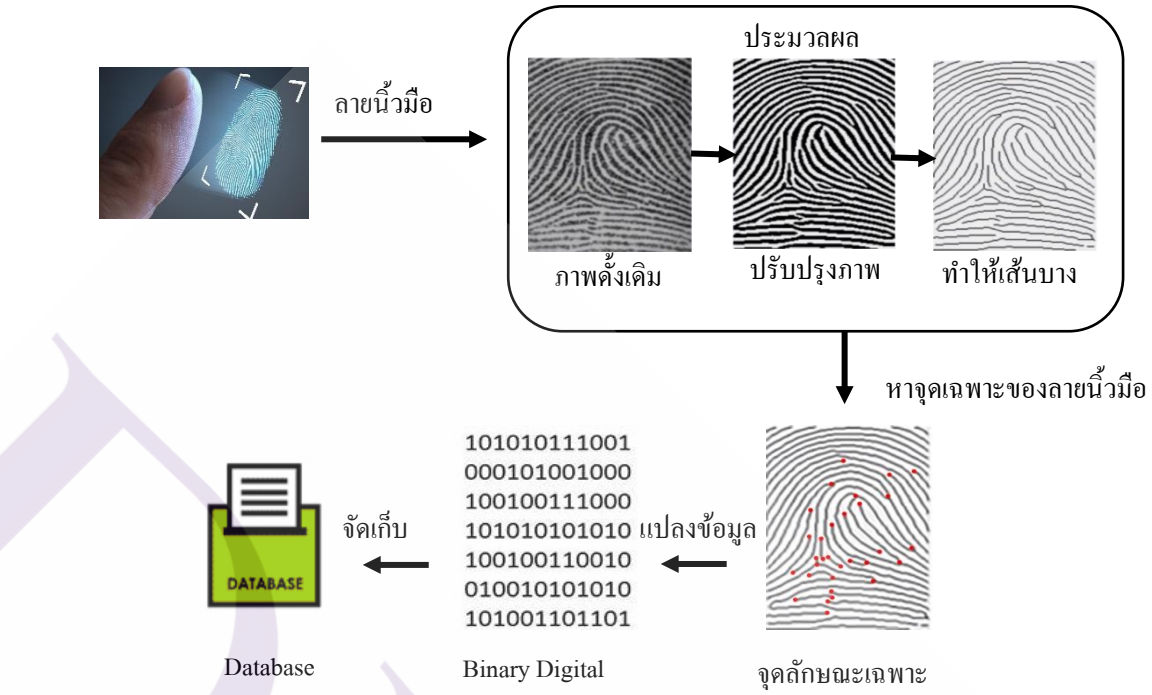


ภาพที่ 2.12 ก้นหอย (whorl) มัดหวายคู่ (double loop) มัดหวายปัดหัวแม่มือ (radial loop) โค้ง (arch) และมัดหวายปัดก้อย (ulnar loop) บนมือซ้าย

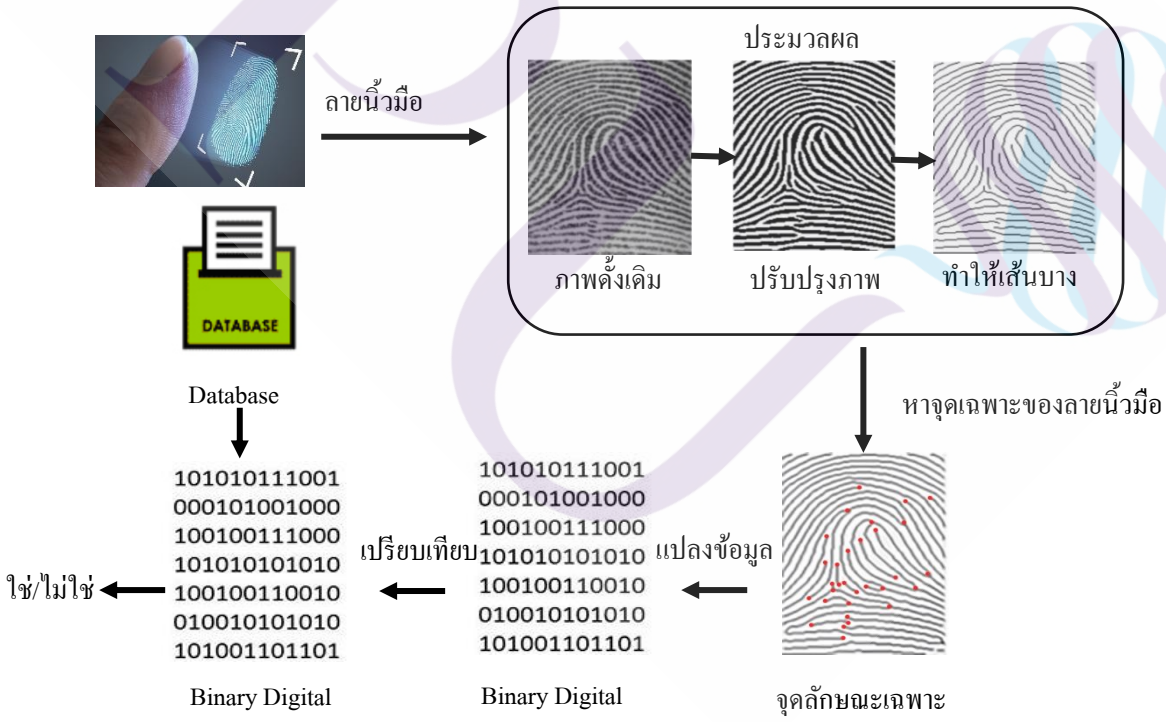
ภาพที่ 2.13 แบบแผนลายเส้นพื้นฐานสามแบบหลักๆ ได้แก่โค้ง (arch) มัดหวาย (loop) และก้นหอย (whorl)

2.5 หลักการวิเคราะห์ลายนิ้วมือ

การวิเคราะห์ลายนิ้วมือของบุคคลโดยทั่วไปนั้น จะเริ่มด้วยการนำลายนิ้วมือของแต่ละบุคคลแต่ละนิ้วมาหาจุดลักษณะเฉพาะที่สำคัญ กระบวนการแรกเริ่มของการตรวจพิสูจน์ลายนิ้วมือ คือ การอ่านภาพลายนิ้วมือเข้ามาเก็บไว้ในหน่วยความจำถาวรซึ่งในส่วนนี้จะใช้ EEPROM เป็นส่วนที่เก็บข้อมูลไว้ โดยข้อมูลที่อ่านหรือสแกนเข้ามานั้นจะนำมาผ่านการประมวลผลก่อนแล้วจึงเก็บข้อมูลนั้นไว้ ซึ่งข้อมูลนี้จะถูกเก็บไว้เป็นต้นแบบหรือรหัสของผู้ใช้แต่ละคนในขั้นตอนก่อนที่จะนำลายนิ้วเมือเข้าไปเก็บนั้นจะต้องผ่านขั้นตอนการประมวลผล ก่อนในกระบวนการนี้จะทำให้ภาพที่ได้รับการสแกนเข้ามาเกิดความสมบูรณ์มากขึ้นเพราะเมื่อเครื่องได้รับการสแกนภาพเข้ามาแล้ว ภาพที่อ่านได้อาจไม่ชัดเจน พร่าเลือน ก็จะทำให้การประมวลผลในขั้นตอนถัดไปทำได้ด้วยความยากลำบากหรือทำไม่ได้ ซึ่งจะทำให้ผลที่ได้ก็อาจไม่ถูกต้องตามที่ควรจะเกิดปัญหาในกระบวนการนี้จึงได้มีการกระทำหลายกระบวนการด้วยกันคือการกำจัดสัญญารบกวน การปรับความมือสว่างและความแตกต่างของตัวภาพและฉากของภาพ, การแปลงภาพเป็นภาพสองระดับการทำให้เส้นลายนิ่วมือบาง, และอื่นๆอีกมาก ซึ่งกระบวนการจะมากหรือน้อยขึ้นอยู่กับว่าตัวอุปกรณ์นั้นมีการอ่านค่าลายนิ่วมือที่ได้ภาพออกมาละเอียดและสมบูรณ์แค่ไหนเมื่อได้ลายนิ้วมือที่ผ่านกระบวนการประมวลผลแล้ว ก็จะนำข้อมูลหรือภาพนี้ไปจัดเก็บในหน่วยความจำถาวร (EEPROM) เพื่อใช้ในการเปรียบเที่ยบกับลายนิ้วมือต่อไป



ภาพที่ 2.14 กระบวนการจัดเก็บลายนิ้วมือ



ภาพที่ 2.15 กระบวนการเปรียบเทียบลายนิ้วมือ

จากภาพที่ 2.1.4 จะแสดงให้เห็นถึงกระบวนการเปรียบเทียบลายนิ้วมือที่ได้รับการสแกนเข้ามาโดยเริ่มที่การสแกนภาพเข้ามา แล้วทำการประมวลผลขั้นตอนเดียวกันกับการจัดเก็บตอนแรกแล้วนำภาพที่เก็บไว้ในตอนแรกมาเปรียบเทียบกับภาพที่สแกนเข้ามา ณ ตอนนั้นเพื่อเปรียบเทียบว่ามีความเหมือนหรือแตกต่างมา เพียงใดทั้ง 2 ขั้นตอนนั้นต้องผ่านการประมวลผลซึ่งจะทำให้ได้ภาพที่มีประสิทธิภาพในการเปรียบเทียบซึ่งผลที่ได้จากการทำจะทำให้ได้จุดลักษณะเฉพาะซึ่งจุดเหล่านี้เองจะเป็นสิ่งในการเปรียบเทียบลายนิ้วมือของแต่ละคนหรือกล่าวได้ว่าเป็นตัวบ่งชี้ความแตกต่างของนิ้วแต่ละคน

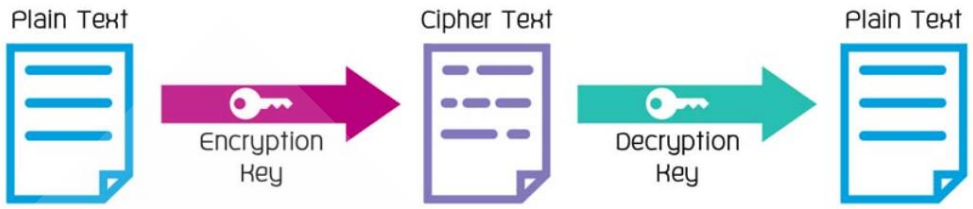
2.6 การแปลงข้อมูล

2.6.1 Encryption/Decryption

เป็นกระบวนการสำหรับการแปลงข้อมูลเล็กทรอนิกส์ธรรมดาให้อยู่ในรูปที่บุคคลทั่วไปไม่สามารถอ่านเข้าใจได้ ซึ่งโดยทั่วไปแล้วการเข้ารหัสจะกระทำก่อนการจัดเก็บข้อมูลหรือก่อนการส่งข้อมูล โดยการนำข้อมูลอิเล็กทรอนิกส์ธรรมดากับกุญแจ (Key) ซึ่งเป็นตัวเลข มาผ่านกระบวนการทางคณิตศาสตร์ ผลที่ได้ก็คือข้อมูลที่เข้ารหัส ขั้นตอนที่กล่าวมานี้จะเรียกว่า **“การเข้ารหัสลับ” (Encryption)** และเมื่อต้องการอ่านข้อมูล จะนำเอาข้อมูลที่เข้ารหัสกับกุญแจมาผ่านเข้าสู่กระบวนการทางคณิตศาสตร์ ผลลัพธ์ที่ได้ก็คือข้อมูลดั้งเดิม ซึ่งขั้นตอนนี้จะเรียกว่า **“การถอดรหัสลับ” (Decryption)**

โดยทั่วไปเทคโนโลยีระบบรหัสแบ่งได้เป็น 2 ประเภทหลัก ได้แก่ ระบบรหัสแบบสมมาตร (Symmetric Key Cryptography) และ ระบบรหัสแบบอสมมาตร (Asymmetric Key Cryptography)

2.6.1.1 ระบบรหัสแบบสมมาตร (Symmetric-key Cryptography) เป็นระบบรหัสที่ใช้กุญแจชุดเดียวกันทั้งผู้ส่งและผู้รับในการเข้าและถอดรหัสลับ จากสาเหตุนี้จึงเป็นที่มาของชื่อระบบรหัสแบบสมมาตร เนื่องจากคำว่า “สมมาตร” เป็นการอธิบายถึงความเท่ากันหรือเหมือนกันของสองข้าง ซึ่งในที่นี้ก็คือตัวกุญแจนั่นเอง กุญแจซึ่งอยู่ในรูปรหัสคอมพิวเตอร์นี้เป็นตัวแปรสำคัญสำหรับการเข้าและถอดรหัสลับข้อมูล ซึ่งขนาดของกุญแจ (มีหน่วยเป็นบิต : bit) จะแสดงถึงระดับความปลอดภัยของข้อมูลที่ได้รับการเข้ารหัสลับ โดยการใช้กุญแจที่มีความยาวหรือจำนวนบิตสูงจะทำให้การเข้ารหัสลับข้อมูลนั้นมีความปลอดภัยมากยิ่งขึ้น



ภาพที่ 2.16 การเข้ารหัสลับ (Encryption) ด้วยระบบรหัสแบบสมมาตร

2.6.1.2 ระบบรหัสแบบอสมมาตร (Asymmetric-key Cryptosystem) เป็นระบบรหัสที่ใช้กุญแจคู่ (Key Pair) ซึ่งประกอบด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) กล่าวคือ ผู้ใช้ 1 คนหรือที่เรียกว่าเจ้าของกุญแจจะใช้กุญแจคู่นี้ในการติดต่อสื่อสารกับบุคคลอื่นโดยไม่จำเป็นต้องมีกุญแจเป็นจำนวนมากเช่นเดียวกับกรณีของระบบรหัสแบบสมมาตร ทั้งนี้ในการเก็บรักษากุญแจนั้น กุญแจส่วนตัวจะต้องเก็บรักษาไว้กับเจ้าของกุญแจและห้ามไม่ให้ผู้อื่นล่วงรู้ ส่วนกุญแจสาธารณะนั้นต้องมีการประกาศให้ผู้อื่นรับรู้หรือเก็บไว้ในที่ซึ่งบุคคลอื่นสามารถเข้ามาสืบค้นได้ ในการเข้ารหัสลับข้อมูลจะต้องใช้กุญแจดอกหนึ่งในการเข้ารหัสลับและใช้กุญแจอีกดอกหนึ่งที่เป็นคู่กันในการถอดรหัสลับ เช่น หากใช้กุญแจสาธารณะในการเข้ารหัสลับก็จะต้องใช้กุญแจส่วนตัวในการถอดรหัสลับ ในทางกลับกัน หากใช้กุญแจส่วนตัวในการเข้ารหัสลับก็จะต้องใช้กุญแจสาธารณะในการถอดรหัสลับ ซึ่งวิธีการเลือกใช้กุญแจจะขึ้นอยู่กับวัตถุประสงค์ของการใช้งาน

ภาพที่ 2.17 การเข้ารหัสลับ (Encryption) ด้วยระบบรหัสแบบอสมมาตร

2.6.2 BASE64 (เบส 64) คือ วิธีการแปลงข้อมูลข้อความ หรือข้อมูลต้นฉบับไปเป็นข้อความหรือข้อมูลชุดใหม่ ที่ไม่สามารถอ่าน หรือรู้ว่าข้อมูลชุดนี้คืออะไร ซึ่งการแปลงข้อมูลชนิดนี้จะแทนที่ข้อมูลด้วยตัวอักษร 64 ตัว นั่นคือที่มาของ BASE64 ตามตัวอย่างต่อไปนี้ Table ASCII - Binary Character (เทเบิ้ล แอสกี้ ไบนารี่ ชาเรคเจอร์)

ตารางที่ 2.2 Table ASCII - Binary Character

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	s	115	01110011	K	075	01001011
b	098	01100010	t	116	01110100	L	076	01001100
c	099	01100011	u	117	01110101	M	077	01001101
d	100	01100100	v	118	01110110	N	078	01001110
e	101	01100101	w	119	01110111	O	079	01001111
f	102	01100110	x	120	01111000	P	080	01010000
g	103	01100111	y	121	01111001	Q	081	01010001
h	104	01101000	z	122	01111010	R	082	01010010
i	105	01101001	A	065	01000001	S	083	01010011
j	106	01101010	B	066	01000010	T	084	01010100
k	107	01101011	C	067	01000011	U	085	01010101
l	108	01101100	D	068	01000100	V	086	01010110
m	109	01101101	E	069	01000101	W	087	01010111
n	110	01101110	F	070	01000110	X	088	01011000
o	111	01101111	G	071	01000111	Y	089	01011001
p	112	01110000	H	072	01001000	Z	090	01011010
q	113	01110001	I	073	01001001			
r	114	01110010	J	074	01001010			

Table BASE64 (เทเบิ้ลเบส 64)

ตารางที่ 2.3 Table BASE64

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	-

2.6.2.1 วิธีการเข้ารหัส BASE64

ยกตัวอย่าง ต้องการแปลงข้อความนี้ "mind" จะมีขั้นตอนคือ

2.6.2.1 (1) นำข้อมูลที่ต้องการมาแปลงเป็นเลขฐานสอง 8 bit ดูตามตาราง Table ASCII - Binary Character

m = 01101101

i = 01101001

m = 01101101

d = 01100100

01101101 01101001 01101101 01100100

2.6.2.1 (2) จากนั้น เรียงบิตใหม่จากทางด้านซ้าย แบ่งเลขฐานสองออกเป็นชุด ชุดละ 6 bit กรณีที่ชุดสุดท้ายไม่ครบ ให้เติม 0 ไปจนครบ จะได้ดังนี้

011011 010110 100101 101101 011001 000000

** bit ที่ถูกเติมเข้าไปที่เป็น 00 แทนด้วย "="

กรณี bit สุดท้าย เป็น 000000 ก็จะได้ == สองตัวต่อ

2.6.1.1 (3) แปลงเลขฐาน 2 แบบ 6 bit เป็นเลขฐาน 10

จำนวนบิต จะเริ่มจากขวาไปซ้าย สูตรการคำนวณบิต n^2

ตารางที่ 2.4 ผลการแปลง

32	16	8	4	2	1	ผลรวมฐานสิบ
0	1	1	0	1	1	27
0	1	0	1	1	0	22
1	0	0	1	0	1	37
1	0	1	1	0	1	45
0	1	1	0	0	1	25
0	0	0	0	0	0	0

เมื่อนำไปเปรียบเทียบกับตาราง Table BASE64 จะได้ดังนี้ bWltZA==

<u>ตัวอย่างในภาษา php</u>

รูปแบบ Syntax : base64_encode (string $data) : string

ตัวอย่างการนำไปใช้ในการ encode

```
<?php
$str = 'This is an encoded string';
echo base64_encode($str);
?>
```

ผลลัพธ์ที่ได้คือ VGhpcyBpcyBhbiBlbmNvZGVkIHN0cmluZw==

2.6.2.2 วิธีการถอดรหัส BASE64

วิธีการถอดรหัส BASE64 ทำย้อนกลับให้นำข้อมูลมาแปลงเป็นฐานสอง 6 bit มาเรียงต่อกันก่อน แล้วนำมาจัดกลุ่ม กลุ่มละ 8 bit โดย bit สุดท้ายที่เหลือไม่ครบ 8 bit ให้ตัดทิ้ง หลังจากนั้นก็แปลงเลขฐานสอง 8 bit แต่ละชุดเป็นข้อมูล ASCII เท่านี้ก็จะได้ข้อมูลต้นฉบับแล้ว

ตัวอย่างการในภาษา php

รูปแบบ Syntax : base64_decode (string $data [, bool $strict = FALSE]) : string

ตัวอย่างการถอดรหัสโดยใช้ฟังก์ชันนี้

```
<?php
$str = 'VGhpcyBpcyBhbiBlbmNvZGVkIHN0cmluZw==';
echo base64_decode($str);
?>
```

ผลลัพธ์ที่ได้คือ This is an encoded string

2.6.3 MD5 ย่อมาจาก Message-Digest algorithm 5 คือ รูปแบบการใช้ฟังก์ชันHash (Cryptographic hash) คือ การแปลงรูปแบบของข้อมูลที่รับเข้ามาไม่ว่าขนาดเท่าใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ เพราะฉะนั้น จะไม่สามารถเรียกดูข้อมูลต้นฉบับได้ ทำได้เพียงตรวจสอบว่าข้อมูลที่ให้มาแต่ละครั้งเหมือนกันหรือไม่ ความปลอดภัยจึงค่อนข้างสูง ในที่นี้ MD5 เป็นการเข้ารหัสแบบ 128-bit ให้ค่าเป็นตัวเลขฐาน 16 (0123456789abcd) ขนาด 32 ตัวอักษร แต่ก็มีบางประเภทที่ให้ค่าเป็น binary และ base64

ประโยชน์ของการเข้ารหัสแบบ MD5

2.6.3.1 นำไปตรวจสอบความถูกต้องของไฟล์ สมมติว่ามีไฟล์สองไฟล์ ถ้าเนื้อหาในไฟล์เหมือนกันทุกประการ ก็จะได้ค่า MD5 เหมือนกัน แต่หากว่า ค่า MD5 ไม่ตรงกัน นั้นแสดงว่าต้องมีไฟล์ใดๆไฟล์หนึ่งที่ไม่สมบูรณ์ ซึ่งการตรวจสอบ MD5 สามารถทำได้ ด้วยการใช้โปรแกรมช่วย เช่น WinMD5Sum

2.6.3.2 นำไปใช้ในการเก็บข้อมูลที่ไม่ต้องการเปิดเผย เช่น เก็บรหัสผ่านไว้ในฐานข้อมูลการแปลงค่า MD5 ทำได้โดย วิธีการที่เรียกว่า Brute-Force (หาค่าตั้งแต่ a-z และนำไปเปรียบเทียบ จากนั้นก็เป็น aa-zz และต่อไปเรื่อยๆ) นอกเหนือไปจากนี้ยังมีวิธีการที่เรียกว่า Hash Collision (การชนกันของ Hash)

2.6.3.3 ภาพรวมของคำสั่ง md5

2.6.3.3 (1) รูปแบบคำสั่งคือ md5([MESSAGE])

2.6.3.3 (2) MD5 เป็นรูปแบบการเข้ารหัสแบบ One-Way Encapsulating หรือการเข้ารหัสแบบทางเดียว กล่าวคือ ไม่สามารถถอดรหัสได้เหมือนกับการเข้ารหัสแบบอื่น ๆ เช่น base64

ตัวอย่างโปรแกรม

```
<?
    $password = "01234";
    $md5_password = md5( $password );
    echo "Original Password = ".$password;
    echo "<br/>";
    echo "After Encapsulating with md5 = ".$md5_password;
?>
```

ผลลัพธ์ที่ได้คือ

```
1   Original Password = 01234
2   After Encapsulating with md5 = 4100c4d44da9177247e44a5fc1546778
```

2.7 การประยุกต์ใช้งาน Finger Scan

2.7.1 การใช้งาน Finger Scan ในการพิสูจน์ตัวตน ซึ่งในปัจจุบัน ได้รับการยอมรับอย่างกว้างขวาง ในทุกวงการ เช่น ทางด้านการศึกษาโดยนำ Finger Scan เข้ามาช่วยยืนยันตัวตนในการเข้าชั้นเรียนของนักเรียนนักศึกษา การส่งคืนหนังสือในห้องสมุด ทางด้านธุรกิจโดยนำ Finger Scan เข้ามาช่วยยืนยันตัวตนในการเข้าทำงานของพนักงาน เพื่อตรวจเวลาการทำงาน การขาดลามาสายของพนักงาน ทางด้านการเงินโดยนำ Finger Scan เข้ามาช่วยยืนยันตัวตนในการอนุญาตเข้าทำธุรกรรมทางการเงินของธนาคาร และอื่นอีกมากมาย

2.7.2 การใช้งาน Finger Scan ในทางทหารซึ่งนำมาประยุกต์ใช้ในหน่วยงานหลายรูปแบบ เช่นการสแกนลายนิ้วมือยืนยันตัวบุคคลในการเข้าห้องลับทางราชการเพื่อช่วยคัดกรองเฉพาะบุคคลที่สามารถเข้าไปปฏิบัติหน้าที่ ณ ห้องนั้นๆ ทำให้ห้องลับทางราชการนั้นปลอดภัยจากบุคคลที่ไม่เป็นผู้เกี่ยวข้องในการปฏบัติงาน ซึ่งจะเห็นได้ว่าทางทหารได้นำเทคโนโลยีอุปกรณ์ Finger Scan เข้ามาช่วยอำนวยความสะดวกในการปฏิบัติงาน และเพิ่มการรักษาความปลอดภัยให้กับองค์กรอีกทางหนึ่ง

2.8 สรุป

การเก็บรักษาความลับทางราชการนั้นมีความสำคัญจะต้องมีมาตราการในการรักษาข้อมูลชั้นความลับตามนโยบายของผู้บังคับบัญชา เพื่อความปลอดภัยของข้อมูล Finger scan ก็เป็นอุปกรณ์หนึ่งที่หลายองค์กรณ์นำไปประยุกต์ใช้ในหน่วยงานเพื่อพิสูจน์ตัวบุคคล เพิ่มความสะดวกรวดเร็วและทำให้การทำงานมีประสิทธิภาพมากยิ่งขึ้น

ดังนั้นการนำ Finger scan มาประยุกต์ใช้ในหน่วยงานสำนักงานปลัดกระทรวงกลาโหม เพื่อยืนยันตัวบุคคลในการรับ-ส่ง หนังสือราชการชั้นความลับนั้น จะตอบสนองนโยบายของผู้บังคับบัญชาในการเพิ่มประสิทธิภาพการรักษาความลับทางราชการมากยิ่งขึ้น

บทที่ 3
ระเบียบวิธีวิจัย

ในบทนี้จะกล่าวถึงการออกแบบของโครงงานรวมทั้งอธิบายถึงแนวทางการวิจัยและพัฒนาเครื่องมือที่ใช้ในงานวิจัย แผนการดำเนินงาน ขั้นตอนและวิธีการดำเนินงาน

3.1 แนวทางการวิจัยและพัฒนา

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา ออกแบบ และพัฒนาระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ โดยทำการศึกษาระบบงานเดิมและเพิ่มฟังก์ชั่นการรับเอกสาร โดยบุคคลที่สามารถเข้าถึงข้อมูลนั้นต้องมีการยืนยันสิทธิ์ผ่าน Fingerprint Scan เพื่อตรวจสอบสิทธิ์การเข้าถึงข้อมูล โดยมีแนวทางในการวิจัยและพัฒนาดังนี้

3.1.1 การศึกษาและวิเคราะห์ระบบ

3.1.2 การออกแบบระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

3.1.3 การออกแบบระบบสแกนลายนิ้วมือ

3.1.4 กระบวนการทำงาน ระบบการรับ-ส่ง หนังสือ

3.2 การศึกษาและวิเคราะห์ระบบ

ในขั้นตอนการศึกษาและวิเคราะห์ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ จะทำการศึกษาระบบงานเดิม โดยระบบงานรับ-ส่งหนังสือราชการของสำนักงานปลัดกระทรวงกลาโหมนั้น แบ่งเป็นการรับ-ส่งหนังสือราชการ ออกเป็น 2 ส่วน คือ การรับ-ส่งหนังสือราชการธรรมดา และ การรับ-ส่งหนังสือราชการชั้นความลับ โดยมีขั้นตอนการทำงาน ดังนี้

3.2.1 การรับ-ส่งหนังสือราชการธรรมดา

การรับ-ส่งหนังสือราชการธรรมดา จะเป็นการรับ-ส่งหนังสือในรูปแบบออนไลน์ ควบคุมการรับ-ส่ง ผ่านระบบงานสารบรรณอิเล็กทรอนิกส์ โดยมีขั้นตอนดังนี้

3.2.1.1 ผู้บังคับบัญชาเซ็นอนุมัติหนังสือราชการ ส่งหนังสือผ่านเจ้าหน้าที่ธุรการดำเนินการต่อไป

3.2.1.2 เจ้าหน้าที่ส่งหนังสือบนระบบงานสารบรรณอิเล็กทรอนิกส์

3.2.1.3 เจ้าหน้าที่นำสารส่งหนังสือให้หน่วยงานปลายทาง

3.2.1.4 เจ้าหน้าที่ปลายทางรับเอกสารฉบับจริง

3.2.1.5 เจ้าหน้าที่ปลายทางนำหนังสือราชการเสนอผู้บังคับบัญชาเพื่อสั่งการต่อไป

3.2.2 การรับ-ส่งหนังสือราชการชั้นความลับ

การรับ-ส่ง หนังสือราชการชั้นความลับ จะเป็นการรับ-ส่งหนังสือโดยใช้สมุดทะเบียนรับ-ส่ง ในการควบคุมหนังสือราชการชั้นความลับโดยมีขั้นตอนการทำงานดังนี้

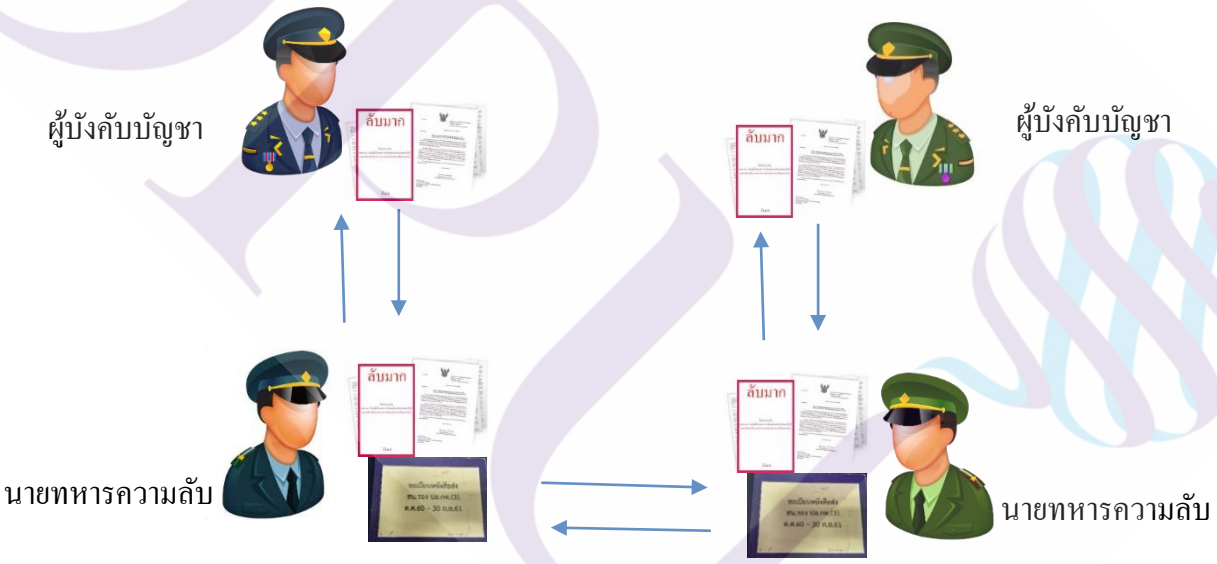
3.2.2.1 ผู้บังคับบัญชาเซ็นอนุมัติหนังสือราชการชั้นความลับ ส่งหนังสือผ่านนายทหารความลับดำเนินการต่อ

3.2.2.2 นายทหารความลับต้นทางลงบันทึกข้อมูลลงสมุดทะเบียนส่ง

3.2.2.3 นายทหารความลับนำสารหนังสือ ส่งให้หน่วยงานปลายทาง

3.2.2.4 นายทหารความลับปลายทาง ทำการบันทึกข้อมูลหนังสือลงสมุดทะเบียนรับ

3.2.2.5 นายทหารความลับปลายทาง นำหนังสือเสนอผู้บังคับบัญชาเพื่อสั่งการต่อไป

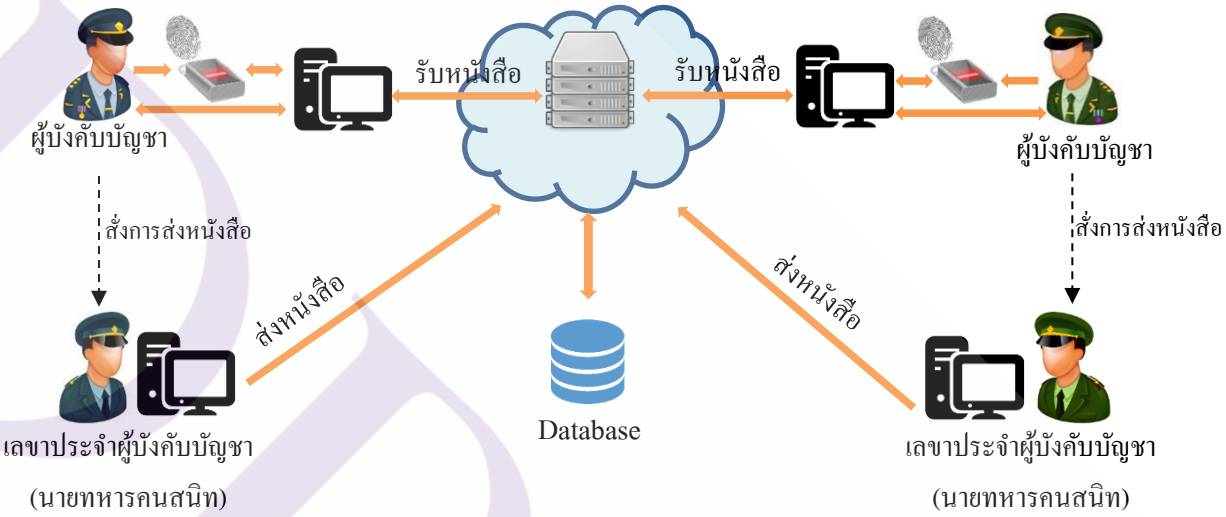


ภาพที่ 3.1 ระบบการรับ-ส่ง หนังสือราชการชั้นความลับในปัจจุบัน

3.3 การออกแบบระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

จากการศึกษาผลดำเนินงานในระบบงานเดิมนั้น ทำให้ทราบถึงปัญหาและข้อบกพร่องของกระบวนการ รับ -ส่ง หนังสือราชการชั้นความลับ ซึ่งกระบวนการทำงานเดิมไม่สามารถรักษาความลับทางราชการให้ปลอดภัยได้อย่างแท้จริง จึงได้นำระบบงานสารบรรณอิเล็กทรอนิกส์ที่ใช้

ในการรับ-ส่งหนังสือราชการธรรมดา มาพัฒนาและออกแบบให้สามารถรับ-ส่งหนังสือราชการชั้นความลับให้มีการรักษาความปลอดภัยของข้อมูล และยกเลิกการนำสารเอกสารฉบับจริงซึ่งเป็นข้อบกพร่องของการรักษาความลับของข้อมูล โดยจะเป็นการส่งเอกสารในรูปแบบไฟล์เอกสาร และนำอุปกรณ์ Fingerprint Sensor มายืนยันตัวบุคคลในการเข้าถึงข้อมูลชั้นความลับ โดยมีกระบวนการออกแบบระบบงาน ดังนี้



ภาพที่ 3.2 ภาพรวม ระบบการรับ-ส่ง หนังสือราชการชั้นความลับใหม่

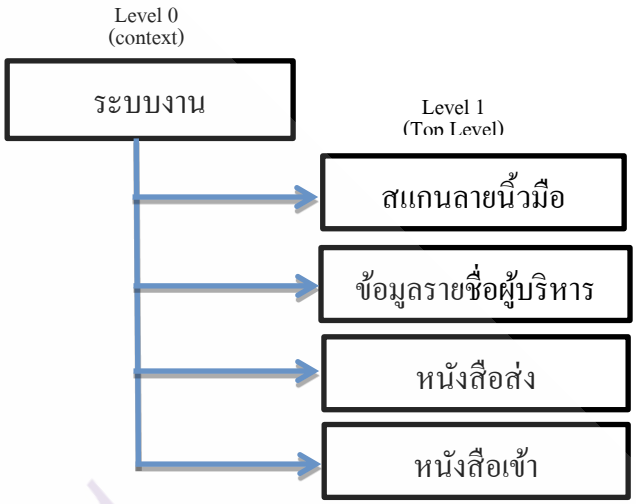
จากภาพที่ 3.2 สามารถอธิบายภาพรวมของระบบการรับ-ส่ง หนังสือราชการชั้นความลับโดยมีขั้นตอนดังนี้

1. เมื่อหนังสือราชการชั้นความลับได้รับการอนุมัติจากผู้บังคับบัญชาให้ส่งหนังสือ เลขาประจำผู้บังคับบัญชาจะทำการแนบไฟล์และส่งหนังสือไปยังผู้รับปลายทาง ผ่านระบบงานบนระบบ Localhost

2. ผู้รับที่สามารถรับหนังสือได้คือผู้บังคับบัญชาของแต่ละหน่วยงาน โดยการแสกนลายนิ้วมือเพื่อตรวจสอบสิทธิ์การเข้าถึงข้อมูล

3. เมื่อตรวจสอบสิทธิ์ในการรับหนังสือแล้วถูกต้องระบบจะอนุญาตให้เปิดไฟล์หนังสือ

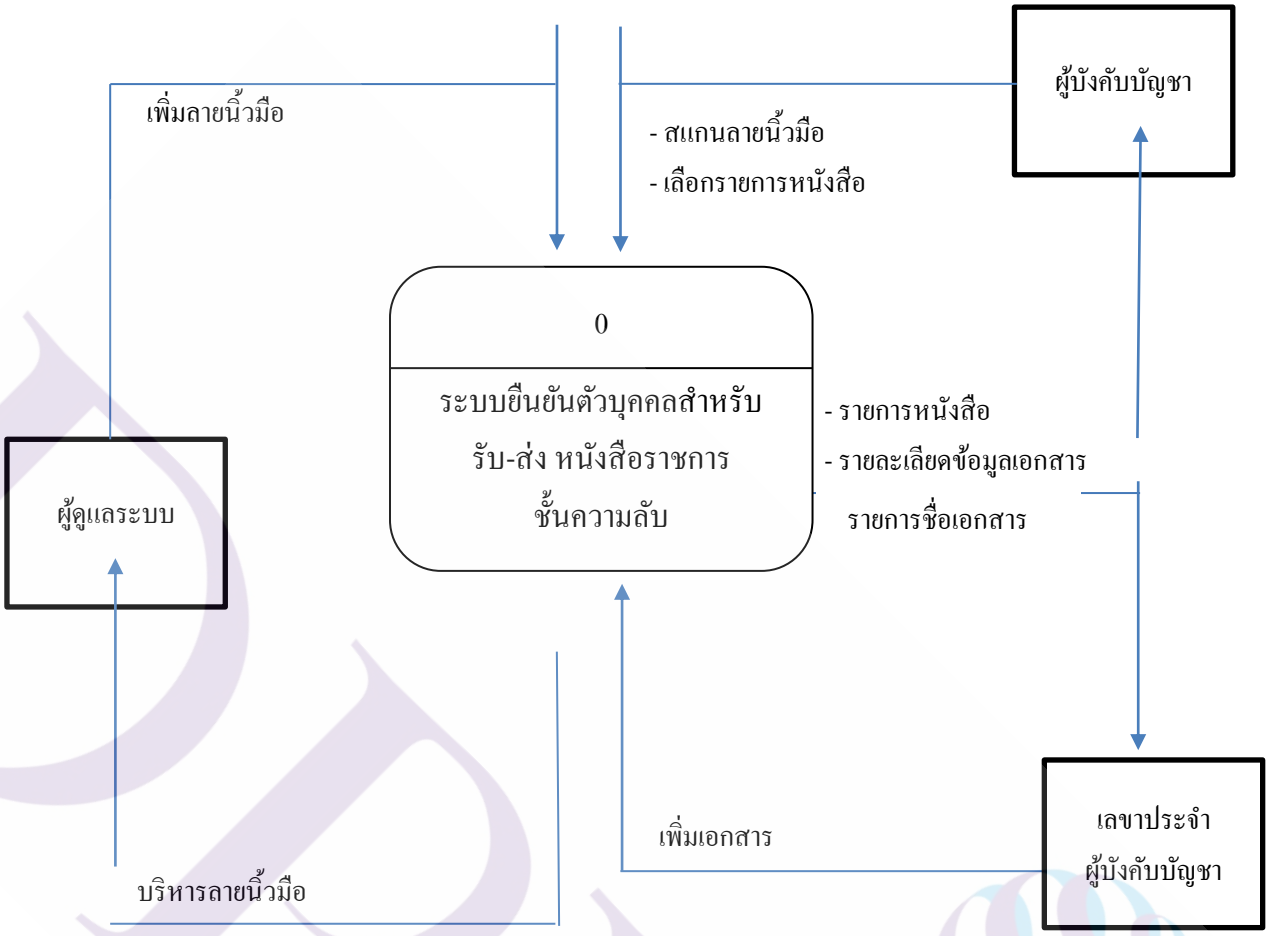
3.3.1 ออกแบบบ Process Decomposition ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



ภาพที่ 3.3 แผนภาพ Process Decomposition

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

3.3.2 ออกแบบ Context Diagram ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

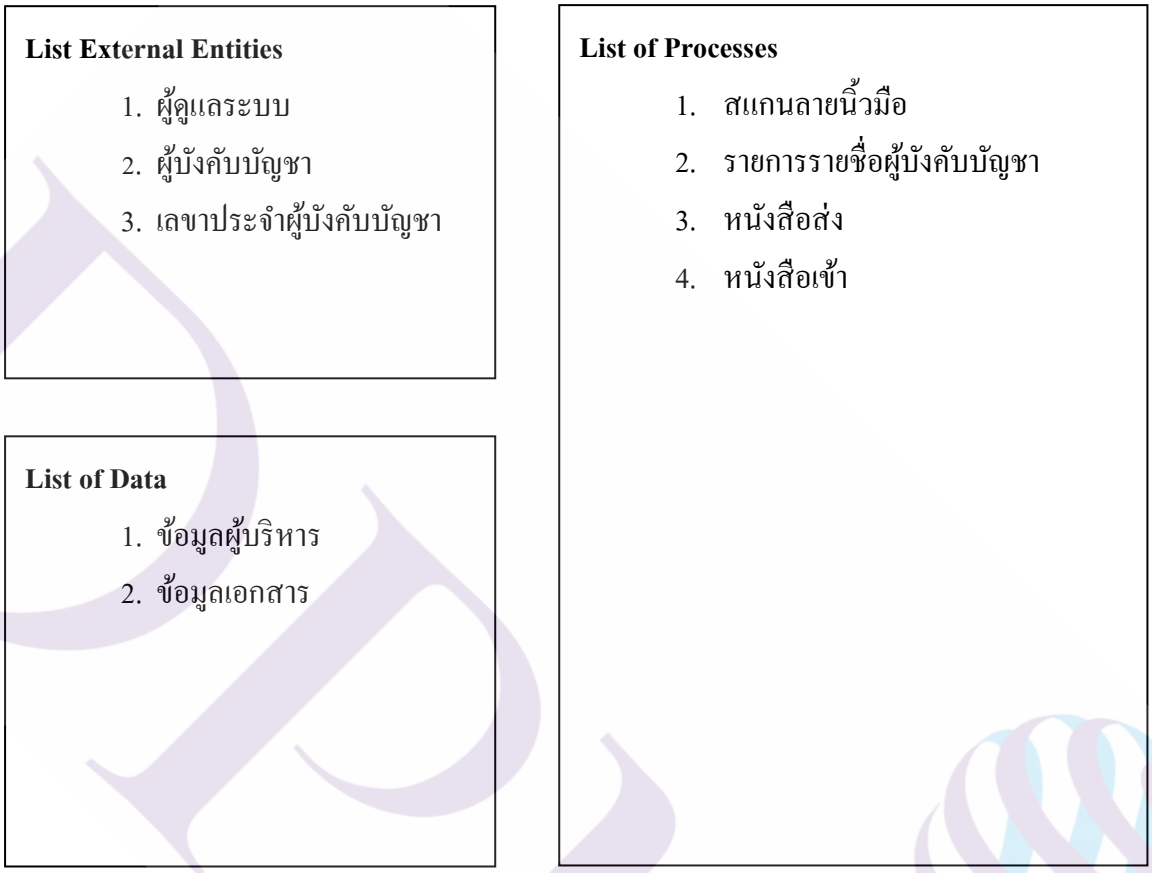


ภาพที่ 3.4 Context Diagram ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

จากรูปภาพ Context Diagram สามารถอธิบายได้ว่าในระบบนี้มีตัวแปรภายนอกที่เกี่ยวข้องกับระบบจำนวน 3 ตัวแปรด้วยกันซึ่งก็คือผู้ใช้งานในระบบจำนวน 3 ระดับ

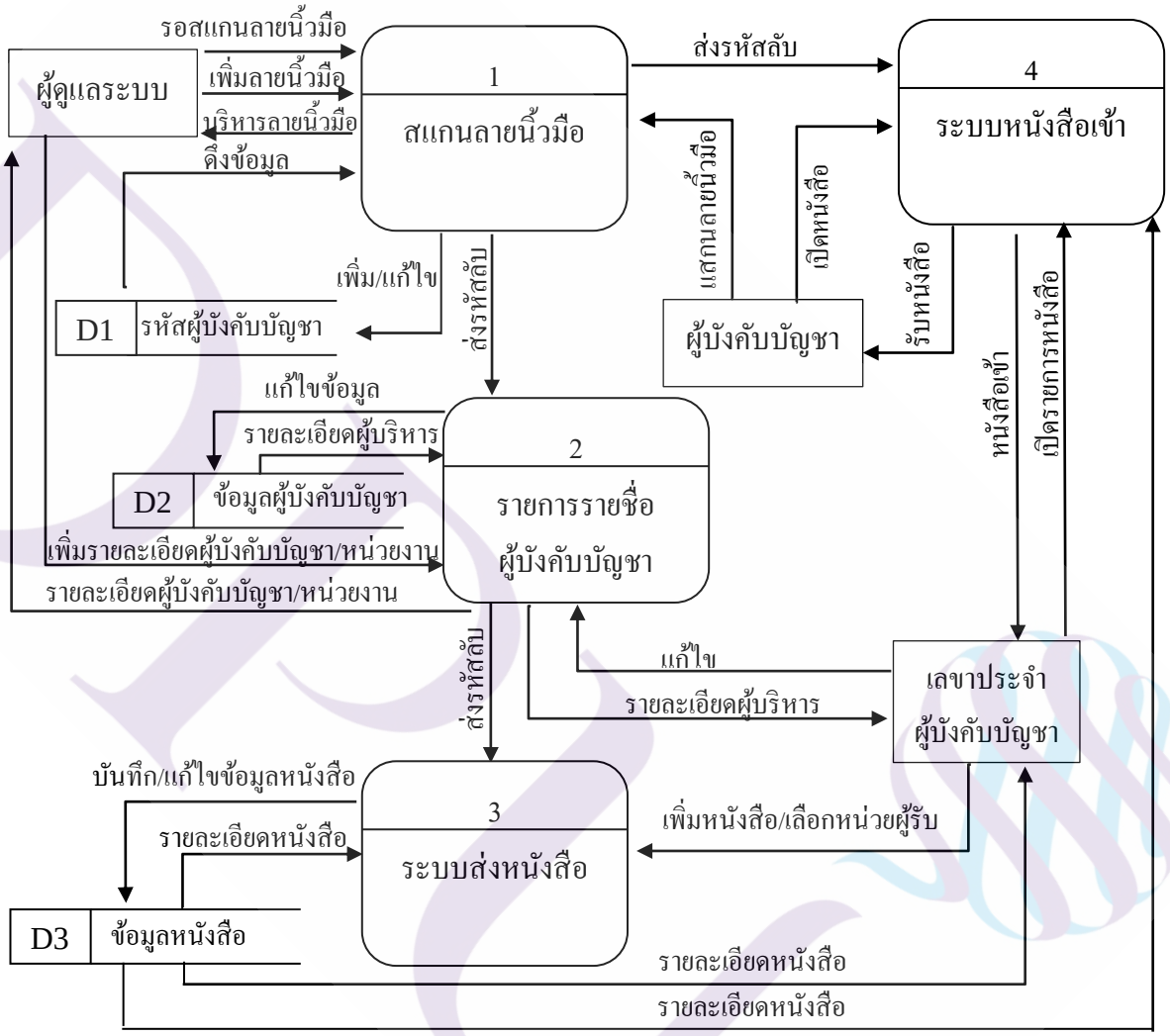
1. ผู้ดูแลระบบ
2. ผู้บังคับบัญชา
3. เลขาประจำผู้บังคับบัญชา

3.3.3 ออกแบบ Data Flow Diagram level 0 ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



ภาพที่ 3.5 แสดง List รายละเอียดที่เกี่ยวข้อง

3.3.4 ออกแบบ Data Flow Diagram level 1 ระบบยืนยันตัวบุคคลสำหรับรับ-ส่ง หนังสือราชการชั้นความลับ



ภาพที่ 3.6 Data Flow Diagram level 1

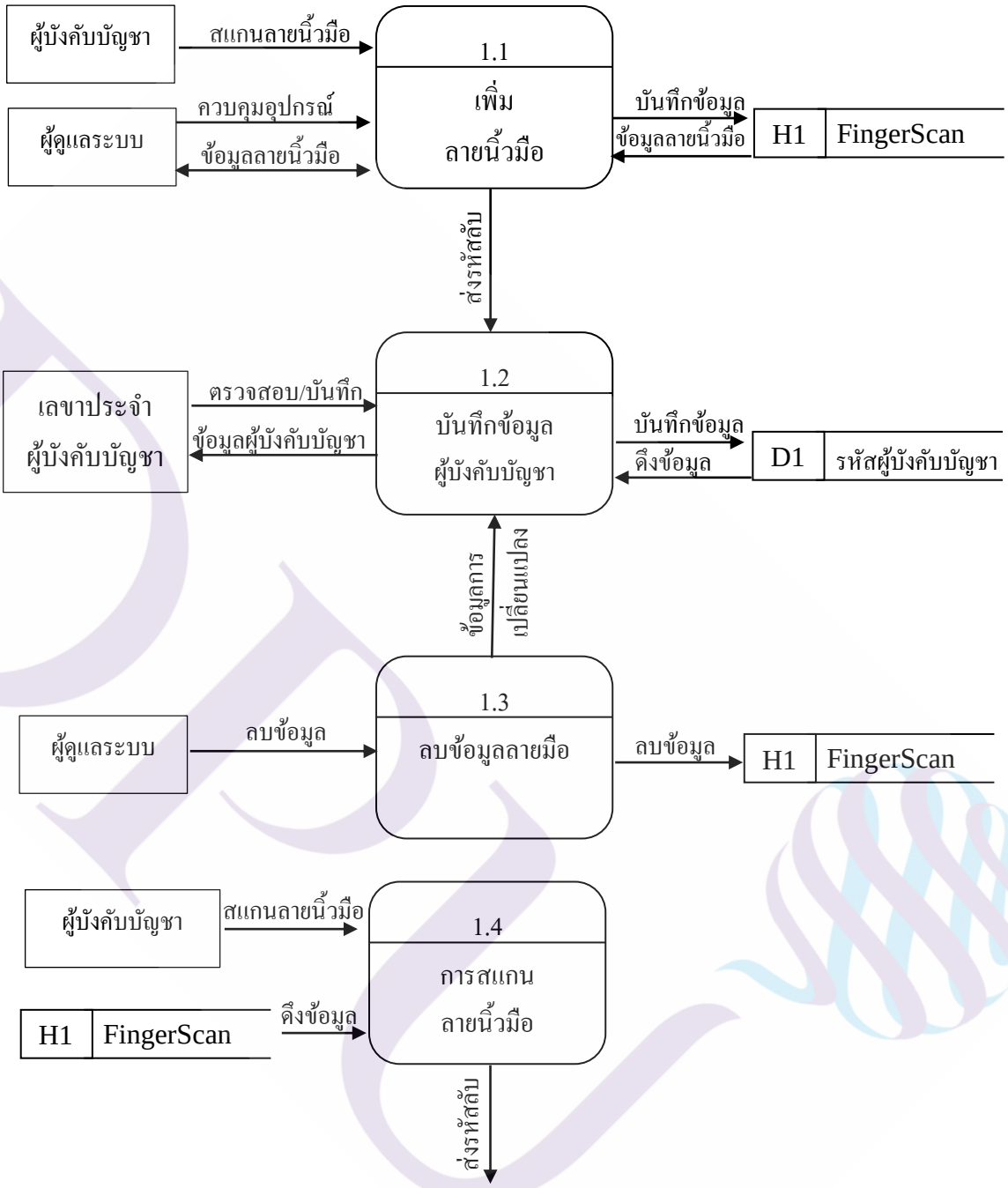
3.3.4.1 ระบบสแกนลายนิ้วมือ มีระบบงานย่อยดังนี้

3.3.4.1(1) เพิ่มลายนิ้วมือผู้บังคับบัญชา

3.3.4.1(2) บันทึกข้อมูลผู้บังคับบัญชา

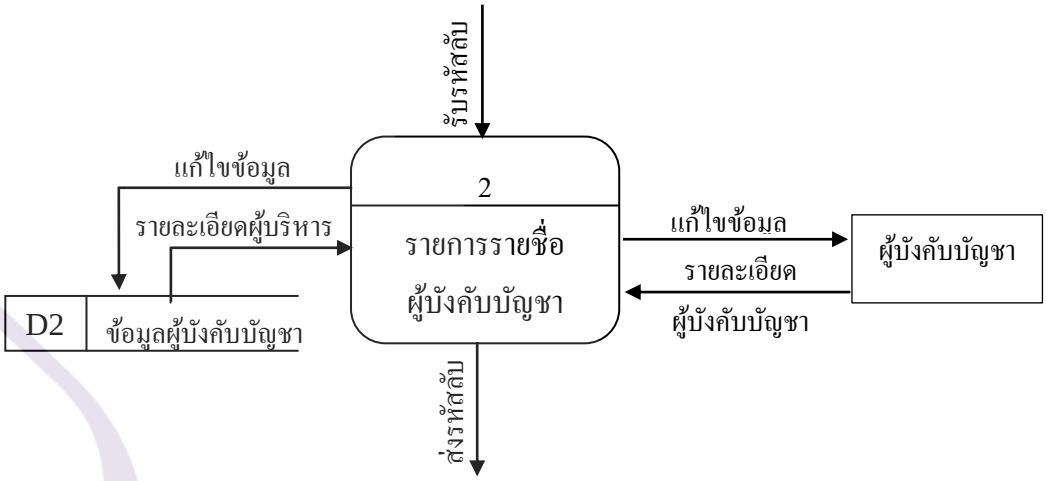
3.3.4.1(3) ลบข้อมูลลายนิ้วมือผู้บังคับบัญชา

3.3.4.1(4) การสแกนลายนิ้วมือผู้บังคับบัญชา



ภาพที่ 3.7 Data Fragment 1 : ระบบสแกนลายนิ้วมือ

3.3.4.2 ระบบรายการรายชื่อผู้บังคับบัญชา



ภาพที่ 3.8 Data Fragment 2: ระบบรายการรายชื่อผู้บังคับบัญชา

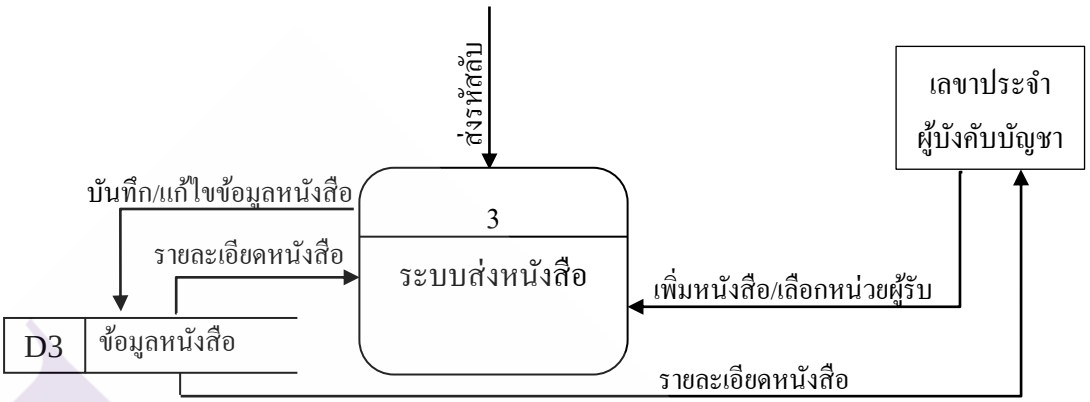
3.3.4.3 ระบบส่งหนังสือ มีระบบงานย่อยดังนี้

3.3.4.3(1) สร้างหนังสือ

- กำหนดรายละเอียดหนังสือชื่อเรื่อง ชั้นความลับ ชั้นความเร่งด่วน พร้อมหมายเหตุ ถ้ามี
- แนบไฟล์เอกสาร โดยจะทำการแนบเฉพาะไฟล์นามสกุล .pdf
- ลบไฟล์เอกสารต้นฉบับ

3.3.4.3(2) หนังสือรอส่ง

- เลือกหนังสือที่ได้ทำการสร้างแล้ว (หนังสือรอส่ง)
- เลือกหน่วยงานปลายทาง
- ทำการส่งหนังสือ



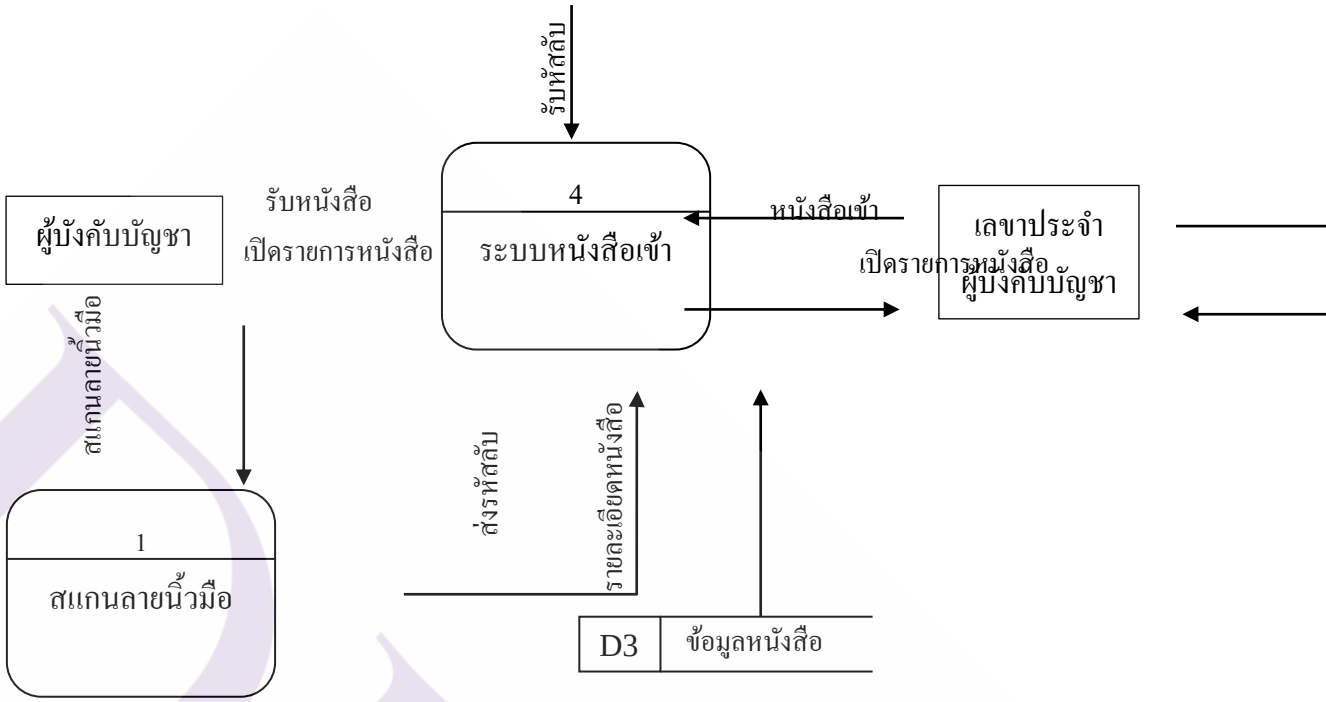
ภาพที่ 3.9 Data Fragment 3: ระบบส่งหนังสือ

4) ระบบหนังสือเข้า มีรายละเอียดดังนี้

4.1 หนังสือเข้าหน่วยงาน คือรายการหัวข้อเรื่องแต่ละเรื่องที่ส่งมาถึงหน่วยงาน บุคคลที่สามารถเข้าถึงรายการหัวข้อเรื่องมี 2 ผู้ใช้คือ ผู้บังคับบัญชา และ เลขาประจำผู้บังคับบัญชา

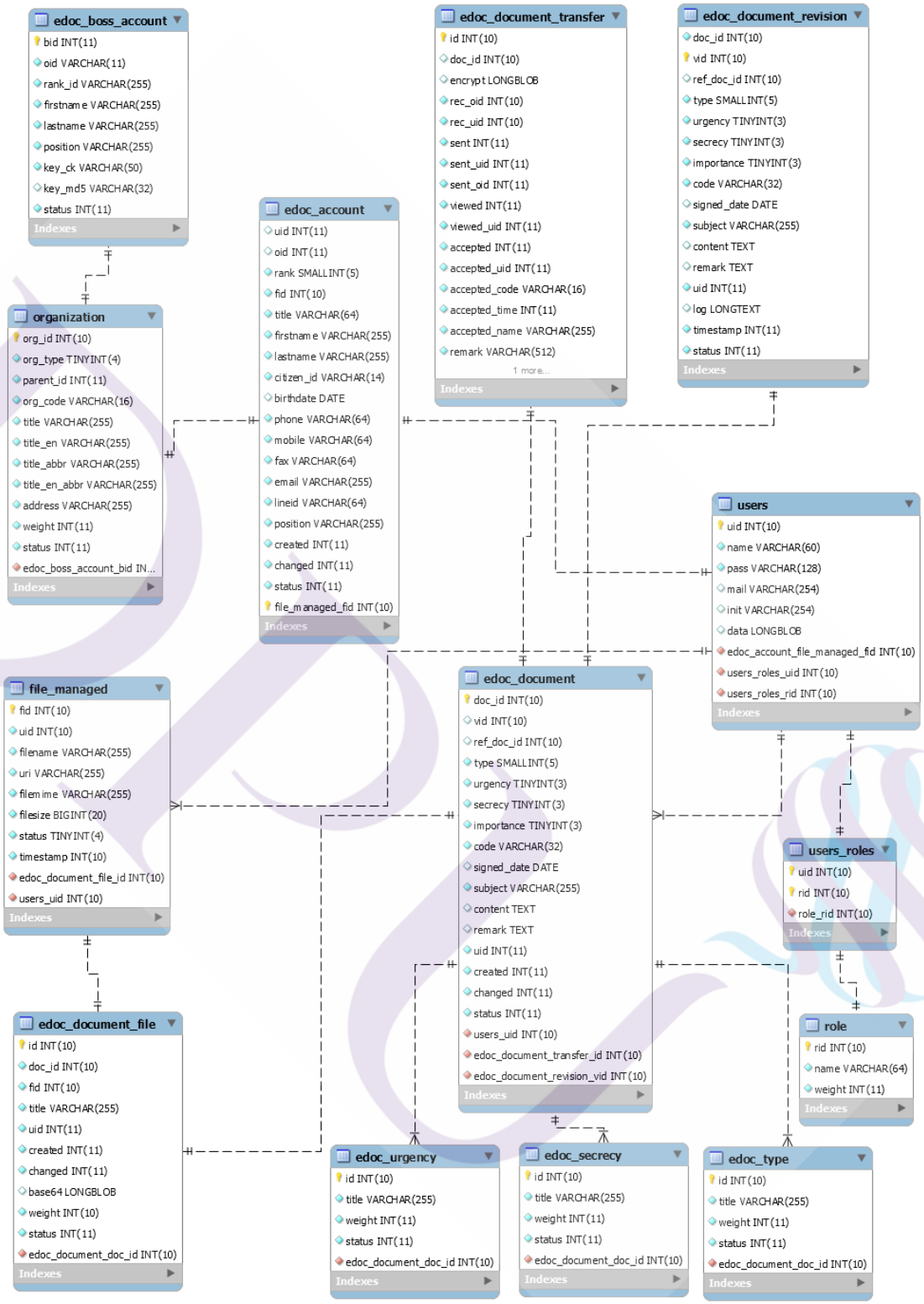
4.2 การรับหนังสือ คือขั้นตอนการเข้าถึงข้อมูลชั้นความลับบุคคลที่สามารถเข้าถึงข้อมูลได้คือผู้บังคับบัญชาเท่านั้น มีกระบวนการดำเนินการ ดังนี้

- คลิกเลือกรายการหัวข้อที่จะเข้าถึงแล้วทำการสแกนลายนิ้วมือเพื่อตรวจสอบข้อมูล
- ระบบทำการตรวจสอบสิทธิ์
- เมื่อตรวจสอบพบว่าเป็นผู้มีสิทธิ์ ระบบจะรับหนังสือ



ภาพที่ 3.10 Data Fragment 4: ระบบหนังสือเข้า

3.3.5 ออกแบบ ER-Diagram ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



ภาพที่ 3.11 แผนภาพ ER-Diagram

3.3.6 การกำหนดรายละเอียดของแฟ้มข้อมูล (Data Dictionary)

การกำหนดรายละเอียดของแฟ้มข้อมูล จุดมุ่งหมายเพื่อนำเอาโครงสร้างฐานข้อมูลที่ได้มากำหนดรูปแบบและรายละเอียดต่าง ๆ ให้อยู่ในรูปแบบของโครงสร้างที่จะนำไปใช้ในการสร้างฐานข้อมูลที่เลือกใช้ซึ่งก็คือ MySqlโดยมีรายละเอียดดังนี้

ตารางที่ 3.1 แสดงโครงสร้างตาราง หน่วยงาน (edoc_account)

Field_name	Key	Data_type	Size	Desciption
uid	PK	int	10	หมายเลขผู้ใช้งาน (user
oid	FK	int	10	หมายเลขหน่วยงาน
rank	FK	smallint	5	รหัสยศ
fid	FK	int	10	File ID โลโก้หน่วยงาน
title		varchar	64	ชื่อหน่วยงาน
firsname		varchar	255	ชื่อ
lastname		varchar	255	สกุล
citizen_id		varchar	14	รหัสบัตรประชาชน
birthdate		date		วันเดือนปีเกิด
phone		varchar	64	หมายเลขโทรศัพท์
mobile		varchar	64	หมายเลขโทรศัพท์
fax		varchar	64	หมายเลขโทรศัพท์
email		varchar	255	อีเมล์
lineid		varchar	64	ไอดีไลน์
position		varchar	64	ตำแหน่ง
created		int	10	วันที่สร้างaccount
changed		int	10	วันที่แก้ไข
status		int	10	สถานะของผู้ใช้งาน

ตารางที่ 3.2 แสดงโครงสร้างตาราง รายละเอียดหนังสือ (edoc_boss_account)

Field_name	Key	Data_type	Size	Desciption
bid	PK	int	10	รหัสผู้บริหาร
oid	FK	varchar	10	หมายเลขหน่วยงาน
rank_id	FK	varchar	255	รหัสยศ
firstname		varchar	255	ชื่อ
lastname		varchar	255	นามสกุล
position		varchar	255	ตำแหน่ง
key_ck		varchar	50	รหัสหมายเลขนิ้วมือ
key_md5		varchar	32	เก็บข้อมูลรหัสลับที่แปลมาแล้ว
status		int	10	สถานะ (ยังเป็นผู้ใช้งาน)

ตารางที่ 3.3 แสดงโครงสร้างตาราง ชั้นความลับหนังสือ (edoc_document)

Field_name	Key	Data_type	Size	Desciption
doc_id	PK	int	10	ลำดับเอกสารที่สร้าง
vid	FK	int	10	รหัสผู้สร้างเอกสาร
ref_doc_id		int	10	รหัสอ้างอิง
type		smallint	5	ประเภทหนังสือ
urgency		tinyint	3	ชั้นความเร่งด่วน
secrecy		tinyint	3	ชั้นความลับ
importance		tinyint	3	ชนิดหนังสือ
code		varchar	32	เลขที่หนังสือ
signed_date		date		ลงวันที่หนังสือ
subject		varchar	255	หัวข้องเรื่อง

Field_name	Key	Data_type	Size	Desciption
content		text		เนื้อหา
remark		text		หมายเหตุ
uid		int	10	หมายเลขผู้ใช้งาน (user)
created		int	10	วันเวลาที่สร้างเอกสาร
changed		int	10	วันที่แก้ไขเอกสาร
status		int	10	สถานะ

ตารางที่ 3.4 แสดงโครงสร้างตาราง หมวดหนังสือ (edoc_document_file)

Field_name	Key	Data_type	Size	Desciption
id	PK	int	10	ลำดับไฟล์
doc_id		int	10	ลำดับเอกสารที่สร้าง
fid		int	10	หมายเลขไฟล์
title		varchar	255	ชื่อเอกสาร
uid		int	10	หมายเลขผู้ใช้งาน (user)
created		int	10	วันเวลาที่สร้างเอกสาร
changed		int	10	วันที่แก้ไขเอกสาร
base64		longblob		ไฟล์เอกสารที่ถูกเข้ารหัส
weight		int	10	ลำดับความสำคัญ (ถ้ามีหลายไฟล์)
status		int	10	สถานะ

ตารางที่ 3.5 แสดงโครงสร้างตาราง ความเร่งด่วน (edoc_document_revision)

Field_name	Key	Data_type	Size	Desciption
doc_id	PK	int	10	ลำดับเอกสารที่สร้าง
vid		int	10	รหัสผู้สร้างเอกสาร
ref_doc_id		int	10	รหัสอ้างอิง
type		smallint	5	ประเภทหนังสือ
urgency		tinyint	3	ชั้นความเร่งด่วน
secrecy		tinyint	3	ชั้นความลับ
importance		tinyint	3	ชนิดหนังสือ
code		varchar	32	เลขที่หนังสือ
signed_date		date		ลงวันที่หนังสือ
subject		varchar	255	หัวข้องเรื่อง
content		text		รายละเอียด
remark		text		หมายเหตุ
uid		int	10	หมายเลขผู้ใช้งาน (user) ปลายทางที่รับ
log		longtext		
timestamp		int	10	เวลาที่สร้างหนังสือ
status		int	10	สะถานะ

ตารางที่ 3.6 แสดงโครงสร้างตาราง หนังสือรอส่ง (edoc_document_transfer)

Field_name	Key	Data_type	Size	Desciption
id	PK	int	10	ลำดับ
doc_id	FK	int	10	ลำดับเอกสารที่สร้าง
encrypt		longblob		ข้อมูลที่ถูกเข้ารหัส
rec_oid	FK	int	10	หมายเลขหน่วยงานที่รับ
rec_uid	FK	int	10	หมายเลขผู้ใช้งานที่รับ
sent		int	10	สถานะส่ง
sent_uid		int	10	ผู้ส่ง
sent_oid		int	10	หน่วยงานผู้ส่ง
viewed		int	10	สถานะการเปิดอ่าน
viewed_uid		int	10	ผู้เปิดอ่าน
accepted		int	10	รับหนังสือ
accepted_uid		int	10	ผู้รับหนังสือ
accepted_code		varchar	16	เลขรับเอกสาร
accepted_time		int	10	เวลาที่รับเอกสาร
accepted_name		varchar	255	ชื่อผู้รับเอกสาร
remark		varchar	512	หมายเหตุ
status		int	10	สถานะ

ตารางที่ 3.7 แสดงโครงสร้างตาราง ชั้นความลับ (edoc_secrecy)

Field_name	Key	Data_type	Size	Desciption
id	PK	int	10	ลำดับ
title		varchar	255	ชั้นความลับของหนังสือ
weight		int	10	ลำดับความสำคัญ
status		int	10	สถานะ

ตารางที่ 3.8 แสดงโครงสร้างตาราง ประเภทหนังสือ (edoc_type)

Field_name	Key	Data_type	Size	Desciption
id	PK	int	10	ลำดับ
title		varchar	255	ประเภทของหนังสือ
weight		int	10	ลำดับความสำคัญ
status		int	10	สถานะ

ตารางที่ 3.9 แสดงโครงสร้างตาราง ความเร่งด่วน (edoc_urgency)

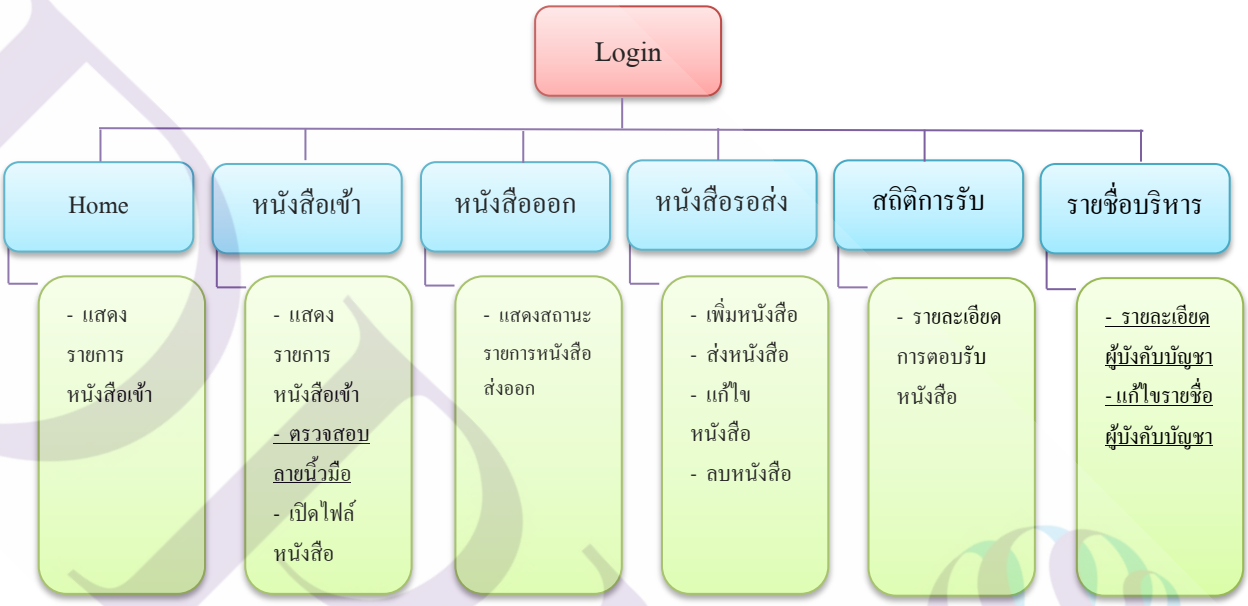
Field_name	Key	Data_type	Size	Desciption
id	PK	int	10	ลำดับ
title		varchar	255	ชั้นความเร็วของหนังสือ
weight		int	10	ลำดับความสำคัญ
status		int	10	สถานะ

3.3.7 แผนผังเว็บไซต์ (Site Map) ของระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

ออกแบบเพิ่มเติมจากระบบงานเดิม 2 ส่วน

3.3.7.1 หนังสือเข้า เพิ่มเติมหน้าต่าง ตรวจสอบลายนิ้วมือ

3.3.7.2 รายชื่อบริหาร เพิ่มหน้าต่างรายละเอียดผู้บังคับบัญชา และ หน้าต่างแก้ไขรายชื่อผู้บังคับบัญชา



ภาพที่ 3.12 แผนผังเว็บไซต์ (Site Map)

3.3.8 การเข้ารหัสข้อมูล(Encryption) และการถอดรหัสข้อมูล(Decryption) ของไฟล์เอกสาร

โดยจะใช้ การเข้ารหัสแบบสมมาตร หรือ Symmetric key Cryptosystemในรูปแบบอัลกอริทึม AES ในการเข้ารหัสและถอดรหัส ซึ่งจะมีการเข้ารหัสและถอดรหัส 2 ครั้ง ดังนี้

3.3.8.1 การเข้ารหัสและถอดรหัส ครั้งที่ 1 โดยใช้คีย์ระบบที่กำหนดไว้

```php
function encrypt($string){
 $salting = substr(md5(microtime()),-1) . $string;
 return my_simple_crypt( $salting, 'e' );
}

function decrypt($string){
 $encode = my_simple_crypt( $string, 'd' );
 return substr($encode, 1);
}
```

ภาพที่ 3.13 คำสั่งการเข้ารหัสและถอดรหัส ครั้งที่ 1

3.3.8.2 การเข้ารหัสและถอดรหัส โดยใช้คีย์รหัสลับ 32 ตัวอักษร (ที่ได้มาจากรหัสผู้บังคับบัญชาที่สแกนลายนิ้วมือ และ ลำดับเอกสารที่สร้าง มาทำการเข้ารหัสแบบ MD5)

```php
$key = $res_1['key_md5']."".$doc_c;
$ken_en= md5($key);//32
$encrype = encrypt($encoder.$ken_en);
```

```php
$key_code = $build['search_showlistmember_form']['key_md5']['#value'];
$key = $key_code."".$doc_id;
$code = md5($key);
$key_len = strlen($code);
$decrypt = decrypt($res_2['encrypt'],$code);
```

ภาพที่ 3.14 คำสั่งการเข้ารหัสและถอดรหัส ครั้งที่ 2

3.4 ระบบสแกนลายนิ้วมือ

3.4.1 อุปกรณ์และคุณสมบัติ

3.4.1.1 FingerPrint sensor คือ เซนเซอร์สำหรับสแกนลายนิ้วมือเพื่อตรวจสอบว่าตรงกับของใครในฐานข้อมูล สามารถบันทึกลายนิ้วมือในโมดูลได้สูงสุด 127 ลายนิ้วมือ ใช้ไฟเลี้ยง 4.2V-6V กระแสสูงสุด 150mA เชื่อมต่อแบบ UART มีคุณสมบัติดังนี้

3.4.1.1.(1) Supply voltage: 4.2 - 6.0VDC

3.4.1.1.(1) Operating current: 120mA max

3.4.1.1.(1) Peak current: 150mA max

3.4.1.1.(1) Fingerprint imaging time:

3.4.1.1.(1) Window area: 14mm x 18mm

3.4.1.1.(1) Signature file: 256 bytes

3.4.1.1.(1) Template file: 512 bytes

3.4.1.1.(1) Storage capacity: 127 templates

3.4.1.1.(1) Safety ratings (1-5 low to high safety)

3.4.1.1.(1) False Acceptance Rate: <0.001% (Security level 3)

3.4.1.1.(1) False Reject Rate: <1.0% (Security level 3)

3.4.1.1.(1) Interface: TTL Serial

3.4.1.1.(1) Baud rate: 9600, 19200, 28800, 38400, 57600 (default is 57600)

3.4.1.1.(1) Working temperature rating: -20C to +50C

3.4.1.1.(1) Working humidy: 40%-85% RH

3.4.1.1.(1) Full Dimensions: 47 x 20 x 21.5mm

ภาพที่ 3.15 อุปกรณ์ Finger Print Sensor

3.4.1.2 สาย USB Port : PL2303HX USB Transfer to TTL RS232 Serial Port Adapter Cable Module PL2303 Console Recovery Upgrade เพื่อเชื่อมต่อระหว่าง Fingerprint sensor กับเครื่องคอมพิวเตอร์ จ่ายกระแสไฟ 3.3V และ 5.0V

ภาพที่ 3.16 อุปกรณ์สาย USB Port

3.4.2 ระบบบริหารจัดการลายนิ้วมือ

ระบบบริหารจัดการลายนิ้วมือนั้นได้ออกแบบโดยการใช้ภาษา phyton ในการเขียนคำสั่งเพื่อบริหารจัดการลายนิ้วมือและติดต่อกับเว็บไซต์รวมทั้งฐานข้อมูล

```
##################### main menu ##############################
def menu():
    print("----------------")
    if finger.read_templates() != adafruit_fingerprint.OK:
        raise RuntimeError('Failed to read templates')
    print("Fingerprint templates:", finger.templates)
    print("e) enroll print")
    print("f) find print")
    print("d) delete print")
    print("----------------")
################## Key board ##############################
```

ภาพที่ 3.17 คำสั่งแต่ละเมนูบนระบบบริหารจัดการลายนิ้วมือ

3.4.2.1 คำสั่ง e) enroll print (การเพิ่มลายนิ้วมือ)

```
def enroll_finger(location):
    """Take a 2 finger images and template it, then store in 'location'"""
    for fingerimg in range(1, 3):
        if fingerimg == 1:
            print("Place finger on sensor...", end="", flush=True)
        else:
            print("Place same finger again...", end="", flush=True)

        while True:
            i = finger.get_image()
            if i == adafruit_fingerprint.OK:
                print("Image taken")
                break
            elif i == adafruit_fingerprint.NOFINGER:
                print(".", end="", flush=True)
            elif i == adafruit_fingerprint.IMAGEFAIL:
                print("Imaging error")
                return False
            else:
                print("Other error")
                return False

        print("Templating...", end="", flush=True)
        i = finger.image_2_tz(fingerimg)
        if i == adafruit_fingerprint.OK:
            print("Templated")
        else:
            if i == adafruit_fingerprint.IMAGEMESS:
                print("Image too messy")
            elif i == adafruit_fingerprint.FEATUREFAIL:
                print("Could not identify features")
            elif i == adafruit_fingerprint.INVALIDIMAGE:
                print("Image invalid")
            else:
                print("Other error")
            return False

        if fingerimg == 1:
            print("Remove finger")
            time.sleep(1)
            while i != adafruit_fingerprint.NOFINGER:
                i = finger.get_image()
    print("Creating model...", end="", flush=True)
    i = finger.create_model()
    if i == adafruit_fingerprint.OK:
        print("Created")
    else:
        if i == adafruit_fingerprint.ENROLLMISMATCH:
            print("Prints did not match")
        else:
            print("Other error")
        return False
```

```
    print("Storing model #%d..." % location, end="", flush=True)
    i = finger.store_model(location)
    if i == adafruit_fingerprint.OK:
        print("Stored")
    else:
        if i == adafruit_fingerprint.BADLOCATION:
            print("Bad storage location")
        elif i == adafruit_fingerprint.FLASHERR:
            print("Flash storage error")
        else:
            print("Other error")
        return False

    return True
```

ภาพที่ 3.18 คำสั่งการเพิ่มลายนิ้วมือ

จากภาพเป็นคำสั่งสำหรับการเพิ่มลายนิ้วมือเก็บไว้ในความจำของ Finger Print โดยพิมพ์คำว่า e หลังจากนั้นใส่ตัวเลขประจำหน่วยงาน จะไม่ซ้ำกัน ซึ่งผู้ดูแลระบบจะกำหนดไว้แล้วว่าหน่วยงานไหนเลขประจำหน่วยงานคืออะไร เมื่อใส่เลขประจำหน่วยงานแล้วให้ทำการสแกนลายนิ้วมือผู้บริหาร 2 ครั้ง

3.4.2.2 คำสั่ง f) find print (การตรวจสอบลายนิ้วมือ)

```
def get_fingerprint():
    """Get a finger print image, template it, and see if it matches!"""
    print("Waiting for image...")
    while finger.get_image() != adafruit_fingerprint.OK:
        pass
    print("Templating...")
    if finger.image_2_tz(1) != adafruit_fingerprint.OK:
        return False
    print("Searching...")
    if finger.finger_fast_search() != adafruit_fingerprint.OK:
        return False
    return True
```

ภาพที่ 3.19 คำสั่งการตรวจสอบลายนิ้วมือ

จากภาพเป็นคำสั่งสำหรับการตรวจสอบลายนิ้วมือโดยพิมพ์คำสั่ง f สำหรับการตรวจสอบลายนิ้วมือว่าเป็นบุคคลใด จะแสดงยศ-ชื่อ-นามสกุล และตำแหน่ง

3.4.2.3 คำสั่ง d) deleted print (การลบลายนิ้วมือ)

```
#print('d')
if finger.delete_model(get_num()) == adafruit_fingerprint.OK:
    print("Deleted!")
else:
    print("Failed to delete")
```

ภาพที่ 3.20 คำสั่งการตรวจสอบลายนิ้วมือ

จากภาพเป็นคำสั่งสำหรับการตรวจสอบลายนิ้วมือโดยพิมพ์คำสั่ง d สำหรับการลบลายนิ้วมือ กรณีปรับเปลี่ยนผู้บังคับบัญชา และกรณีอื่นๆ

3.4.2.4 คำสั่ง k) check finger (การส่งข้อมูลลายนิ้วมือ)

```
def Keyboard() :

    while True :
        if get_fingerprint_id():
            #print("Detected #", finger.finger_id, "with confidence", finger.confidence)
            res = str(finger.finger_id)
            words = hashlib.md5(res.encode('utf-8'))
            keyboard.type(words.hexdigest())
            keyboard.press(Key.enter)
            keyboard.release(Key.enter)


if list == [] :
    print('Could not open port')
    exit()
else :
    print("Connected COM ports: " + str(connected))
    if sys.platform.startswith('win'):
    # !attention assumes pyserial 3.x
        ports = ['COM%s' % (i + 1) for i in range(256)]
    elif sys.platform.startswith('linux') or sys.platform.startswith('cygwin'):
        # this excludes your current terminal "/dev/tty"
        ports = glob.glob('/dev/tty[A-Za-z]*')
    elif sys.platform.startswith('darwin'):
        ports = glob.glob('/dev/tty.*')
    else:
        raise EnvironmentError('Unsupported platform')
    ports = connected[0]
    uart = serial.Serial(ports , 57600)
    finger = adafruit_fingerprint.Adafruit_Fingerprint(uart)
```

ภาพที่ 3.21 คำสั่งการส่งข้อมูลลายนิ้วมือ

จากภาพเป็นคำสั่งสำหรับการส่งข้อมูลลายนิ้วมือ เพื่อส่งรหัสข้อมูลไปยังเว็บไซต์ โดยพิมพ์คำสั่ง k เมื่อจะเข้าใช้งานเว็บไซต์จำเป็นต้องอยู่ในคำสั่ง k ตลอดเวลา มิฉะนั้นแล้วข้อมูลรหัสจะไม่ถูกส่งไป ขั้นตอนนี้จะเป็นขั้นตอนการนำตัวเลขประจำหน่วยงานคือตัวเลข 1 – 127 มาทำการเข้ารหัส MD5 แล้วทำการส่งข้อมูลไปยังเว็บไซต์ต่อไป

3.4.2.5 คำสั่ง x) exit (ออกจากระบบ)

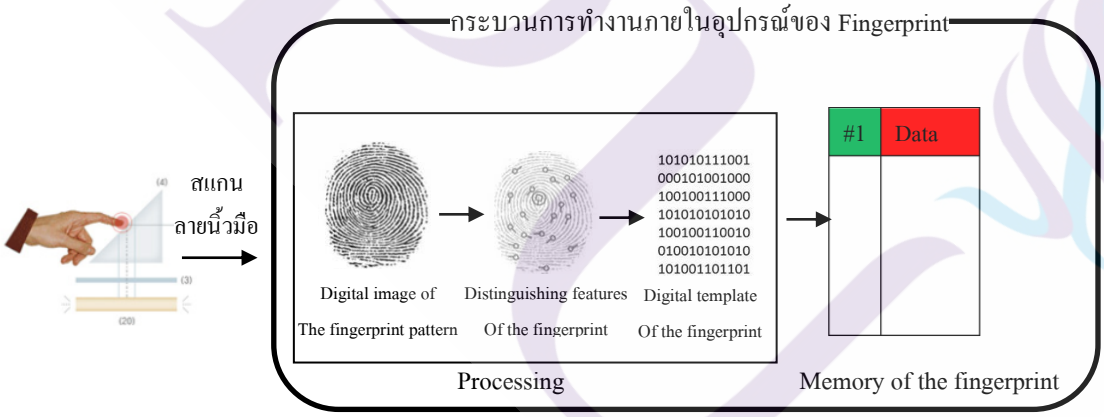
```
elif c == 'x':
    #print('Exit Program')
    break
```

ภาพที่ 3.22 คำสั่งการออกจากระบบ

จากภาพเป็นคำสั่งสำหรับการออกจากระบบบริหารจัดการลายนิ้วมือ โดยพิมพ์คำสั่ง x

3.4.3 การตรวจพิสูจน์ลายนิ้วมือ

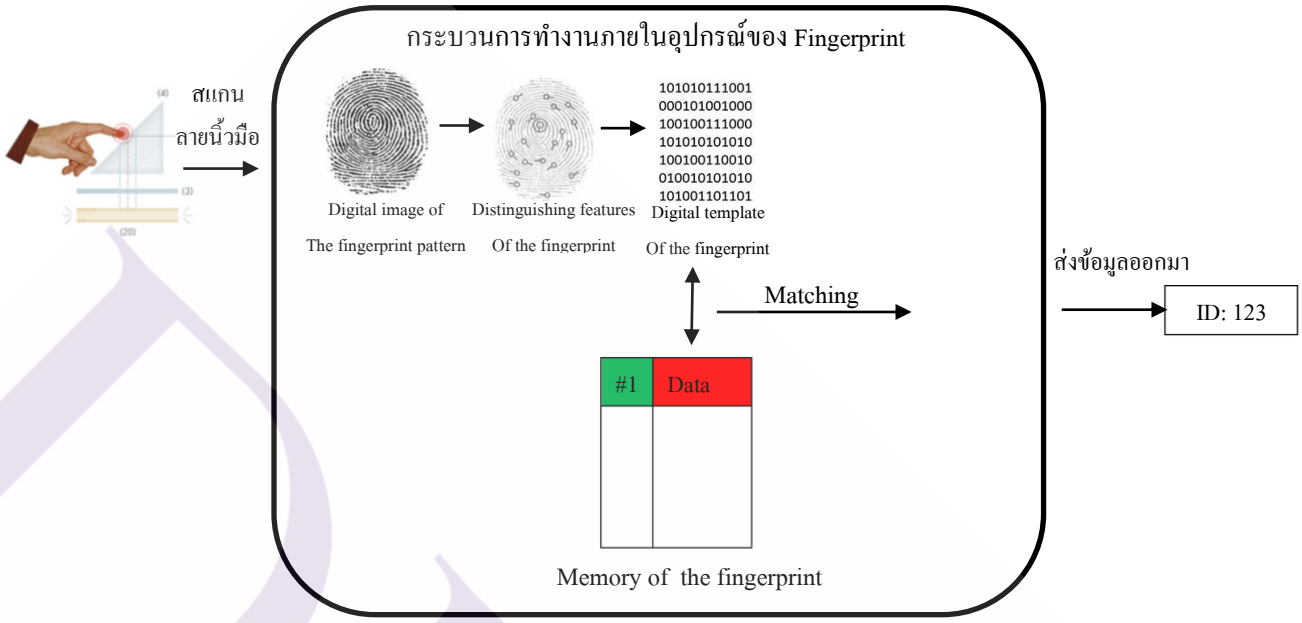
3.4.3.1 การจัดเก็บข้อมูลลายนิ้วมือ



ภาพที่ 3.23 ขั้นตอนการจัดเก็บข้อมูลลายนิ้วมือ

จากภาพที่ 3.19 อธิบายถึงกระบวนการแรกเริ่มของการตรวจพิสูจน์ลายนิ้วมือ เป็นกระบวนการทำงานภายในอุปกรณ์ของ Fingerprint จะเริ่มด้วยการนำลายนิ้วมือของแต่ละบุคคลแต่ละนิ้ว มาหาจุดลักษณะเฉพาะและทำการจัดเก็บข้อมูลไว้ในหน่วยความจำของ Fingerprint

3.4.3.2 การเปรียบเทียบข้อมูลลายนิ้วมือ

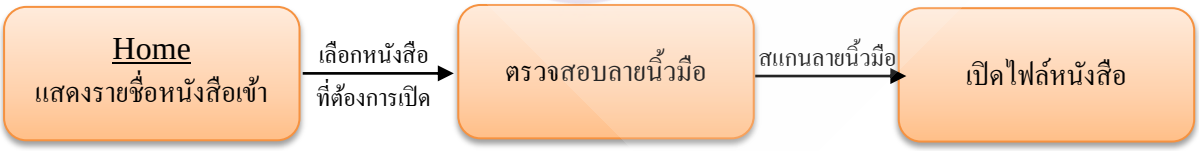


ภาพที่ 3.24 ขั้นตอนการเปรียบเทียบข้อมูลลายนิ้วมือ

จากภาพที่ 3.20 จะแสดงให้เห็นถึงขั้นตอนการเปรียบเทียบข้อมูลลายนิ้วมือ โดยเริ่มที่การสแกนลายนิ้วมือเข้ามา แล้วทำการประมวลผลเหมือนกันกับขั้นตอนการจัดเก็บข้อมูลลายนิ้วมือ หลังจากได้ข้อมูลจากการประมวลผลแล้ว ก็จะทำการเปรียบเทียบข้อมูลที่อยู่ในหน่วยความจำของอุปกรณ์ Fingerprint เข้ากับชุดไหน แล้วส่งข้อมูลเป็นตัวเลข 1 – 127 ออกมา

3.4.4 การเชื่อมต่อระหว่าง FingerPrint Sensor กับเว็บไซต์ของระบบงาน

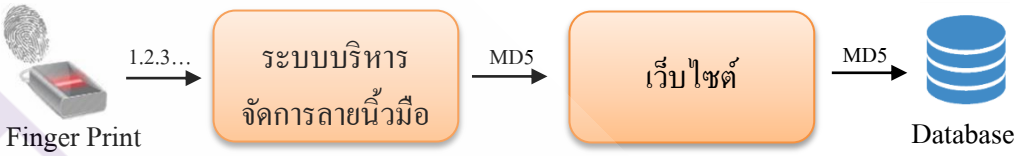
3.4.4.1 ออกแบบหน้าต่างเว็บไซต์ใหม่ในการตรวจสอบลายนิ้วมือของผู้ที่มีสิทธิ์ในการเปิดไฟล์หนังสือ



ภาพที่ 3.25 ออกแบบหน้าต่างเว็บไซต์สำหรับตรวจสอบลายนิ้วมือ

จากภาพที่ 3.15 อธิบายถึงเมื่อคลิกเลือกรายการเอกสารที่จะเปิดแล้วจะเข้าหน้าต่างในการตรวจสอบลายนิ้วมือ เมื่อสแกนลายนิ้วมือพบว่าเป็นผู้ที่มีสิทธิ์ในการเข้าถึงไฟล์นั้นก็สามารถเปิดไฟล์หนังสือได้

3.4.4.2 กระบวนการส่งข้อมูลจาก FingerPrint ไปยังเว็บไซต์



ภาพที่ 3.26 กระบวนการส่งข้อมูลจาก FingerPrint ไปยังเว็บไซต์

จากภาพที่ 3.14 อธิบายถึงการทำงานของ Finger Print ส่งข้อมูลไปยังเว็บไซต์มีขั้นตอนดังนี้

3.3.9.2.(1) เมื่อทำการสแกนลายนิ้วมือ Finger Print จะส่งตัวเลข ID ออกมา

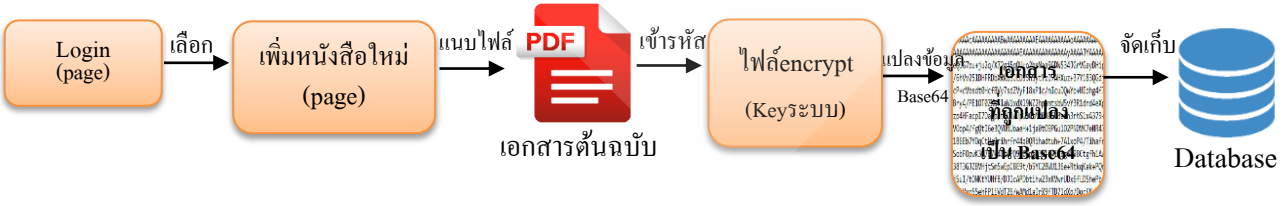
3.3.9.2.(2) ระบบบริหารจัดการลายนิ้วมือจะทำการนำตัวเลข ID มาทำการเข้ารหัสในรูปแบบ MD5 และทำการส่งข้อมูลสู่เว็บไซต์

3.3.9.2.(3) เว็บไซต์ในหน้าต่างของการตรวจสอบลายนิ้วมือก็จะทำการรับข้อมูลเพื่อไปตรวจสอบในฐานข้อมูลว่าตรงกับผู้ที่มีสิทธิ์ในการเปิดหนังสือหรือไม่ ซึ่งในฐานข้อมูลจะมีรหัสข้อมูลของผู้บังคับบัญชาที่แตกต่างกัน

3.5 กระบวนการทำงาน ระบบการรับ-ส่ง หนังสือ

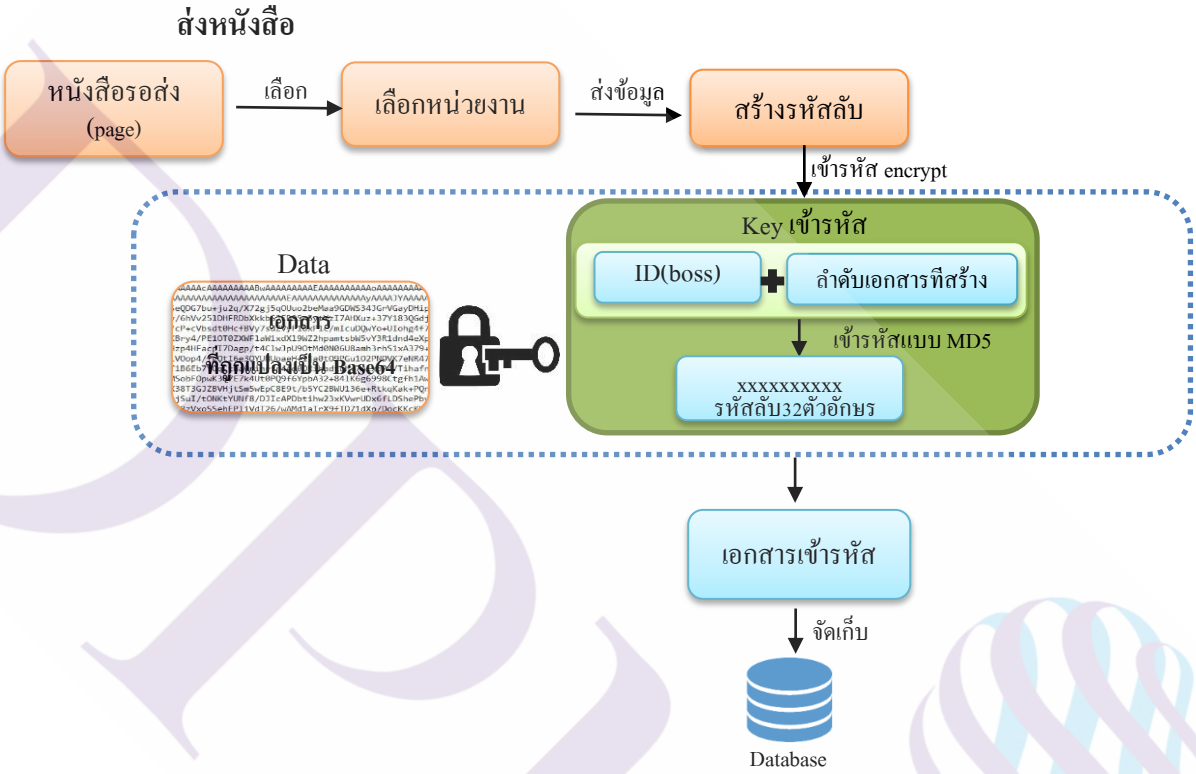
3.5.1 ขั้นตอนการทำงาน ระบบการส่งหนังสือ

สร้างหนังสือ



ภาพที่ 3.27 ขั้นตอนการสร้างหนังสือ

1. login เข้าระบบ เลือกเพิ่มหนังสือ และทำการแนบไฟล์เอกสารที่ต้องการส่ง
2. ระบบทำการเข้ารหัสไฟล์เอกสาร ด้วย คีย์ของระบบที่กำหนดไว้
3. จะได้ ไฟล์encrypt มาทำการแปลงข้อมูล ในรูปแบบ Base64
4. จะได้ เอกสารที่ถูกแปลง เก็บไว้ในฐานข้อมูล



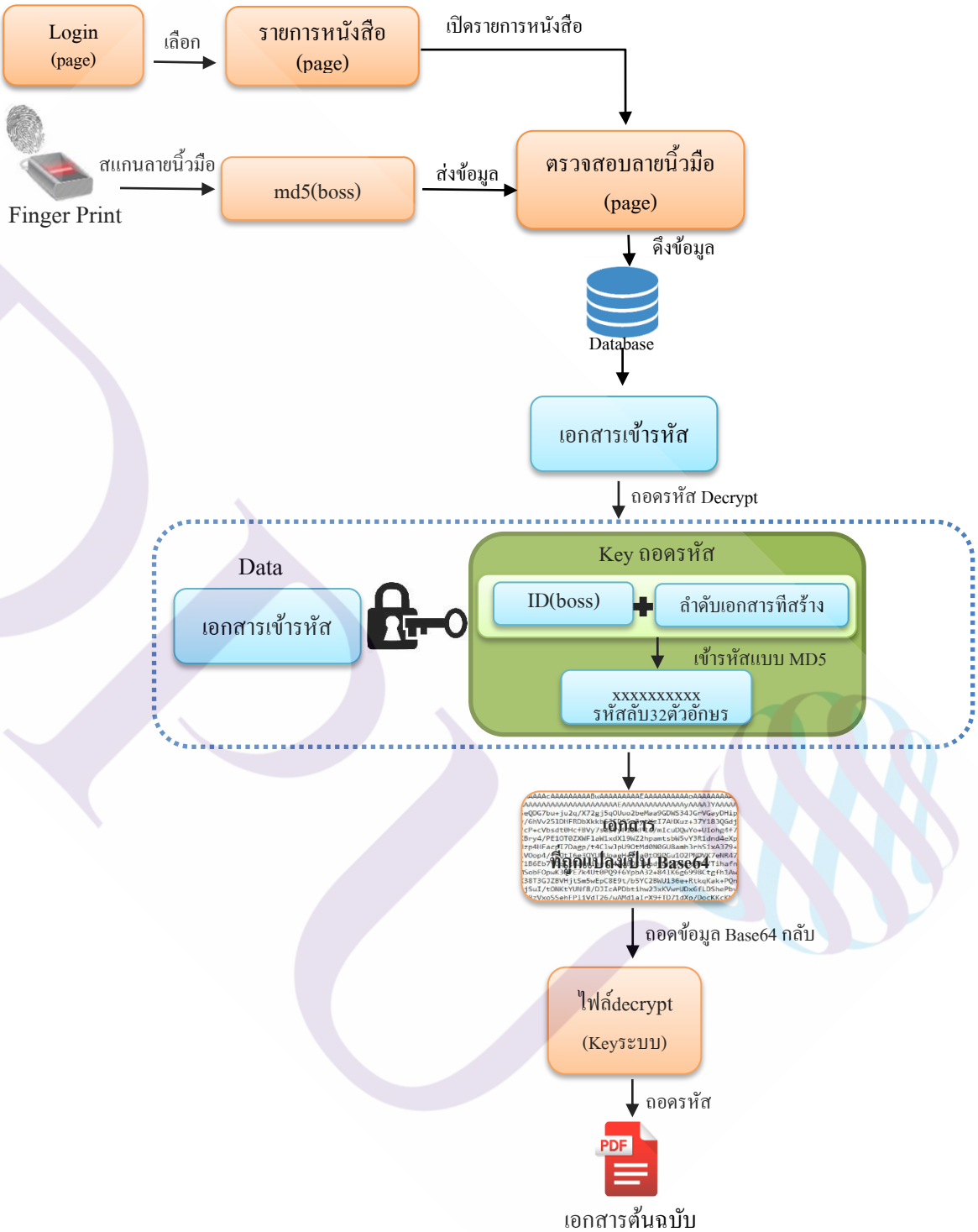
ภาพที่ 3.28 ขั้นตอนการส่งหนังสือ

1. คลิกหัวข้อหนังสือรอส่ง เลือกหน่วยงานปลายทางที่ต้องการส่ง

2. ระบบจะทำการสร้างรหัสลับ โดยทำการเข้ารหัสของเอกสารที่ถูกแปลงเป็น Base64 ด้วย คีย์รหัสลับ 32 ตัวอักษร (ที่ได้มาจาก รหัสผู้บังคับบัญชา และ ลำดับเอกสารที่สร้างมาทำการเข้ารหัสแบบ MD5)

3. จะได้เอกสารเข้ารหัสเก็บไว้ในฐานข้อมูล

3.5.2 ขั้นตอนการทำงาน ระบบการรับหนังสือ



ภาพที่ 3.29 ขั้นตอนการรับหนังสือ

1. login เข้าระบบ เลือกรายการหนังสือที่ต้องการเปิด หลังจากนั้นระบบจะเข้าหน้าต่างตรวจสอบลายนิ้วมือ

2. สแกนลายนิ้วมือของผู้บังคับบัญชาจากอุปกรณ์ Fingerprint Sensor จะได้ข้อมูล md5 ออกมาส่งข้อมูลเข้าหน้าเว็บเพจเพื่อทำการตรวจสอบ ดังนี้

2.1 ดึงข้อมูลเอกสารเข้ารหัสจากฐานข้อมูลมาทำการถอดรหัสด้วยคีย์รหัสลับ 32 ตัวอักษร (ที่ได้มาจากรหัสผู้บังคับบัญชาที่สแกนลายนิ้วมือ และ ลำดับเอกสารที่สร้าง มาทำการเข้ารหัสแบบ MD5)

2.2 จะได้ เอกสารที่ถูกแปลงเป็น Base64 มาทำการแปลงข้อมูลในรูปแบบ Base64 กลับ

2.3 จะได้ ไฟล์encrypt มาทำการถอดรหัสข้อมูลด้วย คีย์ของระบบที่กำหนดไว้

2.4 จะได้ เอกสารต้นฉบับ

บทที่ 4
ผลการดำเนินงาน

จากการดำเนินการพัฒนาระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ โดยมีการเชื่อมต่อ Fingerprint Sensor เข้ากับระบบงานสารบรรณอิเล็กทรอนิกส์ เพื่อยืนยันตัวบุคคลผู้ที่มีสิทธิ์ในการเข้าถึงข้อมูลเอกสารชั้นความลับ บนเครือข่าย localhost ภายในสำนักงานปลัดกระทรวงกลาโหม ซึ่งแบ่งการทดสอบระบบงาน ออกเป็น 3 ส่วน คือ (1) ทดสอบระบบบริหารจัดการลายนิ้วมือ (2) ทดสอบประสิทธิภาพของอุปกรณ์ Fingerprint Sensor และ (3) ทดสอบการทำงานในภาพรวมของระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ โดยมีรายละเอียด ดังนี้

4.1 ทดสอบระบบบริหารจัดการลายนิ้วมือ

แบ่งการทดสอบระบบบริหารจัดการลายนิ้วมือ แบ่งออกเป็น 5 หัวข้อ ดังนี้

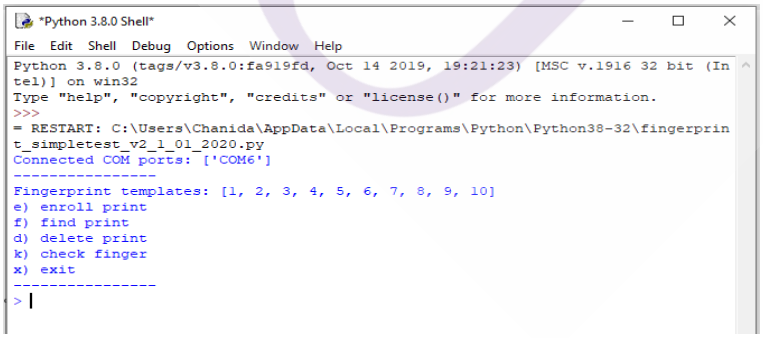
4.1.1 e) enroll print (การเพิ่มลายนิ้วมือ)

4.1.2 f) find print (การตรวจสอบลายนิ้วมือ)

4.1.3 d) delete print (การลบลายนิ้วมือ)

4.1.4 k) check finger (การส่งข้อมูลลายนิ้วมือ)

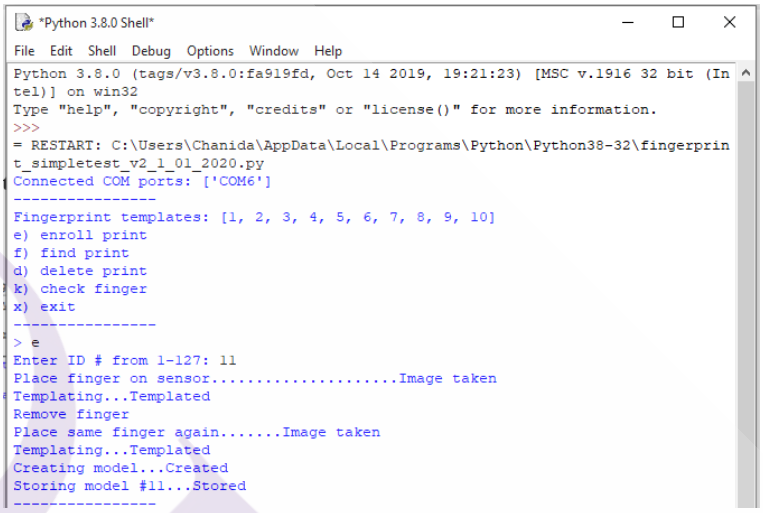
4.1.5 x) exit (ออกจากระบบ)



ภาพที่ 4.1 หัวข้อระบบบริหารจัดการลายนิ้วมือ

e) enroll print (การเพิ่มลายนิ้วมือ)

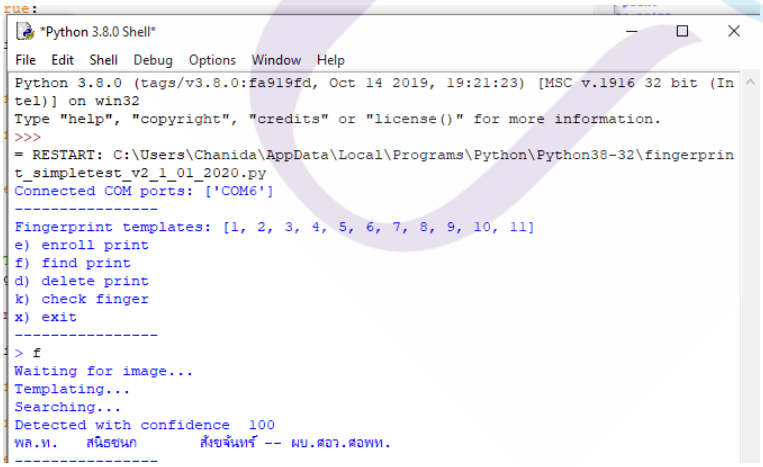
โดยพิมพ์คำว่า e สำหรับการเพิ่มลายนิ้วมือ ใส่ตัวเลขประจำหน่วยงาน แล้วทำการสแกนลายนิ้วมือผู้บริหาร 2 ครั้ง



ภาพที่ 4.2 การเพิ่มลายนิ้วมือ

f) find print (การตรวจสอบลายนิ้วมือ)

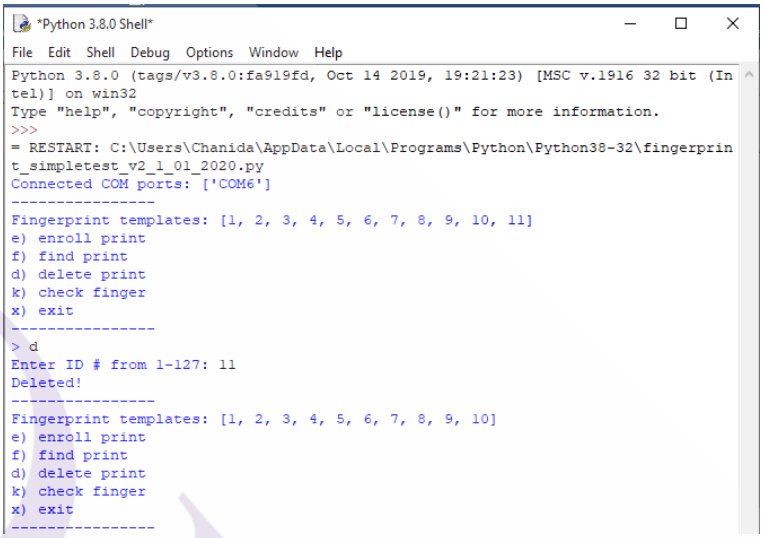
โดยพิมพ์คำสั่ง f สำหรับการตรวจสอบลายนิ้วมือว่าเป็นบุคคลใด จะแสดงยศ-ชื่อ-นามสกุลและตำแหน่งออกมา



ภาพที่ 4.3 การตรวจสอบลายนิ้วมือ

d) delete print (การลบลายนิ้วมือ)

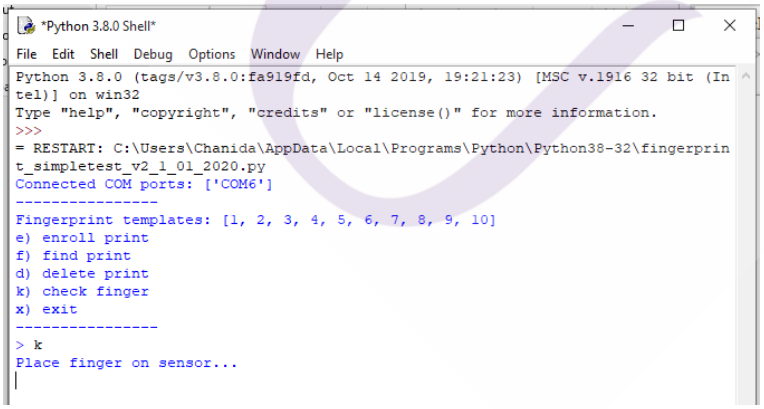
โดยพิมพ์คำสั่ง d หลังจากนั้นพิมพ์หมายเลขผู้บังคับบัญชาที่ต้องการลบลายนิ้วมือลงไป



ภาพที่ 4.4 การลบลายนิ้วมือ

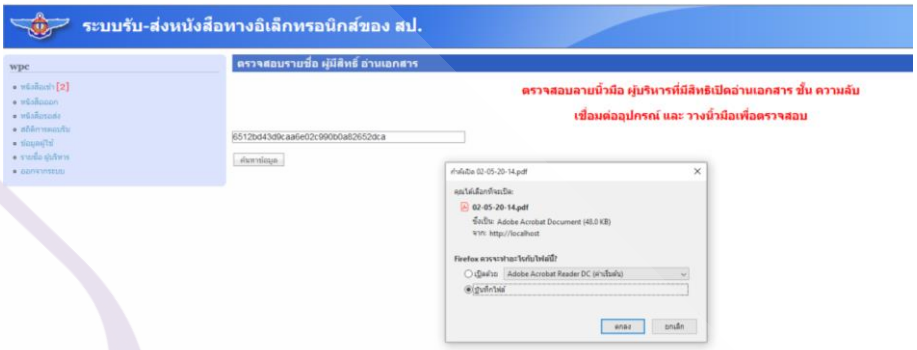
k) check finger (การส่งข้อมูลลายนิ้วมือ)

1. โดยพิมพ์คำสั่ง k สำหรับการส่งรหัสข้อมูลไปยังเว็บไซต์ จะเป็นขั้นตอนการยืนยันตัวตนในการรับหนังสือ สถานะนี้ต้องเปิดตลอดในการเชื่อมต่อข้อมูลระหว่างระบบการรับ-ส่งหนังสือราชการชั้นความลับ

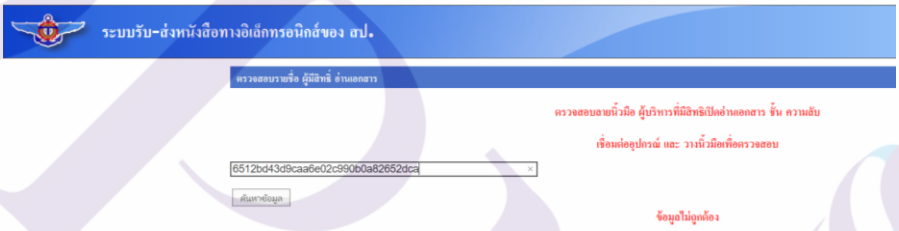


ภาพที่ 4.5 การส่งข้อมูลลายนิ้วมือ

2. หน้าต่างการตรวจสอบลายนิ้วมือ ในระบบการรับ-ส่ง หนังสือราชการชั้นความลับ โดยรับข้อมูลจากระบบบริหารจัดการลายนิ้วมือ ส่งข้อมูลมาเพื่อตรวจสอบว่าสามารถเข้าถึงชั้นความลับได้หรือไม่



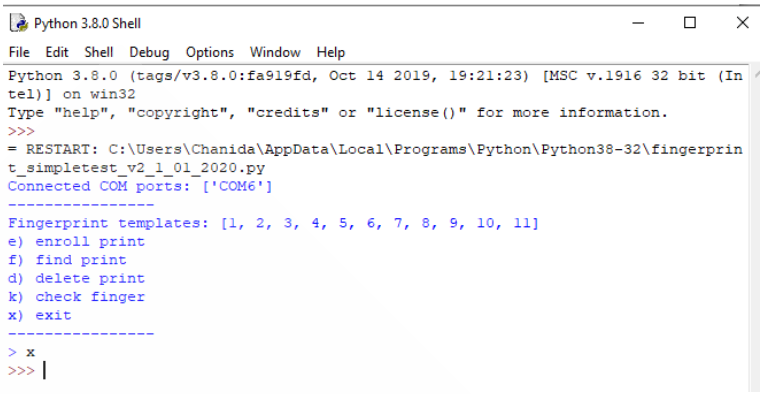
ภาพที่ 4.6 หน้าต่างการตวจสอบลายนิ้วมือ กรณีถูกต้อง



ภาพที่ 4.7 หน้าต่างการตวจสอบลายนิ้วมือ กรณีไม่ถูกต้อง

x) exit (ออกจากระบบ)

โดยพิมพ์คำสั่ง x สำหรับการออกจากระบบบริหารจัดการลายนิ้วมือ



ภาพที่ 4.8 ออกจากระบบบริหารจัดการลายนิ้วมือ

4.2 ทดสอบประสิทธิภาพของอุปกรณ์ Fingerprint Sensor

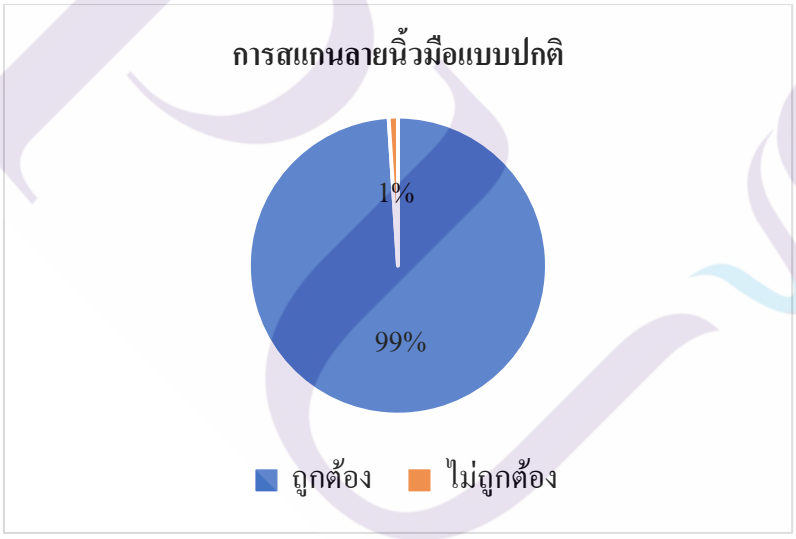
การทดสอบประสิทธิภาพของอุปกรณ์ Fingerprint Sensor โดยทำการทดสอบผ่านระบบการรับ-ส่ง หนังสือราชการชั้นความลับ ผู้เข้ารับการทดสอบจำนวน 10 คน โดยแบ่งการทดสอบเป็น 4 รายการ ดังนี้

4.2.1 ทดสอบการสแกนลายนิ้วมือแบบปกติ

การทดสอบโดยสแกนลายนิ้วมือแบบปกติ ทำการทดสอบการสแกนลายนิ้วมือจำนวน 10 ครั้ง จากผลการทดสอบทั้งหมด สแกนลายนิ้วมือผ่าน จำนวน 99 ครั้ง คิดค่าความถูกต้องเป็นร้อยละ 99 และสแกนลายนิ้วมือไม่ผ่าน จำนวน 1 ครั้ง คิดค่าความถูกต้อง เป็นร้อยละ 1 ดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 ทดสอบการสแกนลายนิ้วมือแบบปกติ

ทดสอบการสแกนลายนิ้วมือแบบปกติ										
ผู้เข้ารับการทดสอบ	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ครั้งที่ 4	ครั้งที่ 5	ครั้งที่ 6	ครั้งที่ 7	ครั้งที่ 8	ครั้งที่ 9	ครั้งที่ 10
บุคคลที่ 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 7	✓	✓	✓	✕	✓	✓	✓	✓	✓	✓
บุคคลที่ 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



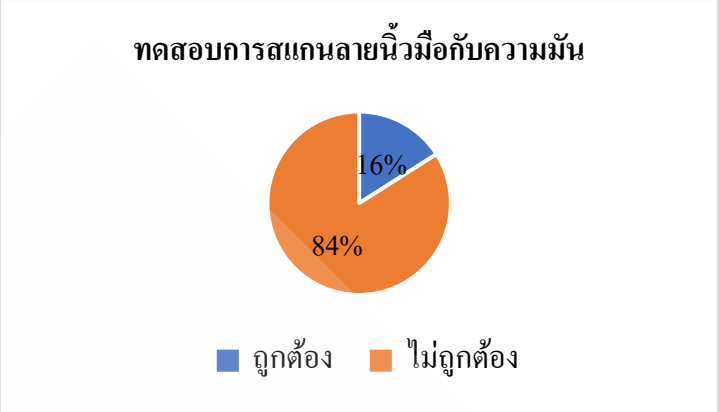
ภาพที่ 4.9 แผนภูมิผลการทดสอบการสแกนลายนิ้วมือแบบปกติ

4.2.2 ทดสอบการสแกนลายนิ้วมือกับความมัน

การทดสอบโดยสแกนลายนิ้วมือที่มีความมัน ซึ่งจะใช้ของเหลวที่มีความมันหยดลงบนลายนิ้วมือของผู้ทดสอบแต่ละคนก่อนทำการทดสอบ ทำการทดสอบการสแกนลายนิ้วมือจำนวน 10 ครั้ง จากผลการทดสอบทั้งหมด สแกนลายนิ้วมือผ่าน จำนวน 16 ครั้ง คิดค่าความถูกต้องเป็นร้อยละ 16 และสแกนลายนิ้วมือไม่ผ่าน จำนวน 84 ครั้ง คิดค่าความถูกต้อง เป็นร้อยละ 84 ดังแสดงในตารางที่ 4.2

ตารางที่ 4.2 ทดสอบการสแกนลายนิ้วมือกับความมัน

ทดสอบการสแกนลายนิ้วมือกับความมัน										
ผู้เข้ารับการทดสอบ	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ครั้งที่ 4	ครั้งที่ 5	ครั้งที่ 6	ครั้งที่ 7	ครั้งที่ 8	ครั้งที่ 9	ครั้งที่ 10
บุคคลที่ 1	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗
บุคคลที่ 2	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓
บุคคลที่ 3	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
บุคคลที่ 4	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓
บุคคลที่ 5	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
บุคคลที่ 6	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
บุคคลที่ 7	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗
บุคคลที่ 8	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
บุคคลที่ 9	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
บุคคลที่ 10	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗



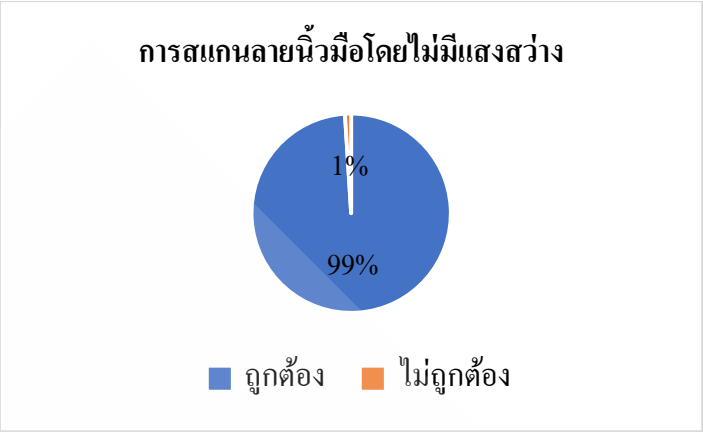
ภาพที่ 4.10 แผนภูมิผลการทดสอบการสแกนกับความมันของลายนิ้วมือ

4.2.3 ทดสอบการสแกนลายนิ้วมือโดยไม่มีแสงสว่าง

การทดสอบการสแกนลายนิ้วมือโดยไม่มีแสงสว่าง โดยทดสอบในห้องที่ทำการปิดไฟให้มีความสว่างน้อยที่สุด ทำการทดสอบการสแกนลายนิ้วมือ จำนวน 10 ครั้ง จากผลการทดสอบทั้งหมด สแกนลายนิ้วมือผ่าน จำนวน 99 ครั้ง คิดค่าความถูกต้อง เป็นร้อยละ 99 และสแกนลายนิ้วมือไม่ผ่าน จำนวน 1 ครั้ง คิดค่าความถูกต้อง เป็นร้อยละ 1 ดังแสดงในตารางที่ 4.3

ตารางที่ 4.3 ทดสอบการสแกนโดยไม่มีแสงสว่าง

ทดสอบการสแกนโดยไม่มีแสงสว่าง										
ผู้เข้ารับการทดสอบ	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ครั้งที่ 4	ครั้งที่ 5	ครั้งที่ 6	ครั้งที่ 7	ครั้งที่ 8	ครั้งที่ 9	ครั้งที่ 10
บุคคลที่ 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 7	✓	✓	✓	✓	✓	✓	✕	✓	✓	✓
บุคคลที่ 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



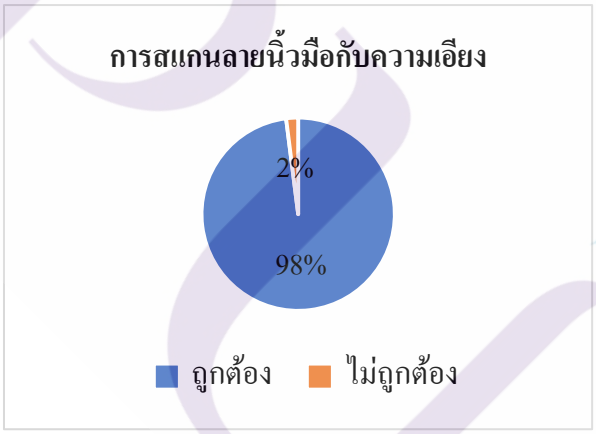
ภาพที่ 4.11 แผนภูมิการทดสอบการสแกนโดยไม่มีแสงสว่าง

4.2.4 ทดสอบการสแกนลายนิ้วมือกับความเอียง

การทดสอบการสแกนโดยทำการเอียงลายนิ้วมือ โดยทำการทดสอบแต่ละครั้งจะเอียงลายนิ้วมือโดยหมุนรอบเครื่องสแกน 180 องศา ทำการทดสอบการสแกนลายนิ้วมือ จำนวน 10 ครั้ง จากผลการทดสอบทั้งหมด สแกนลายนิ้วมือผ่าน จำนวน 98 ครั้ง คิดค่าความถูกต้อง เป็นร้อยละ 98 และสแกนลายนิ้วมือไม่ผ่าน จำนวน 2 ครั้ง คิดค่าความถูกต้องเป็นร้อยละ 2 ดังแสดงในตารางที่ 4.3

ตารางที่ 4.4 ทดสอบการสแกนลายนิ้วมือกับความเอียง

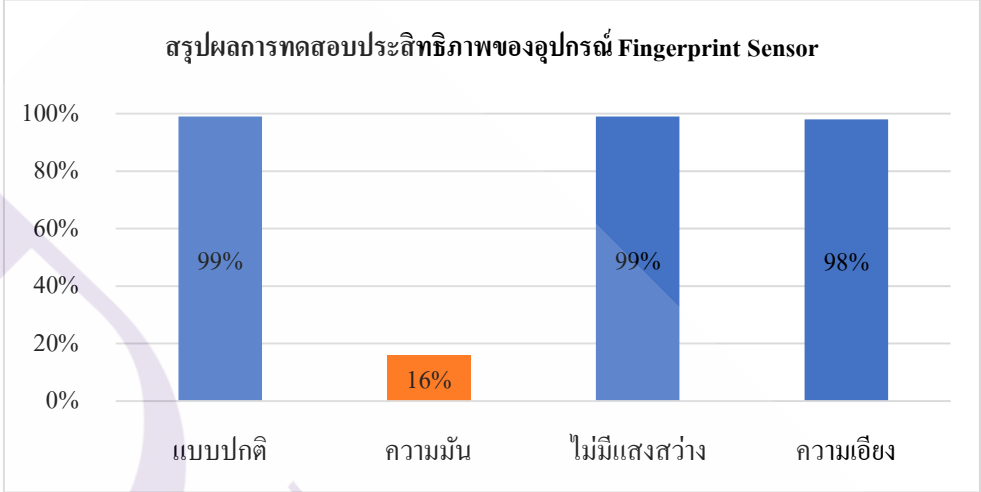
ทดสอบการสแกนลายนิ้วมือกับความเอียง										
ผู้เข้ารับการทดสอบ	ครั้งที่ 1	ครั้งที่ 2	ครั้งที่ 3	ครั้งที่ 4	ครั้งที่ 5	ครั้งที่ 6	ครั้งที่ 7	ครั้งที่ 8	ครั้งที่ 9	ครั้งที่ 10
บุคคลที่ 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 3	✓	✓	✕	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✕
บุคคลที่ 6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
บุคคลที่ 10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



ภาพที่ 4.12 แผนภูมิผลการทดสอบการสแกนลายนิ้วมือกับความเอียง

สรุปการทดสอบประสิทธิภาพของอุปกรณ์ Fingerprint Sensor ทั้งหมด 4 รายการแล้วนั้น พบว่าการสแกนลายนิ้วมือแบบปกติมีความถูกต้อง 99% สแกนลายนิ้วมือโดยไม่มีแสงสว่างมีความถูกต้อง 99% และสแกนลายนิ้วมือกับความเอียงมีความถูกต้อง 98% ซึ่งสรุปได้ว่าทั้ง 3 รายการนี้ไม่มีผลกระทบต่อประสิทธิภาพการทำงาน ในส่วนของการสแกนลายนิ้วมือกับความมันมี

ความถูกต้อง 16% ซึ่งมีผลกระทบต่อประสิทธิภาพการทำงานอย่างมาก อุปกรณ์ไม่สามารถทำงานได้อย่างถูกต้อง ดังแสดงในภาพที่ 4.12



ภาพที่ 4.13 แผนภูมิสรุปผลการทดสอบประสิทธิภาพของอุปกรณ์ Fingerprint Sensor

4.3 ทดสอบการทำงานในภาพรวมของระบบการรับ-ส่ง หนังสือราชการชั้นความลับ

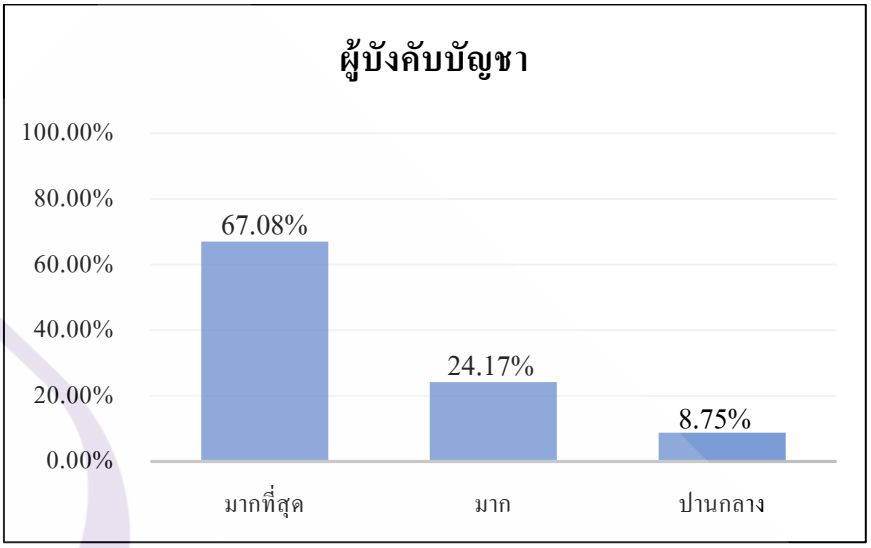
ทดสอบการทำงานตั้งแต่กระบวนการสร้างหนังสือจนถึงการรับหนังสือ โดยให้บุคคลที่ปฏิบัติงานเกี่ยวข้องในระบบงานทำการทดสอบ ซึ่งจะแบ่งบุคคลออกเป็น 3 กลุ่ม คือ ผู้บังคับบัญชา (ชั้นยศตั้งแต่ พ.อ.ขึ้นไป) จำนวน 10 คน, นายทหารคนสนิท จำนวน 10 คน และเจ้าหน้าที่ธุรการ จำนวน 20 คน รวมทั้งสิ้น 40 คน ทำการทดสอบระบบการ รับ-ส่ง หนังสือราชการชั้นความลับ ผ่าน Locallhost ทั้งนี้ผู้เข้ารับการทดสอบได้ทำการประเมินความพึงพอใจการใช้งานของระบบงาน ดังแสดงในตารางที่ 4.5 โดยใช้เกณฑ์ประเมินผลดังนี้

ระดับคะแนน	ค่าเฉลี่ย	ระดับความพึงพอใจ
5	4.51 – 5.00	มากที่สุด
4	3.51 – 4.50	มาก
3	2.51 – 3.50	ปานกลาง
2	1.51 – 2.50	น้อย
1	1.00 – 1.50	น้อยที่สุด

ตารางที่ 4.5 สรุปผลการประเมินความพึง

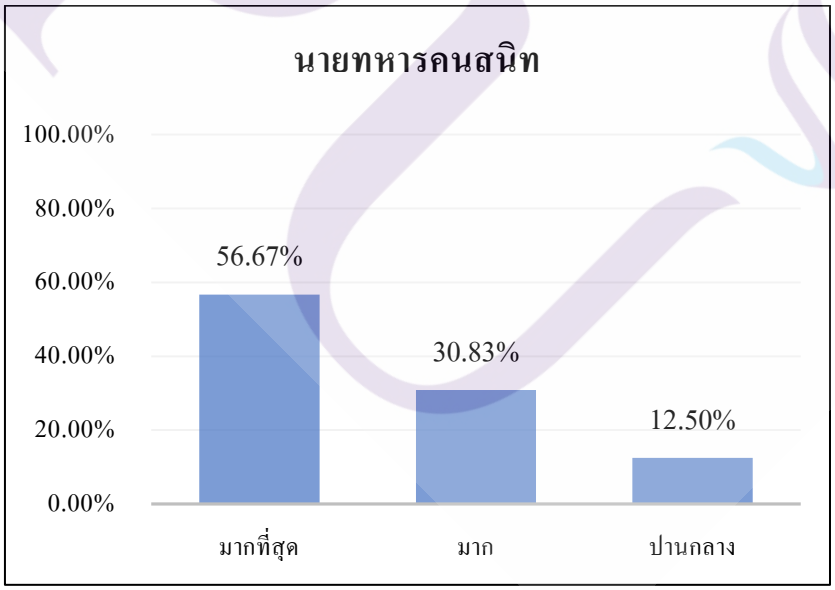
หัวข้อการประเมิน	ค่าเฉลี่ย	ความพึงพอใจ	ร้อยละ
1. ด้านการใช้ระบบงาน			
1.1 ความสะดวกสบายในการรับ-ส่ง หนังสือราชการชั้นความลับ	4.18	มาก	80.50
1.2 ความรวดเร็วในการรับ-ส่ง หนังสือราชการชั้นความลับ	4.93	มากที่สุด	98.50
1.3 การใช้งานของระบบงานไม่ซับซ้อน มีความเข้าใจง่าย	4.20	มาก	84
1.4 ความเหมาะสมของบุคคลในการเข้าถึงข้อมูลชั้นความลับ	3.80	มาก	76
1.5 ความเหมาะสมในการนำอุปกรณ์ Fingerprint sensor เข้ามายืนยันตัวบุคคล	4.95	มากที่สุด	99
1.6 ความเหมาะสมของระบบงาน	4.43	มาก	88.50
1.7 ความเร็วในการยืนยันตัวบุคคล	4.95	มากที่สุด	99
1.8 ความถูกต้องในการยืนยันตัวบุคคล	4.75	มากที่สุด	95
1.9 ระบบงานนี้สามารถรักษาหนังสือราชการชั้นความลับได้มากน้อยเพียงใด	4.33	มาก	86.50
1.10 ความปลอดภัยของข้อมูลชั้นความลับ	4.30	มาก	86
1.11 ความน่าเชื่อถือของระบบงานในการรักษาหนังสือราชการชั้นความลับ	4.28	มาก	85.50
1.12 ความน่าสนใจในการนำระบบงานมาประยุกต์ใช้งานจริง	4.93	มากที่สุด	98.50
	4.50	**มาก**	**90**
2. ด้านตัวอุปกรณ์ Fingerprint			
2.1 ความปลอดภัยในการใช้งาน	4.93	มากที่สุด	98.50
2.2 ความสะดวกสบายในการใช้งาน	4.95	มากที่สุด	97.50
2.3 อุปกรณ์สามารถยืนยันตัวบุคคลได้	4.90	มากที่สุด	98
2.4 ขนาดของอุปกรณ์ Fingerprint sensor มีความเหมาะสม	4.88	มากที่สุด	97.50
2.5 ความแข็งแรงของอุปกรณ์	4.73	มากที่สุด	94.50
2.6 ความง่ายในการใช้งานอุปกรณ์ Fingerprint sensor	5	มากที่สุด	100
	4.90	**มากที่สุด**	**97.92**
ผลรวม	**4.70**	**มากที่สุด**	**93.96**

การใช้งานระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



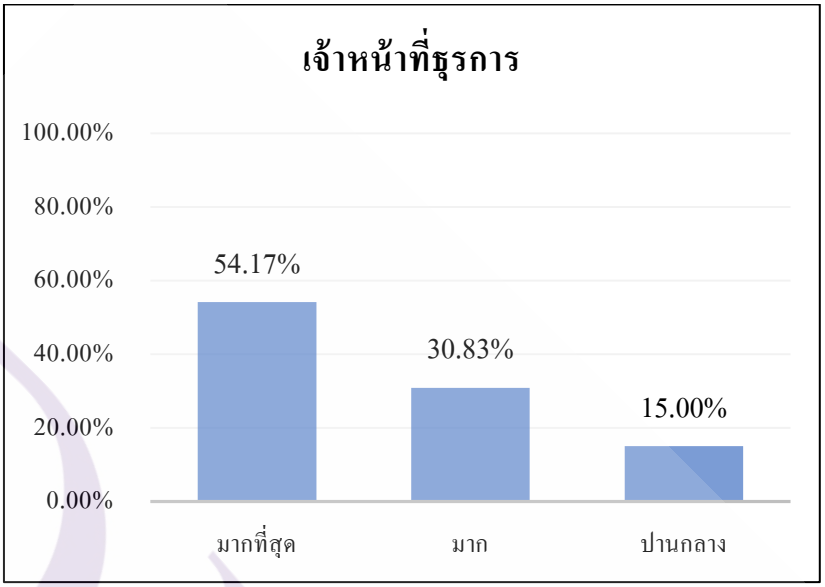
ภาพที่ 4.14 แผนภูมิความพึงพอใจของผู้บังคับบัญชาด้านการใช้งาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



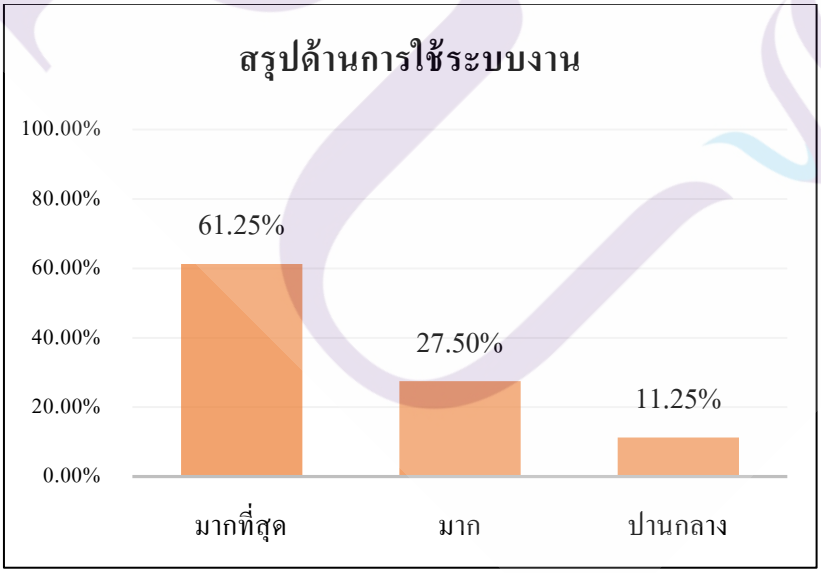
ภาพที่ 4.15 แผนภูมิความพึงพอใจของนายทหารคนสนิท ด้านการใช้งาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



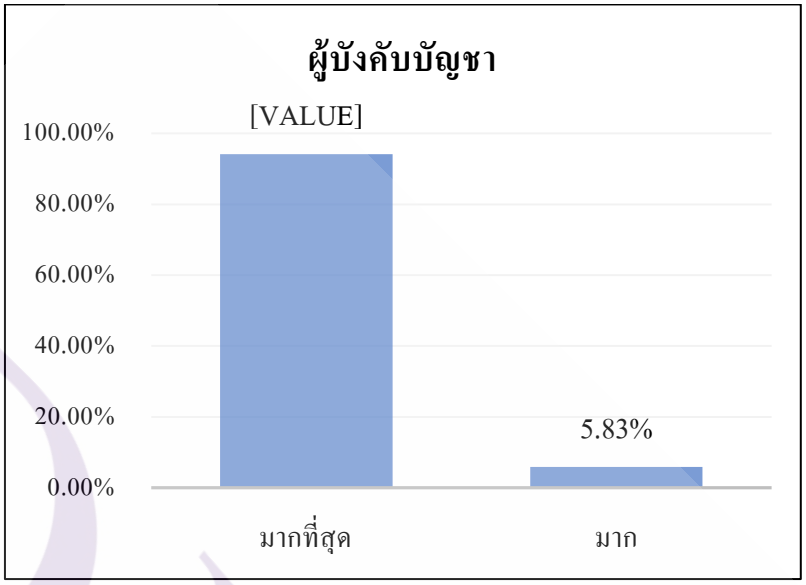
ภาพที่ 4.16 แผนภูมิความพึงพอใจของเจ้าหน้าที่ธุรการด้านการใช้งาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



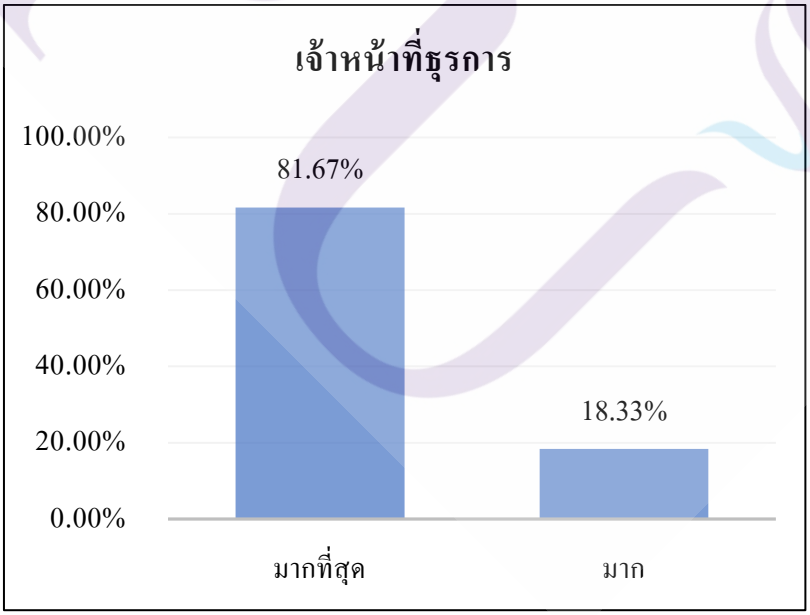
ภาพที่ 4.17 แผนภูมิสรุปความพึงพอใจด้านการใช้งาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



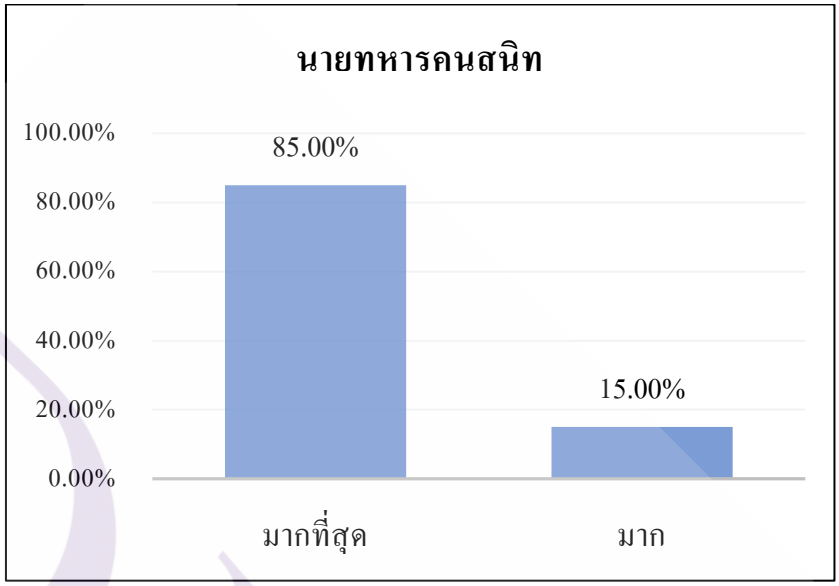
ภาพที่ 4.18 แผนภูมิความพึงพอใจของผู้บังคับบัญชา ด้านอุปกรณ์ Fingerprint sensor

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



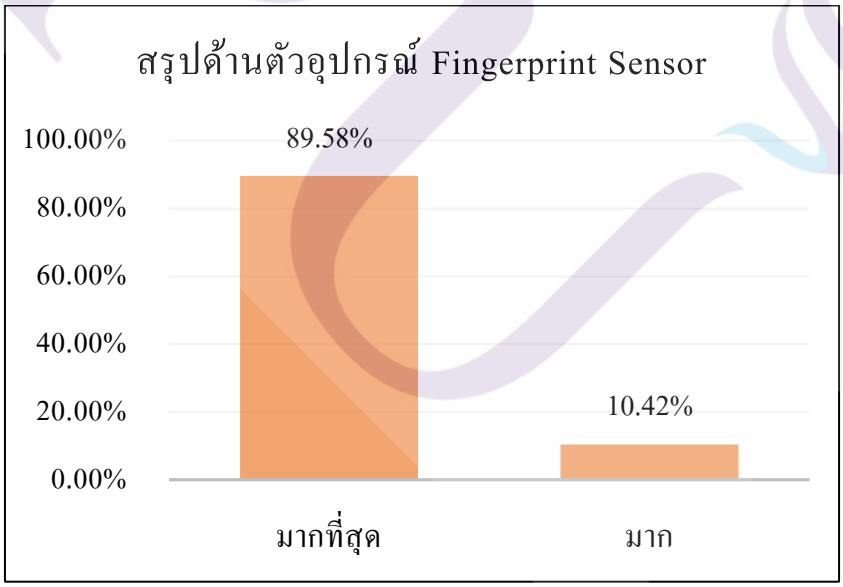
ภาพที่ 4.19 แผนภูมิความพึงพอใจของนายทหารคนสนิท ด้านอุปกรณ์ Fingerprint sensor

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



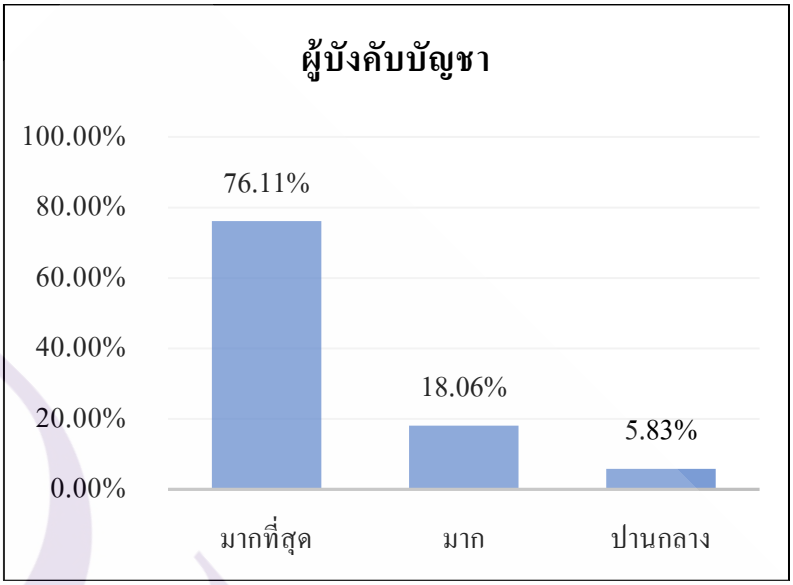
ภาพที่ 4.20 แผนภูมิความพึงพอใจของนายทหารคนสนิท ด้านอุปกรณ์ Fingerprint sensor

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



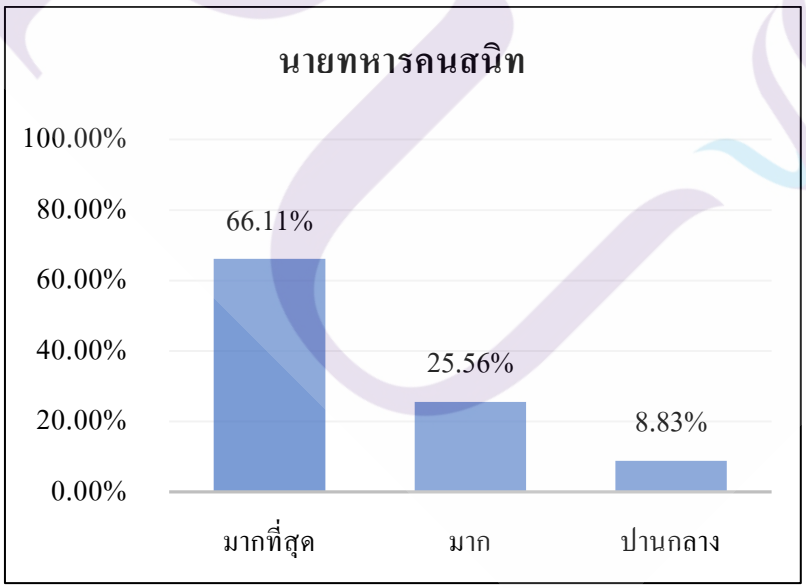
ภาพที่ 4.21 แผนภูมิสรุปความพึงพอใจ ด้านอุปกรณ์ Fingerprint sensor

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



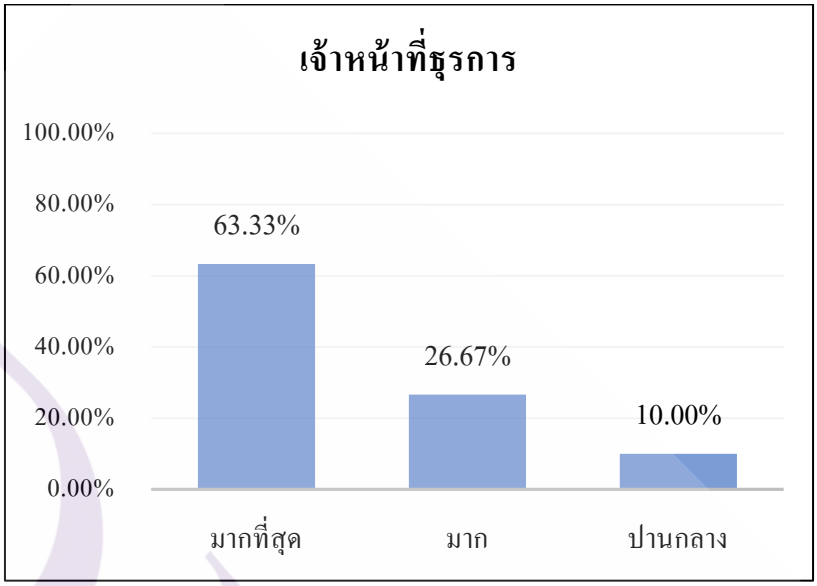
ภาพที่ 4.22 แผนภูมิความพึงพอใจของผู้บังคับบัญชาในภาพรวมทั้งหมดของระบบงาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



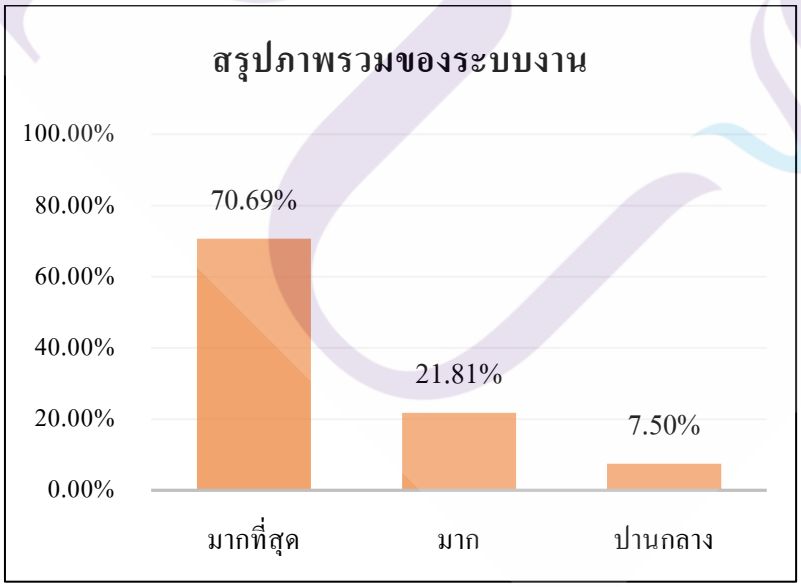
ภาพที่ 4.23 แผนภูมิความพึงพอใจของนายทหารคนสนิทในภาพรวมทั้งหมดของระบบงาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



ภาพที่ 4.24 แผนภูมิความพึงพอใจของเจ้าหน้าที่ธุรการในภาพรวมทั้งหมดของระบบงาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ



ภาพที่ 4.25 แผนภูมิสรุปความพึงพอใจในภาพรวมทั้งหมดของระบบงาน

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

สรุปผลการประเมินความพึงพอใจในภาพรวมทั้งหมดของระบบงาน เฉลี่ยอยู่ในระดับความพึงพอใจมากที่สุด คิดเป็นค่าเฉลี่ย 4.70 หรือร้อยละ 93.96 โดยแบ่งเป็น 2 ส่วนคือ

1. ส่วนด้านการใช้งานระบบงาน เฉลี่ยอยู่ในระดับความพึงพอใจมาก คิดเป็นค่าเฉลี่ย 4.50 หรือร้อยละ 90

2. ส่วนด้านตัวอุปกรณ์ Fingerprint sensor เฉลี่ยอยู่ในระดับความพึงพอใจมากที่สุด คิดเป็นค่าเฉลี่ย 4.90 หรือร้อยละ 97.92

บทที่ 5
สรุปผลและข้อเสนอแนะ

ในบทนี้เป็นการอภิปรายเพื่อสรุปผลที่ได้จากการทดสอบงานวิจัย รวมทั้งข้อจำกัดของระบบที่พบจากการทดสอบระบบ และข้อเสนอแนะสำหรับแนวทางในการพัฒนางานวิจัยนี้ต่อไป เพื่อแก้ไขข้อบกพร่องของระบบให้มีประสิทธิภาพมากขึ้น

5.1 สรุปผลการวิจัย

5.1.1 สรุปผลตามวัตถุประสงค์ของงานวิจัย

ในงานวิจัยนี้ออกแบบและพัฒนาระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ ให้มีการเชื่อมต่อกับ Fingerprint sensor เพื่อยืนยันตัวบุคคลในการรับหนังสือราชการชั้นความลับและสามารถบริหารจัดการลายนิ้วมือได้เป็นไปตามวัตถุประสงค์ของงานวิจัย ตลอดจนการประเมินผลของงานวิจัยจากผู้ทดสอบระบบงานอยู่ในเกณฑ์ที่ผู้วิจัย

5.1.2 สรุปผลตามขอบเขตของงานวิจัย

หลังจากทดสอบระบบในด้านต่าง ๆ แล้วนั้น ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ สามารถทำงานได้ตามขอบเขตงานวิจัย ตามที่กำหนดไว้ดังนี้

5.1.2.1 ระบบบริหารจัดการลายนิ้วมือสามารถ เพิ่ม, ลบ และ ค้นหาลายนิ้วมือพร้อมทั้งส่งข้อมูลไปยังระบบ รับ-ส่ง หนังสือราชการชั้นความลับได้

5.1.2.2 ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ สามารถเชื่อมต่อกับ Fingerprint sensor เพื่อยืนยันตัวบุคคลในการรับหนังสือราชการชั้นความลับได้อย่างถูกต้อง

5.1.2.3 บุคคลผู้ที่ปฏิบัติหน้าที่เกี่ยวข้องกับงานวิจัยทดสอบระบบงานพร้อมทั้งได้แสดงความคิดเห็นและข้อเสนอแนะ เพื่อเป็นข้อมูลประกอบการตัดสินใจสำหรับผู้บังคับบัญชาในการพิจารณาพัฒนาระบบงานต่อไป โดยผลสรุปการประเมินผลในภาพรวมของระบบงาน อยู่ในความพึงพอใจ ระดับมากที่สุด คิดเป็น 93.96 % บรรลุขอบเขตที่ตั้งไว้ โดยสรุปผลดังนี้

1) ผู้บังคับบัญชา มีความพึงพอใจในการใช้งาน ระบบมีความปลอดภัยในการรักษาข้อมูลชั้นความลับได้ดี เนื่องจากใช้เทคโนโลยีเข้ามาช่วยในการปกปิดข้อมูล โดยปฏิบัติระหว่างผู้บังคับบัญชาและผู้บังคับบัญชาโดยตรง จึงทำให้ขั้นตอนปฏิบัติรัดกลุมมากยิ่งขึ้น จึงทำให้ระบบงานมีความเหมาะสมที่จะนำระบบงานมาพัฒนาใช้แทนระบบงานเดิม ในส่วนของการเพิ่มขั้นตอนการปฏิบัติงานสำหรับผู้บังคับบัญชาซึ่งมองในการปฏิบัติงานจริงอาจเป็นการเพิ่มขั้นตอนการทำงานแต่ซึ่งเป็นการพัฒนาประสิทธิภาพการปฏิบัติงาน และเป็นการรักษาความมั่นคงแห่งรัฐ เห็นควรต้องปรับปรุงการปฏิบัติงานให้สอดคล้องต่อภาระกิจหน้าที่ อีกทั้งได้ให้ข้อเสนอแนะเพิ่มเติม โดยระบบควรพัฒนาเพิ่มบุคคลผู้มีสิทธิ์เข้าถึงข้อมูลชั้นความลับ เพื่อรองรับการสั่งการของผู้บังคับบัญชา จะเป็นการเพิ่มประสิทธิภาพการรักษาข้อมูลชั้นความลับให้มีประสิทธิภาพมากยิ่งขึ้น

2) เลขาประจำผู้บังคับบัญชา (นายทหารคนสนิท) มีความพึงพอใจในการใช้งาน ระบบมีความปลอดภัยในการรักษาข้อมูลชั้นความลับได้ดี และมีความเหมาะสมในพัฒนาระบบงานใช้แทนระบบงานเดิม อีกทั้งได้ให้ข้อเสนอแนะเพิ่มเติมเกี่ยวกับการปฏิบัติงานของผู้บังคับบัญชา ซึ่งอาจจะเป็นการเพิ่มภาระการทำงานให้กับผู้บังคับบัญชาหรือไม่ ซึ่งอาจจะต้องปรับเปลี่ยนระบบการปฏิบัติงานและทำความเข้าใจกันขั้นตอนการทำงานที่ตรงกัน

3) เจ้าหน้าที่ธุรการ มีความพึงพอใจในการใช้งาน ระบบมีความปลอดภัยในการรักษาข้อมูลชั้นความลับได้ดี และมีความเหมาะสมในพัฒนาระบบงานใช้แทนระบบงานเดิม ซึ่งเป็นระบบรับ-ส่ง หนังสือราชการชั้นความลับระหว่างผู้บังคับบัญชาโดยตรง ไม่ผ่านสายงานธุรการเป็นการลดขั้นตอนการปฏิบัติงานลงในส่วนธุรการ อีกทั้งเป็นการป้องกันการรั่วไหลของข้อมูลชั้นความลับได้ และหนังสือส่งถึงผู้บังคับบัญชาโดยตรงได้รวดเร็ว

5.2 ข้อจำกัดของระบบ

สารนิพนธ์ฉบับนี้ยังมีข้อจำกัดของระบบงานโดยมีรายละเอียดดังนี้

5.2.1 ระบบบริหารจัดการลายนิ้วมือต้องเปิดระบบตลอดเวลา มิฉะนั้นแล้วเมื่อสแกนลายนิ้วมือระบบบริหารจัดการจะไม่ส่งข้อมูลลายนิ้วมือไปยังระบบ รับ-ส่ง หนังสือราชการชั้นความลับ เพื่อทำการเข้าถึงข้อมูลชั้นความลับนั้นได้

5.2.2 ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับนั้น สามารถใช้งานภายในสำนักงานปลัดกระทรวงกลาโหมได้เท่านั้น

5.3 ข้อเสนอแนะ

ข้อเสนอแนะของระบบงานโดยสรุปผลจากการสำรวจความพึงพอใจ และผู้เข้ารับการทดสอบได้แสดงความคิดเห็นพร้อมข้อเสนอแนะหลังจากได้ทำการสอบระบบงาน สามารถสรุปผลได้ดังนี้

5.3.1 ระบบควรพัฒนาและออกแบบให้ผู้บังคับบัญชาแต่ละหน่วยงานมีผู้เข้าถึงชั้นความลับมากกว่า 1 คน ให้มีผู้ทำการแทน ในกรณีผู้บังคับบัญาติดภารกิจไม่สามารถปฏิบัติงานตามปกติได้

5.3.2 ระบบควรพัฒนาและออกแบบให้ผู้บังคับบัญชาระดับกองเข้าถึงชั้นความลับเพื่อรับการปฏิบัติจากการสั่งการของผู้บังคับชาระดับสูงได้โดยตรง

5.3.3 ระบบควรพัฒนาและออกแบบให้ผู้บังคับบัญชาสามารถสแกนลายนิ้วมือในการยืนยันตัวตนมากกว่า 1 ลายนิ้วมือ

5.3.4 พัฒนาระบบงานให้สามารถใช้งานบน Mobile Phone ได้

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

มนูญ บูลย์ประมุข (2555). ระบบสแกนลายนิ้วมือเคลื่อนที่สำหรับบันทึกการเข้าร่วมกิจกรรมของนักศึกษา. โปรแกรมวิชาเทคโนโลยีไฟฟ้าอุตสาหกรรม คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏกำแพงเพชร. สืบค้นเมื่อวันที่ 15 พฤศจิกายน 2562, จาก https://techno.kpru.ac.th/techno/images/PDF_research/publish/ publish_2557/research_publish_01.pdf

เอกภพ สกุลกิจกาญจน์ (2552). ระบบเซ็นชื่อเข้าและออกงานด้วยลายนิ้วมือผ่านทางเว็บไซต์, สารนิพันธ์วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร. สืบค้นเมื่อวันที่ 10 พฤศจิกายน 2562, จาก http://www.msit.mut.ac.th/thesis/Thesis_2554/027%20ระบบเซ็นชื่อเข้าและออกงานด้วยลายนิ้วมือผ่านทางเว็บไซต์.pdf

เนาวลักษณ์ แสงสนิท. [2556]. การพัฒนาระบบยืมหนังสือด้วยเครื่องสแกนลายนิ้วมือของสำนักหอสมุด. มหาวิทยาลัยทักษิณ, วิทยาเขตพัทลุง. สืบค้นเมื่อวันที่ 10 พฤศจิกายน 2562, จาก https://pulinet.oas.psu.ac.th/index.php/journal/article/view/9

สำรวน เวียงสมุทร. (2554). การระบุบุคคลด้วยไบโอเมตริกซ์. สาขาวิชาวิทยาการคอมพิวเตอร์คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม. สืบค้นเมื่อวันที่ 12 พฤศจิกายน 2562, จาก http://www.thaiscience.info/Journals/Article/JSMU/10888194.pdf

นัยนา มาแสง. (2551). เทคโนโลยีไบโอเมตริก. คณะวิทยาศาสตร์และเทคโนโลยี สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยธนบุรี สืบค้นเมื่อวันที่ 20 กุมภาพันธ์ 2562, จาก http://www.voip4share.com/viewtopic.php?f=12&t=4811

ซีเอ็มซีสเท็มเซอร์วิส. (2560). หลักการทำงาน Fingerprint. สืบค้นเมื่อ 13 พฤศจิกายน 2560, จาก http://www.cm-systemservice.com/Article/Detail/27425

ณัฐวุธ อวยชัยพรเลิศ.(2558). ระบบสแกนลายนิ้วมือ (FINGERPRINT). สืบค้นเมื่อ 13 พฤศจิกายน 2560, จาก https://biometricskmit.wordpress.com/2015/03/03/ระบบสแกนลายนิ้วมือ-fingerprint/

บริษัท ซีเคียวเมท จำกัด. (2561). สาระน่ารู้เกี่ยวกับ เครื่องสแกนลายนิ้วมือ (Finger Scan). สืบค้นเมื่อ 2 ตุลาคม 2562, จาก http://www.securemate.co.th/สาระน่ารู้-ระบบรักษาความปลอดภัย/สาระน่ารู้เกี่ยวกับ-เครื่องสแกนลายนิ้วมือ.html

บรรณานุกรม (ต่อ)

ภาษาไทย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2560). เทคโนโลยีความปลอดภัยของข้อมูล. สืบค้น เมื่อวันที่ 29 พฤษภาคม 2563, จาก https://www.nrca.go.th/content/02-1.html

มายพีเอ็ทพี. (2560). MD5 คืออะไร. สืบค้นเมื่อวันที่ 23 พฤศจิกายน 2562, จาก http://www.mindphp.com/คู่มือ/73-คืออะไร/2067-md5-คืออะไร.html

มายพีเอ็ทพี. (2560). วิธีการเข้ารหัส และถอดรหัส BASE64. สืบค้นเมื่อวันที่ 23 พฤศจิกายน 2562, จาก https://www.mindphp.com/developer/80-php-security/4082-encoding-decoding-base64.html

ภาษาต่างประเทศ

Jianjiang Feng. (2017). Fingerprint Recognition. Department of Automation Tsinghua University. Retrieved November 10, 2019, From http://www.comp.hkbu.edu.hk/wsb17/slides/Jianjiang_Feng.pdf

Mouad.M.H.Ali. (2016). Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching. Retrieved November 5, 2019, From https://ieeexplore.ieee.org/abstract/document/7544858?casa_token=6Czc--ERIMIAAAAA:YXb8TZ5pDWLkDdq9Q_gNiRLx-RnGnDOHHM8fpQK8s5rG9S0qr46Xzq3t2x3op5DmIHDKRBmGf9xD4A

Kambar Technologies. (2012). Biometrics Technology. Retrieved November 5, 2019, From http://accesscontrolconsult.in/biometric.html

ภาคผนวก

ภาคผนวก ก

คู่มือ อุปกรณ์ Fingerprint Module

GROW

R307 Fingerprint Module

User Manual

Hangzhou Grow Technology Co., Ltd

Feb 2011 Ver: 1.20

Preface & Declaration

Thank you for you selection of R307 Fingerprint Identification Module (Module) of GROW.

The Manual is targeted for hardware & software developing engineer, covering hardware interface, system resource, instruction system, installment information, etc. To ensure the developing process goes smoothly, it is highly recommended the Manual is read through carefully.

We will try our best to assure you the correctness of the Manual. However, should you find any problem or error with it, feel free to contact us or the sales representative of us. We would be very grateful.

Holding the principle of constantly improving and perfecting products, so both the module and contents of the Manual might subject to changes. Sorry for separate notice. You may visit our website or call us for the latest information.

The Manual contains proprietary information of GROW, which shall not be used by or disclosed to third parties without the permission of GROW, nor for any reproduction and alteration of information without any associated warranties, conditions, limitations, or notices.

No responsibility or liability is assumed by GROW for the application or use, nor for any infringements of patents or other intellectual property rights of third parties that may result from its use.

All products are sold subject to GROW's terms and conditions of sale supplied at the time of order acknowledgment. Testing, tool and other quality control techniques are used to the extent GROW considers necessary to support the warranty of relevant performance of its products to the specifications, except as expressly agreed to in writing by government requirements, testing of all parameters of each product is not necessarily performed.

GROW

I Introduction

Power	DC 4.2V-6V	**Interface**	UART(TTL logical level)/ USB 2.0
Working current	Typical: 50mA	**Matching Mode**	1:1 and 1:N
Baud rate	(9600*N)bps, N=1～12 (default N=6)	**Character file size**	256 bytes
Image acquiring time	<0.5s	**Template size**	512 bytes
Storage capacity	1000	**Security level**	5 (1, 2, 3, 4, 5(highest))
FAR	<0.001%	**FRR**	<0.1%
Average searching time	< 1s (1:1000)	**Window dimension**	19mm*21mm
Working environment	Temp: -10℃- +40℃	**Storage environment**	Temp: -40℃- +85℃
	RH: 20%-85%		RH: <85%
Outline Dimention	Split type	Module: 44.1*20*23.5 mm	

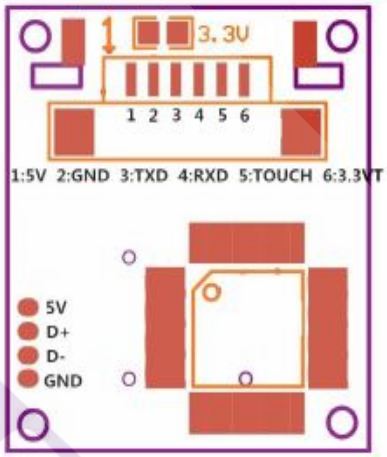
Operation Principle

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N).

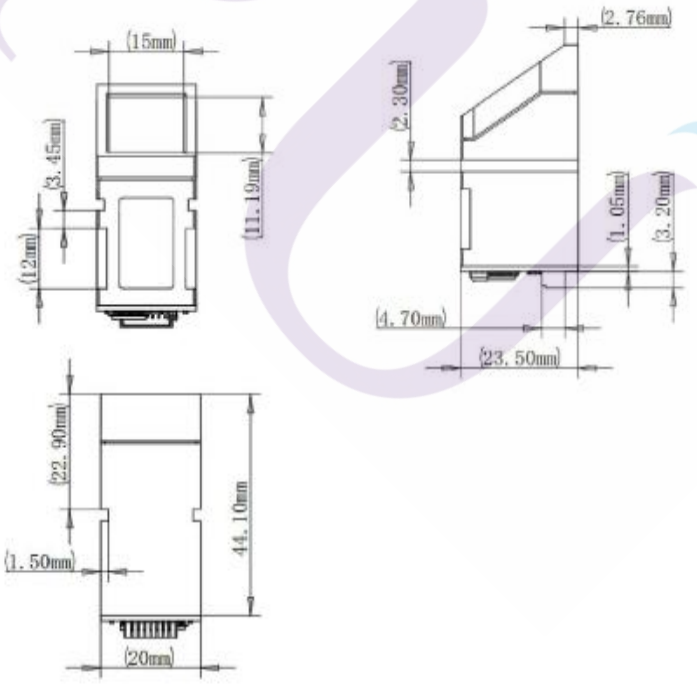
When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

II Hardware Interface

Exterior Interface



Dimension



Serial Communication

When the FP module communicates with user device, definition of J1 is as follows:

Pin Nmuber	Name	Type	Function Description
1	5V	in	Power input (DC4.2V - 6V)
2	GND	-	Signal ground. Connected to power ground
3	TXD	out	Data output. TTL logical level
4	RXD	in	Data input. TTL logical leve
5	Touch	out	Finger detection signal（maximum output current: 50mA）
6	3.3V	in	Finger detection power (DC3.3V - 5V、about 5uA)

Hardware connection

Via serial interface, the Module may communicate with MCU of 3.3V or 5V power: TXD (pin 3 of P1) connects with RXD (receiving pin of MCU), RXD (pin 4 of P1) connects with TXD (transferring pin of MCU). Should the upper computer (PC) be in RS-232 mode, please add level converting circuit, like MAX232, between the Module and PC.

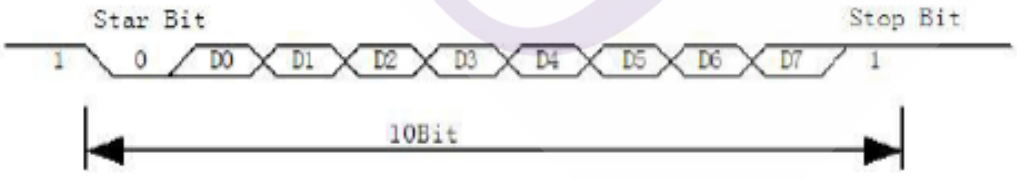
USB Communication

Pin Nmuber	Name	Type	Function Description
7	5V	in	Power input
8	D+	out	USB data output.
9	D-	in	USB data input.
10	GND	—	Signal ground.

Serial communication protocol

The mode is semiduplex asychronism serial communication. And the default baud rate is 57600bps. User may set the baud rate in 9600~115200bps。

Transferring frame format is 10 bit: the low-level starting bit, 8-bit data with the LSB first, and an ending bit. There is no check bit.



Reset time

At power on, it takes about 200ms for initialization. During this period, the Module can't accept commands for upper computer.

III System Resources

To address demands of different customer, Module system provides abundant resources at user's use.

Notepad

512-byte memory is set aside in flash for User's notepad. The notepad is divided into 16 pages logically, 32 bytes per page. The host can access any page by instruction GR_WriteNotepad or GR_ReadNotepad.
Note: when written, the whole page is taken as a whole and its former contents will be replaced.

Buffer

There are an image buffer and two 512-byte-character-file buffer within the RAM space of the module. Users can read & write any of the buffers by instructions.
Note: Contents of the above buffers will be lost at power-off.

Image buffer

ImageBuffer serves for image storage and the image format is 256*288 pixels, form is BMP.
When transferring through UART, to quicken speed, only the upper 4 bits of the pixel is transferred (that is 16 grey degrees). And two adjacent pixels of the same row will form a byte before the transferring. When uploaded to PC, the 16-grey-degree image will be extended to 256-grey-degree format. That's 8-bit BMP format.
When transferring through USB, the image is 8-bit pixel, that's 256 grey degrees.

Character file buffer

Character file buffer, CharBuffer1, CharBuffer2, can be used to store both character file and template file.

Fingerprint Library

Synstem sets aside a certain space within Flash for fingerprint template storage, that's fingerprint library. Contents of the library remain at power off.
Capacity of the library changes with the capacity of Flash, system will recognize the latter automatically. Fingerprint template's storage in Flash is in sequential order. Assume the fingerprint capacity N, then the serial number of template in library is 0, 1, 2, 3 … N. User can only access library by template number.

System Confiuration Parameter

To facilitate user's developing, Module opens part system parameters for use. And the basic instructions are SetSysPara & ReadSysPara. Both instructions take Parameter Number as

parameter.

When upper computer sends command to modify parameter, Module first responses with original configurations, then performs the parameter modification and writes configuration record into Flash. At the next startup, system will run with the new configurations.

Baud rate control (Parameter Number: 4)

The Parameter controls the UART communication speed of the Modul. Its value is an integer N, N= [1, 12]. Cooresponding baud rate is 9600*N bps。

Security Level (Parameter Number: 5)

The Parameter controls the matching threshold value of fingerprint searching and matching. Security level is divided into 5 grades, and cooresponding value is 1, 2, 3, 4, 5. At level 1, FAR is the highest and FRR is the lowest; however at level 5, FAR is the lowest and FRR is the highest.

Data package length (Parameter Number: 6)

The parameter decides the max length of the transferring data package when communicating with upper computer. Its value is 0, 1, 2, 3, corresponding to 32 bytes, 64 bytes, 128 bytes, 256 bytes respectively.

System status register

System status register indicates the current operation status of the Module. Its length is 1 word, and can be read via instruction *ReadSysPara*. Definition of the register is as follows:

Bit Num	15 4	3	2	1	0
Description	Reserved	ImgBufStat	PWD	Pass	Busy

Note:

Busy：1 bit. 1: system is executing commands; 0: system is free;

Pass：1 bit. 1: find the matching finger; 0: wrong finger;

PWD：1 bit. 1: Verified device's handshaking password.

ImgBufStat：1 bit. 1: image buffer contains valid image.

Module password

At power-on reset, system first checks whether the handshaking password has been modified. If not, system deems upper computer has no requirement of verifying password and will enter into normal operation mode. That's, when Module password remains the default, verifying process can be jumped. The password length is 4 bytes, and its default factory value is 0FFH, 0FFH, 0FFH, 0FFH. Should the password have be modified, *refer to instruction SetPwd*, then Module (or device) handshaking password must be verified before the system enter into normal operation mode. Or else, system will refuse to execute and command.

The new modified password is stored in Flash and remains at power off.

GROW

Module address

Each module has an identifying address. When communicating with upper computer, each instruction/data is transferred in data package form, which contains the address item. Module system only responds to data package whose address item value is the same with its identifying address.

The address length is 4 bytes, and its default factory value is 0xFFFFFFFF. User may modify the address via instruction *SetAdder*. The new modified address remains at power off.

Random number generator

Module integrates a hardware 32-bit random number generator (RNG) (without seed). Via instruction *GetRandomCode*, system will generate a random number and upload it.

IV Communication Protocol

The protocol defines the data exchanging format when R30X series communicates with upper computer. The protocol and instruction sets apples for both UART and USB communication mode. For PC, USB interface is strongly recommended to improve the exchanging speed, especially in fingerprint scanning device.

5.1 Data package format

When communicating, the transferring and receiving of command/data/result are all wrapped in data package format.

Data package format

Header	Adder	Package identifier	Package length	Package content (instuction/data/Parameter)	Checksum

Definition of Data package

Name	Symbol	Length	Description	
Header	Start	2 bytes	Fixed value of 0xEF01; High byte transferred first.	
Adder	ADDER	4 bytes	Default value is 0xFFFFFFFF, which can be modified by command. High byte transferred first and at wrong adder value, module will reject to transfer.	
Package identifier	PID	1 byte	01H	Command packet;
			02H	Data packet; Data packet shall not appear alone in executing processs, must follow command packet or acknowledge packet.
			07H	Acknowledge packet;

			08H	End of Data packet.
Package length	LENGTH	2 bytes	Refers to the length of package content (command packets and data packets) plus the length of Checksum(2 bytes). Unit is byte. Max length is 256 bytes. And high byte is transferred first.	
Package contents	DATA	—	It can be commands, data, command' s parameters, acknowledge result, etc. (fingerprint character value, template are all deemed as data);	
Checksum	SUM	2 bytes	The arithmetic sum of package identifier, package length and all package contens. Overflowing bits are omitted. high byte is transferred first.	

Check and acknowledgement of data package

Note: Commands shall only be sent from upper computer to the Module, and the Module acknowledges the commands.

Upon receipt of commands, Module will report the commands execution status and results to upper computer through acknowledge packet. Acknowledge packet has parameters and may also have following data packet. Upper computer can't ascertain Module's package receiving status or command execution results unless through acknowledge packet sent from Module. Acknowledge packet includes 1 byte confirmation code and maybe also the returned parameter.

Confirmation code's definition is :

00h: commad execution complete;
01h: error when receiving data package;
02h: no finger on the sensor;
03h: fail to enroll the finger;
04h: fail to generate character file due to the over-disorderly fingerprint image;
05h: fail to generate character file due to the over-wet fingerprint image;
06h: ail to generate character file due to the over-disorderly fingerprint image;
07h: fail to generate character file due to lackness of character point or over-smallness of fingerprint image
08h: finger doesn't match;
09h: fail to find the matching finger;
0Ah: fail to combine the character files;
0Bh: addressing PageID is beyond the finger library;
0Ch: error when reading template from library or the template is invalid;
0Dh: error when uploading template;
0Eh: Module can't receive the following data packages.
0Fh: error when uploading image;
10h: fail to delete the template;
11h: fail to clear finger library;
13h: wrong password!
15h: fail to generate the image for the lackness of valid primary image;
18h: error when writing flash;
19h: No definition error;

1Ah: invalid register number;
1Bh: incorrect configuration of register;
1Ch: wrong notepad page number;
1Dh: fail to operate the communication port;
others: system reserved;
41h: No finger on sensor when add fingerprint on second time.
42h: fail to enroll the finger for second fingerprint add.
43h: fail to generate character file due to lackness of character point or over-smallness of fingerprint image for second fingerprint add
44h: fail to generate character file due to the over-disorderly fingerprint image for second fingerprint add;
45h: Duplicate fingerprint

V Module Instruction System

R30X series provide 23 instructions. Through combination of different instructions, application program may realize muti finger authentication functions. All commands/data are transferred in package format. *Refer to 5.1 for the detailed information of package.*

System-related instructions

Verify passwoard VfyPwd

Description: Verify Module's handshaking password. (Refer to 4.6 for details)
Input Parameter: PassWord (4 bytes)
Return Parameter: Confirmation code (1 byte)
Instruction code: 13H
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	4 byte	2 bytes
Header	Module address	Package identifier		Instruction code	Password	Checksum
0xEF01	xxxx	01H	07H	13H	PassWord	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package Length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	xxH	sum

Note: Confirmation code = 00H: Correct password;
Confirmation code = 01H: error when receiving package;
Confirmation code = 13H: Wrong password;

Set password SetPwd

Description: Set Module's handshaking password. (Refer to 4.6 for details)
Input Parameter: PassWord (4 bytes)

Return Parameter: Confirmation code (1 byte)

Instruction code: 12H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	4 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Password	Checksum
0xEF01	xxxx	01H	07H	12H	PassWord	sum

Acknowledge package format:

2 bytes	4 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package length	Confirmation code	Checksum
0xEF01	xxxx	03H	xxH	Sum

Note: Confirmation code=00H: password setting complete;

Confirmation code=01H: error when receiving package;

Set Module address SetAdder

Description: Set Module address. (Refer to 4.7 for adderss information)

Input Parameter: None;

Return Parameter: Confirmation code (1 byte)

Instruction code: 15H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	4 bytes	2 bytes
Header	Original Module address	Package identifier	Package length	Instruction code	New Module address	Checksum
0xEF01	xxxx	01H	07H	15H	xxxx	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	New Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	07H	xxH	Sum

Note: Confirmation code=00H: address setting complete;

Confirmation code=01H: error when receiving package;

Set module system's basic parameter SetSysPara

Description: Operation parameter settings. (Refer to 4.4 for more information)

Input Parameter: Parameter number;

Return Parameter: Confirmation code (1 byte)

Instruction code: 0eH

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1byte	1byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Parameter number	Contents	Checksum
0xEF01	Xxxx	01H	05H	0eH	4/5/6	xx	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	Sum

Note: Confirmation code=00H: parameter setting complete;
Confirmation code=01H: error when receiving package;
Confirmation code=1aH: wrong register number;

Port Control Control

Description:

For UART protocol, it control the "on/off" of USB port;
For USB protocol, it control the "on/off" of UART port;

Input Parameter: control code

Control code "0" means turns off the port;
Control code "1" means turns on the port;

Return Parameter: confirmation code;

Instruction code: 17H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1byte	2 bytes
Header	Chip address	Package identifier	Package length	Instruction code	Control code	Checksum
0xEF01	xxxx	01H	04H	17H	0/1	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Chip address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	xxH	sum

Note: Confirmation code=00H: Port operation complete;
Confirmation code=01H: error when receiving package;
Confirmation code=1dH: fail to operate the communication port;

Read system Parameter ReadSysPara

Description: Read Module's status register and system basic configuration parameters;(Refer to 4.4 for system configuration parameter and 4.5 for system status register).

Input Parameter: none

Return Parameter: Confirmation code (1 byte) + basic parameter (16bytes)

Instuction code: 0fH

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	Xxxx	01H	03H	0fH	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	16 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Basic parameter list	Checksum
0xEF01	xxxx	07H	3+16	xxH	See following table	sum

Note: Confirmation code=00H: read complete;

Confirmation code=01H: error when receiving package;

Name	Description	Offset (word)	Size (word)
Status register	Contents of system status register	0	1
System identifier code	Fixed value: 0x0009	1	1
Finger library size	Finger library size	2	1
Security level	Security level (1, 2, 3, 4, 5)	3	1
Device address	32-bit device address	4	2
Data packet size	Size code (0, 1, 2, 3)	6	1
Baud settings	N (baud = 9600*N bps)	7	1

Read valid template number TempleteNum

Description: read the current valid template number of the Module

Input Parameter: none

Return Parameter: Confirmation code (1 byte)，template number:N

Instuction code: 1dH

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	xxxx	01H	0003H	1dH	0021H

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Template number	Checksum
0xEF01	xxxx	07H	5	xxH	N	sum

Note: Confirmation code=00H: read complete;

Confirmation code=01H: error when receiving package;

Fingerprint verification GR_Auto Search

Description: Match captured fingerprint with fingerprint library ,then return the result. Self-define time for capture , Search start position code and search quantity.

Input parameter: capture time, start bit number, search quantity

Return parameter: Confirmation code; page; Match score

Instruction code: 32H

Command (or instruction) package format:

2 bytes	4 bytes	1 bytes	2 bytes	1 bytes	1 bytes	2 bytes	2 bytes	2 bytes
Header	Original	Package	Package	Instructi	Time	start bit	search	Checksu

	Module address	identifier	length	on code	for capture	number	quantity	m
0xEF01	xxxx	01H	08H	32H	xxH	xxxxH	xxH	sum

Note:

1. original module address: 0XFFFFFFFF
2. capture time: 0~ffH，0x20≈ 4.5s，0x25 ≈ 5.5 秒，0x30 ≈ 6.5 秒.
3. Start bit: 0~ max fingerprint capacity
4. Search quantity: 0 ~ N-1 max fingerprint capacity

Acknowledge package format:

2 bytes	4 bytes	1 bytes	2 bytes	1 bytes	2 bytes	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	page	score	Checksum
0xEF01	xxxx	07H	07H	xxH	PageID	MatchScore	sum

Note:

1. Confirmation code=00H: read complete;
2. Confirmation code=01H: error when receiving package
3. Confirmation code=06H:fail to generate character file due to the over-disorderly fingerprint image;
4. Confirmation code=07H: fail to generate character file due to lackness of character point or over-smallness of fingerprint image;
5. Confirmation code=09H: No matching in the library (both the PageID and matching score are 0);

Automatic Fingerprint verification GR_Identify

Description: Automatic collect fingerprint, match captured fingerprint with fingerprint library and return result.

Input parameter: None

Return parameter: Confirmation code; page; Match score

Instruction code: 34H

Command (or instruction) package format:

2 bytes	4 bytes	1 byte	2 byte	1 byte	2 byte
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	xxxx	01H	03H	34H	38H

Note: Default module address: 0XFFFFFFFF

2 bytes	4 bytes	1 bytes	2 bytes	1 bytes	2 bytes	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	page	score	Checksum
0xEF01	xxxx	07H	07H	xxH	PageID	MatchScore	sum

Acknowledge package format:

Note:

1. Confirmation code=00H: read complete;
2. Confirmation code=01H: error when receiving package
3. Confirmation code=06H:fail to generate character file due to the over-disorderly fingerprint image;
4. Confirmation code=07H: fail to generate character file due to lackness of character point or over-smallness of fingerprint image;
5. Confirmation code=09H: No matching in the library (both the PageID and matching score are 0);

Fingerprint-processing instructions

To collect finger image GenImg

Description: detecting finger and store the detected finger image in ImageBuffer while returning successfull confirmation code; If there is no finger, returned confirmation code would be "can't detect finger".

Input Parameter: none

Return Parameter: Confirmation code (1 byte)

Instuction code: 01H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	Xxxx	01H	03H	01H	05H

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	Sum

Note: Confirmation code=00H: finger collection successs;
Confirmation code=01H: error when receiving package;
Confirmation code=02H: can't detect finger;
Confirmation code=03H: fail to collect finger;

Upload image UpImage

Description: to upload the image in Img_Buffer to upper computer. Refer to 1.1.1 for more about image buffer.

Input Parameter: none

Return Parameter: Confirmation code (1 byte)

Instuction code: 0aH

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum

0xEF01	Xxxx	01H	03H	0aH	000eH

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	sum

Note 1： Confirmation code=00H: ready to transfer the following data packet;
Confirmation code=01H: error when receiving package;
Confirmation code=0fH: fail to transfer the following data packet;
2： Module shall transfer the following data packet after responding to the upper computer.

Download the image DownImage

Description: to download image from upper computer to Img_Buffer. Refer to 1.1.1 for more about the image buffer.
Input Parameter: none
Return Parameter: Confirmation code (1 byte)
Instuction code: 0bH
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	Xxxx	01H	03H	0bH	000fH

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	sum

Note: 1：Confirmation code=00H: ready to transfer the following data packet;
Confirmation code=01H: error when receiving package;
Confirmation code=0eH: fail to transfer the following data packet;
2：Module shall transfer the following data packet after responding to the upper computer. Data package length must be 64, 128, or 256。

To generate character file from image Img2Tz

Description: to generate character file from the original finger image in ImageBuffer and store the file in CharBuffer1 or CharBuffer2.
Input Parameter: BufferID (character file buffer number)
Return Parameter: Confirmation code (1 byte)
Instuction code: 02H
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Buffer number	Checksum

0xEF01	xxxx	01H	04H	02H	BufferID	sum

Note: BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values (except 1h, 2h) would be processed as CharBuffer2.

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	XxH	sum

Note: Confirmation code=00H: generate character file complete;
Confirmation code=01H: error when receiving package;
Confirmation code=06H: fail to generate character file due to the over-disorderly fingerprint image;
Confirmation code=07H: fail to generate character file due to lackness of character point or over-smallness of fingerprint image;
Confirmation code=15H: fail to generate the image for the lackness of valid primary image;

To generate template RegModel

Description: To combine information of character files from CharBuffer1 and CharBuffer2 and generate a template which is stroed back in both CharBuffer1 and CharBuffer2.
Input Parameter: none
Return Parameter: Confirmation code (1 byte)
Instuction code: 05H
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	xxxx	01H	03H	05H	09H

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	xxH	sum

Note: Confirmation code=00H: operation success;
Confirmation code=01H: error when receiving package;
Confirmation code=0aH: fail to combine the character files. That's, the character files don't belong to one finger.

To upload character or template UpChar

Description: to upload the character file or template of CharBuffer1/CharBuffer2 to upper computer;
Input Parameter: BufferID (Buffer number)
Return Parameter: Confirmation code (1 byte)

Instuction code: 08H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Buffer number	Checksum
0xEF01	xxxx	01H	04H	08H	BufferID	sum

Note: BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values (except 1h, 2h) would be processed as CharBuffer2.

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	xxH	sum

Note 1: Confirmation code=00H: ready to transfer the following data packet;
Confirmation code=01H: error when receiving package;
Confirmation code=0dH: error when uploading template;
2: Module shall transfer following data packet after responding to the upper computer.;
3: The instruction doesn't affect buffer contents.

To download character file or template DownChar

Description: to download character file or template from upper computer to the specified buffer of Module;

Input Parameter: BufferID (buffer number)

Return Parameter: Confirmation code (1 byte)

Instuction code: 09H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	buffer number	Checksum
0xEF01	xxxx	01H	04H	09H	BufferID	sum

Note: BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values (except 1h, 2h) would be processed as CharBuffer2.

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	xxH	sum

Note 1: Confirmation code=00H: ready to transfer the following data packet;
Confirmation code=01H: error when receiving package;
Confirmation code=0eH: fail to receive the following data packages.
2: Module shall transfer the following data packet after responding to the upper computer.

To store template Store

Description: to store the template of specified buffer (Buffer1/Buffer2) at the designated location of Flash library.

Input Parameter: BufferID(buffer number), PageID（Flash location of the template, two bytes with high byte front and low byte behind）

Return Parameter: Confirmation code (1 byte)

Instuction code: 06H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1 byte	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	buffer number	Location number	Checksum
0xEF01	xxxx	01H	06H	06H	BufferID	PageID	sum

Note: BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values (except 1h, 2h) would be processed as CharBuffer2.

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	sum

Note: Confirmation code=00H: storage success;
Confirmation code=01H: error when receiving package;
Confirmation code=0bH: addressing PageID is beyond the finger library;
Confirmation code=18H: error when writing Flash.

To read template from Flash library LoadChar

Description: to load template at the specified location (PageID) of Flash library to template buffer CharBuffer1/CharBuffer2

Input Parameter: BufferID(buffer number), PageID (Flash location of the template, two bytes with high byte front and low byte behind)。

Return Parameter: Confirmation code (1 byte)

Instuction code: 07H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1 byte	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	buffer number	Page number	Checksum
0xEF01	xxxx	01H	06H	07H	BufferID	PageID	sum

Note: BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values (except 1h, 2h) would be processed as CharBuffer2.

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	XxH	sum

Note: Confirmation code=00H: load success;
Confirmation code=01H: error when receiving package;
Confirmation code=0cH: error when reading template from library or the readout template is invalid;
Confirmation code=0BH: addressing PageID is beyond the finger library;

To delete template DeletChar

Description: to delete a segment (N) of templates of Flash library started from the specified location (or PageID);
Input Parameter: PageID (template number in Flash), N (number of templates to be deleted)
Return Parameter: Confirmation code (1 byte)
Instuction code: 0cH
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes	2bytes	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Page number	number of templates to be deleted	Checksum
0xEF01	Xxxx	01H	07H	0cH	PageID	N	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	sum

Note: Confirmation code=00H: delete success;
Confirmation code=01H: error when receiving package;
Confirmation code=10H: faile to delete templates;

To empty finger library Empty

Description: to delete all the templates in the Flash library
Input Parameter: none
Return Parameter: Confirmation code (1 byte)
Instuction code: 0dH
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	Xxxx	01H	03H	0dH	0011H

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	Xxxx	07H	03H	xxH	sum

Note: Confirmation code=00H: empty success;
Confirmation code=01H: error when receiving package;

Confirmation code=11H: fail to clear finger library;

To carry out precise matching of two finger templates Match

Description: to carry out precise matching of templates from CharBuffer1 and CharBuffer2, providing matching results.

Input Parameter: none

Return Parameter: Confirmation code (1 byte)，matching score.

Instuction code: 03H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	Xxxx	01H	03H	03H	07H

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Matching score	Checksum
0xEF01	Xxxx	07H	05H	XxH	XxH	sum

Note 1: Confirmation code=00H: templates of the two buffers are matching!

Confirmation code=01H: error when receiving package;

Confirmation code=08H: templates of the two buffers aren't matching;

2: The instruction doesn't affect the contents of the buffers.

To search finger library Search

Description: to search the whole finger library for the template that matches the one in CharBuffer1 or CharBuffer2. When found, PageID will be returned.

Input Parameter: BufferID, StartPage (searching start address), PageNum（searching numbers）

Return Parameter: Confirmation code (1 byte), PageID (matching templates location）

Instuction code: 04H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1 byte	2 bytes	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	buffer number	Parameter	Parameter	Checksum
0xEF01	xxxx	01H	08H	04H	BufferID	StartPage	PageNum	sum

Note: BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values (except 1h, 2h) would be processed as CharBuffer2.

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes	2 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	页码	得分	Checksum
0xEF01	xxxx	07H	7	xxH	PageID	MatchScore	sum

Note 1: Confirmation code=00H: found the matching finer;

Confirmation code=01H: error when receiving package;
Confirmation code=09H: No matching in the library (both the PageID and matching score are 0);

2: The instruction doesn't affect the contents of the buffers.

Other instructions

To generate a random code GetRandomCode

Description: to command the Module to generate a random number and return it to upper computer;Refer to 4.8 for more about Random Number Generator;
Input Parameter: none
Return Parameter: Confirmation code (1 byte)
Instuction code: 14H
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Checksum
0xEF01	xxxx	01H	03H	14H	0018H

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	4 bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Random number	Checksum
0xEF01	xxxx	07H	07H	xxH	xxxx	sum

Note: Confirmation code=00H: generation success;
Confirmation code=01H: error when receiving package;

To write note pad WriteNotepad

Description: for upper computer to write data to the specified Flash page (refer to 4.1 for more about Note pad). Also see **ReadNotepad;**
Input Parameter: NotePageNum, user content (or data content)
Return Parameter: Confirmation code (1 byte)
Instuction code: 18H
Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1byte	32 bytes	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Page number	Data content	Checksum
0xEF01	xxxx	01H	36	18H	0~15	content	sum

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	Checksum
0xEF01	xxxx	07H	03H	xxH	sum

Note: Confirmation code=00H: write success;

Confirmation code=01H: error when receiving package;

To read note pad ReadNotepad

Description: to read the specified page's data content; Refer to 4.1 for more about user note pad. Also see **WriteNotepad**.

Input Parameter: none

Return Parameter: Confirmation code (1 byte) + data content

Instuction code: 19H

Command (or instruction) package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	1byte	2 bytes
Header	Module address	Package identifier	Package length	Instruction code	Page number	Checksum
0xEF01	xxxx	01H	04H	19H	0~15	xxH

Acknowledge package format:

2 bytes	4bytes	1 byte	2 bytes	1 byte	32bytes	2 bytes
Header	Module address	Package identifier	Package length	Confirmation code	User content	Checksum
0xEF01	xxxx	07H	3+32	xxH	User content	sum

Note: Confirmation code=00H: read success;

Confirmation code=01H: error when receiving package;

Instruction Table

Classified by functions

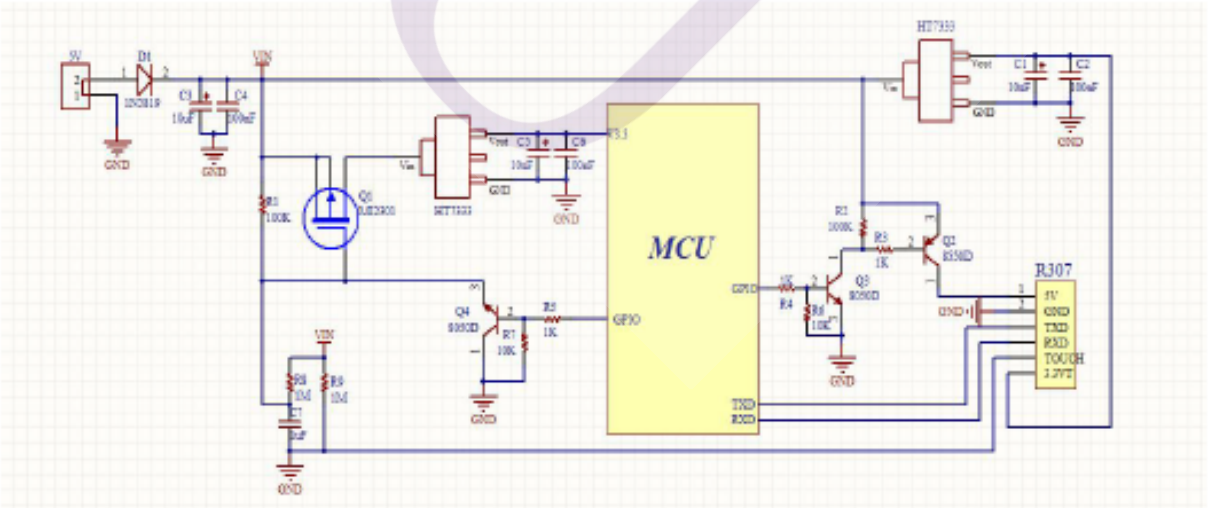
type	num	code	description	Type	num	Code	description
System-related	1	13H	To verify password	Fingerprint processing	13	08H	to upload template
	2	12H	To set password		14	09H	To download template
	3	15H	To set device address		15	06H	To store template;
	4	0EH	To set system Parameter		16	07H	to read/load template
	5	17H	Port control		17	0CH	to delete tempates
	6	0FH	To read system Parameter		18	0DH	to empty the library
	7	1DH	To read finger template numbers		19	03H	Carry out precise matching of two templates;
Fingerprint processing	8	01H	Collect finger image		20	04H	Search the finger library
	9	0AH	To upload image				
	10	0BH	To download image	others	21	14H	to get random code
	11	02H	To generate character file from image		22	18H	to write note pad
	12	05H	To combine character files and generate template		23	19H	To read note pad

GROW

Classified by instruction code

code	identifier	Description	Code	Identifier	Description
01H	GenImg	Collect finger image	0DH	Empty	to empty the library
02H	Img2Tz	To generate character file from image	0EH	SetSysPara	To set system Parameter
03H	Match	Carry out precise matching of two templates;	0FH	ReadSysPara	To read system Parameter
04H	Serach	Search the finger library	12H	SetPwd	To set password
05H	RegModel	To combine character files and generate template	13H	VfyPwd	To verify password
06H	Store	To store template;	14H	GetRandomCode	to get random code
07H	LoadChar	to read/load template	15H	SetAdder	To set device address
08H	UpChar	to upload template	17H	Control	Port control
09H	DownChr	to download template	18H	WriteNotepad	to write note pad
0AH	UpImage	To upload image	19H	ReadNotepad	To read note pad
0BH	DownImage	To download image	1BH	HiSpeedSearch	Search the library fastly
0CH	DeletChar	to delete tempates	1DH	TempleteNum	To read finger template numbers

II Reference Circuit



ภาคผนวก ข

แบบประเมินความพึงพอใจ

ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

แบบประเมินความพึงพอใจ

การใช้งาน ระบบยืนยันตัวบุคคลสำหรับ รับ-ส่ง หนังสือราชการชั้นความลับ

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบประเมิน

1. เพศ : ☐ หญิง ☐ ชาย
2. ชั้นยศ : ☐ นายทหารสัญญาบัตร ☐ นายทหารประทวน
3. ตำแหน่ง : ☐ ผู้บังคับบัญชา (ชั้นยศ พ.อ. ขึ้นไป) ☐ นายทหารคนสนิท

☐ เจ้าหน้าที่ธุรการ ☐ อื่นๆ

ตอนที่ 2 แบบสำรวจความพึงพอใจ

คำชี้แจง ระดับความพึงพอใจ ทำเครื่องหมาย ✓ ลงในช่องระดับความพึงพอใจ

ระดับคะแนน 5 = มากที่สุด, 4 = มาก, 3 = ปานกลาง, 2 = น้อย และ 1 = น้อยที่สุด

หัวข้อการประเมิน	ความพึงพอใจ				
	5	4	3	2	1
1. ด้านการใช้งานระบบงาน					
1.1 ความสะดวกสบายในการรับ-ส่ง หนังสือราชการชั้นความลับ					
1.2 ความรวดเร็วในการรับ-ส่ง หนังสือราชการชั้นความลับ					
1.3 การใช้งานของระบบงานไม่ซับซ้อน มีความเข้าใจง่าย					
1.4 ความเหมาะสมของบุคคลในการเข้าถึงข้อมูลชั้นความลับ					
1.5 ความเหมาะสมในการนำอุปกรณ์ Fingerprint sensor เข้ามายืนยันตัวบุคคล					
1.6 ความเหมาะสมของระบบงาน					
1.7 ความเร็วในการยืนยันตัวบุคคล					
1.8 ความถูกต้องในการยืนยันตัวบุคคล					
1.9 ระบบงานนี้สามารถรักษาหนังสือราชการชั้นความลับได้มากน้อยเพียงใด					
1.10 ความปลอดภัยของข้อมูลชั้นความลับ					
1.11 ความน่าเชื่อถือของระบบงานในการรักษาหนังสือราชการชั้นความลับ					
1.12 ความน่าสนใจในการนำระบบงานมาประยุกต์ใช้งานจริง					

หัวข้อการประเมิน	ความพึงพอใจ				
	5	4	3	2	1
2. ด้านตัวอุปกรณ์ Fingerprint					
1.1 ความปลอดภัยในการใช้งาน					
1.2 ความสะดวกสบายในการใช้งาน					
1.3 อุปกรณ์สามารถยืนยันตัวบุคคลได้					
1.4 ขนาดของอุปกรณ์ Fingerprint sensor มีความเหมาะสม					
1.5 ความแข็งแรงของอุปกรณ์					
1.6 ความง่ายในการใช้งานอุปกรณ์ Fingerprint sensor					

ข้อเสนอแนะ

.....

.....

.....

.....

ประวัติผู้เขียน

ชื่อ – นามสกุล	เรืออากาศโทหญิง ชนิดา รูปเลิศ
ประวัติการศึกษา	วิทยาศาสตร์บัณฑิต
	สาขาวิทยาการคอมพิวเตอร์
	คณะวิทยาศาสตร์
	มหาวิทยาลัยราชภัฏจันทรเกษม
	ปีที่สำเร็จการศึกษา พ.ศ.2555
ตำแหน่งและสถานที่ทำงานปัจจุบัน	ประจำแผนกิจการอวกาศ
	กองนโยบายและแผน ศูนย์กิจการอวกาศ
	กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม