ระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID

โดย

วัชรินทร์ วรินทักษะ

สนับสนุนงบประมาณโดย

มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

ประจำปีงบประมาณ 2567

Centralized electronic service system through digital identity verification and authentication system DOPA-Digital ID

By

Watcharin Warinthaksa

Granted by

Rajamangala University of Technology Rattanakosin

Fiscal year 2024

กิตติกรรมประกาศ

งานวิจัยเรื่องระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID ได้จัดทำขึ้นเพื่อพัฒนาระบบเพื่อสนับสนุนกิจกรรมการดำเนินงานภายในมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์โดยมีวัตถุประสงค์เพื่อเป็นส่วนหนึ่งในการก้าวเข้าสู่การเป็นมหาวิทยาลัยดิจิทัล และเป็นการยกระดับคุณภาพการให้บริการในมหาวิทยาลัยแก่บุคลากร นักศึกษา และผู้มีส่วนได้ส่วนเสียให้ได้รับบริการที่สะดวก รวดเร็ว และปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ต่าง ๆ

ขอขอบคุณบุคลากร และผู้บริหารของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตโกสินทร์ รวมทั้งผู้เข้ารับบริการ ที่ได้ให้ความร่วมมือในการทดสอบและใช้งานระบบจนทำให้สามารถพัฒนาให้เป็นไปตามความต้องการของผู้ใช้งานได้

ขอขอบคุณสถาบันวิจัยและพัฒนา มหาวิทยาลัยเทคโนโลยีราชมงคลรัตโกสินทร์ ผู้ให้การสนับสนุนทุนการทำวิจัย ส่งเสริม และเล็งเห็นคุณค่าของงานวิจัยที่จะช่วยให้เกิดงานวิจัยใหม่ ๆ เพิ่มขึ้นในอนาคต

วัชรินทร์ วรินทักษะ

30 กันยายน 2567

บทคัดย่อ

รหัสโครงการ : c48 / 2567

ชื่อโครงการ : ระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA-Digital ID

ชื่อนักวิจัย : วัชรินทร์ วรินทักษะ

งานวิจัยเรื่องระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID มีวัตถุประสงค์เพื่อสร้างระบบพิสูจน์ตัวตนที่มีความปลอดภัยตามมาตรฐานสากลและเพื่อให้ผู้ใช้บริการสามารถดำเนินการธุรกรรมอิเล็กทรอนิกส์ต่าง ๆ ภายในมหาวิทยาลัยได้อย่างมีประสิทธิภาพ

ผู้วิจัยได้นำ Laravel framework ทำการพัฒนาทั้งระบบ โดยนำ ThaiD ทำการพัฒนาระบบพิสูจน์ตัวตนโดยใช้ข้อมูลจาก ThaiD ของผู้ใช้ในระบบมาทำการพิสูจน์ตัวตนผ่าน Active Directory ให้รองรับมาตรฐาน OAuth 2.0 จากนั้นจึงนำระบบมาใช้งานและศึกษาประสิทธิภาพโดยวัดจากความพึงพอใจของผู้ใช้งานในระบบ

ผลการวิจัยพบว่าความพึงพอใจของผู้ใช้บริการระบบทางด้านการพัฒนาระบบที่มีต่อระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID ได้คะแนนเฉลี่ย 4.36 แปลผลได้ว่าระบบมีประสิทธิภาพดี มีความเหมาะสมในการนำมาให้บริการในมหาวิทยาลัยได้เป็นอย่างดี

คำสำคัญ : การพิสูจน์ตัวตน ดิจิทัลไอดี OAuth

E-mail Address : watcharin.w@rmutr.ac.th

ระยะเวลาโครงการ : ตุลาคม พ.ศ. 2567- พฤศจิกายน พ.ศ. 2568

Abstract

Code of project : c48 / 2024

Project name : Centralized electronic service system through digital identity verification and authentication system DOPA-Digital ID

Researcher name : Watcharin Warinthaksa

The research on the centralized electronic service system through the digital authentication and verification system DOPA -Digital ID aims to create an authentication system that is secure according to international standards and to enable users to efficiently conduct various electronic transactions within the university

The researcher has used the Laravel framework to develop the entire system. ThaiD was used to develop an authentication system using ThaiD data from users in the system to authenticate through Active Directory to support the OAuth 2.0 standard. The system was then implemented and its efficiency was studied by measuring user satisfaction in the system.

The research results found that the satisfaction of users of the system development service with the DOPA-Digital ID digital identity verification and authentication system received an average score of 4.36, which can be interpreted as the system being efficient and suitable for use in universities.

Keywords: Authentication Digital ID OAuth

E-mail Address : **watcharin.w@rmutr.ac.th**

Period of project : October 2024 - November 2025

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันองค์กรต่าง ๆ ทั้งภาครัฐและเอกชน ต่างมีบทบาทในการให้บริการผ่านระบบอิล็กทรอนิกส์เพื่อให้องค์กรมีศักยภาพในการทำงานและการให้บริการที่มีประสิทธิภาพเพิ่มมากขึ้น ซึ่งมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ก็เป็นหน่วยงานหนึ่งที่มีการพัฒนาเทคโนโลยสารสนเทศดิจิทัลในทุกด้าน

ระบบสารสนเทศภายในมหาวิทยาลัยฯ มีการพิสูจน์ตัวตน (Authentication) ผ่านการ Login ด้วย username และ password โดยที่ 1 ระบบจะมีการใช้งาน 1 username ซึ่งอาจจะใช้เหมือนกันหรือแตกต่างกันออกไปนั้น ขึ้นอยู่กับการจัดสิทธิ์และการจัดการของระบบนั้น ๆ จึงทำให้ผู้ใช้งาน เกิดความสับสน เกิดความผิดพลาดจากการจดจำในการใช้งาน บางครั้งผู้ใช้จึงมีความจำเป็นในการจดลงเอกสารเพื่อประกอบการจดจำ ซึ่งทำให้เกิดความไม่ปลอดภัย อาจจะทำให้เกิดการโจรกรรมข้อมูลผู้ใช้ได้

ต่อมีมหาวิทยาลัยฯ ได้นำบริการจัดเก็บบัญชีรายชื่อผู้ใช้ หรือ Active Directory (AD) [1] เพื่อแก้ไขปัญหาเรื่อง “1 ระบบ 1 username” ที่ทำให้เกิดความสับสนการใช้งาน แต่ก็ยังคงพบปัญหา เมื่อมีระบบสารสนเทศจากหน่วยงานภายนอกได้ทำพัฒนาระบบสารสนเทศขึ้นมา ได้มีการเข้าใช้ Active Directory เป็นศูนย์กลางใน Authentication แต่ก็ยังพบปัญหาในการ “ดักเก็บ username password” ทำให้เกิดความไม่ปลอดภัยในการออกแบบระบบ ไม่เป็นไปตามคำแนะนำของหลักการ Open Web Application Security Project (OWASP) [2]

ผู้วิจัยได้เล่งเห็นถึงปัญหาด้านความปลอดภัยดังกล่าว ประกอบกับกฎหมาย PDPA (Personal Data Protection Act) [3] พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลปี 2562 ได้ทำการศึกษา ค้นคว้าและพัฒนา ThaID (ไทยดี) [4] แอปพลิเคชันที่ กรมการปกครอง กระทรวงมหาดไทย พัฒนาขึ้นเพื่อตอบสนองนโยบายรัฐบาลดิจิตอล แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ปี พ.ศ.2566-2570 [5] เพื่อใช้ในการพิสูจน์และยืนยันตัวตน (Digital ID) รวมถึงการเปรียบเทียบภาพใบหน้า (Face Verification System) ทางดิจิทัล เมื่อผู้ใช้เข้าไปใช้บริการจากทางภาครัฐหรือภาคเอกชนที่จำเป็นต้องมีการยืนยันตัวตน ก็สามารถเข้าสู่ระบบแอปพลิเคชัน ThaID เพื่อยืนยันตัวตน อีกทั้งยังสามารถนำมาประยุกต์ใช้กับ Active Directory [1] , [6] เพื่อเสริมสร้างความปลอดภัย ผ่านมาตรฐาน OAuth 2.0 [6] , [7] เป็น Industry-standard protocol มาตรฐาน RFC6749 [8] ใช้สำหรับการทำ Authorization

Framework เปิดให้ Third-party Applications ได้รับสิทธิ์การเข้าถึง [9] ทำให้หน่วยงานภายนอกที่ได้ทำพัฒนาระบบสารสนเทศ ไม่ทราบข้อมูลในส่วนของ username password เมื่อผู้ใช้งานระบบสารสนเทศจะได้รับการยืนยันตัวตนและมีการยินยอมผ่าน ThaiD สำเร็จ ผู้พัฒนาระบบสารสนเทศจะได้ข้อมูลที่มีความจำเป็นกับระบบสารสนเทศเท่านั้น หลังจากนั้น ThaiD จะทำการ Authentication ผ่านไปยัง Active Directory (AD) เพื่อใช้งานระบบสารสนเทศอย่างปลอดภัยและผ่านมาตรตามสากลที่ได้รับการยอมรับ [10] , [11] หลังจากที่มีการพัฒนาสำเร็จเสร็จสิ้นแล้ว จะมีการจัดทำแนวปฏิบัติหรือประกาศให้ระบบสารสนเทศฯ เพื่อเกิดประโยชน์สูงสุดต่อมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์นำไปใช้งานต่อไป

2. วัตถุประสงค์การวิจัย

2.1.1 เพื่อสร้างระบบพิสูจน์ตัวตนที่มีความปลอดภัยตามมาตรฐานสากล

2.1.2 เพื่อให้ผู้ใช้บริการสามารถดำเนินการธุรกรรมอิเล็กทรอนิกส์ต่าง ๆ ภายในมหาวิทยาลัยได้อย่างมีประสิทธิภาพ

2.1.3 เพื่อตอบรับนโยบายของรัฐบาลในเรื่องรัฐบาลดิจิทัล ตามแผนพัฒนารัฐบาลดิจิทัลของประเทศไทยปี พ.ศ.2566-2570

3. คำถามการวิจัย / สมมติฐานการวิจัย

ผู้ใช้บริการระบบให้บริการอิเล็กทรอนิกส์ของมหาวิทยาลัยได้รับความสะดวกในการใช้บริการอย่างมีประสิทธิภาพและมีความพึงพอใจกับระบบให้บริการในระดับมาก

4. ขอบเขตการวิจัย

งานวิจัยนี้จะใช้ประชากรเป็นบุคลากรและนักศึกษาที่เป็นผู้ใช้งานระบบพิสูจน์ตัวตนของมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์

5. นิยามศัพท์

ThaiD หมายถึง แอปพลิเคชันที่ กรมการปกครอง กระทรวงมหาดไทย พัฒนาขึ้นเพื่อใช้ในการพิสูจน์และยืนยันตัวตน (Digital ID) รวมถึงการเปรียบเทียบภาพใบหน้า (Face Verification System) ทางดิจิทัล เมื่อประชาชนเข้าไปใช้บริการจากทางภาครัฐหรือภาคเอกชนที่จำเป็นต้องมีการยืนยันตัวตน ก็สามารถเข้าสู่ระบบแอปพลิเคชัน ThaID เพื่อยืนยันตัวตนได้เลย โดยไม่ต้องกรอกข้อมูล

ให้เสียเวลา ถือเป็นการสร้างมิติใหม่ของการทำธุรกรรมผ่านช่องทางดิจิทัล ที่มีความสะดวก รวดเร็ว และปลอดภัยมากยิ่งขึ้น

Oauth (Open Authorization) คือ โปรโตคอลมาตรฐานเปิดสำหรับการอนุญาต ที่ช่วยให้แอปพลิเคชันหรือบริการหนึ่งได้รับอนุญาตให้เข้าถึงข้อมูลของผู้ใช้ในอีกบริการหนึ่งได้อย่างจำกัด โดยที่ผู้ใช้ไม่ต้องเปิดเผยรหัสผ่านจริงให้กับแอปพลิเคชัน

บทที่ 2
ทบทวนวรรณกรรมที่เกี่ยวข้อง / ทฤษฎีที่เกี่ยวข้อง

ในการพัฒนาระบบระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID มีการศึกษาวรรณกรรมที่เกี่ยวข้องในด้านต่าง ๆ ดังนี้

- การพิสูจน์ตัวตน (Authentication)
- วิธีการพัฒนาระบบด้วย SDLC
- OAuth (Open Authorization)
- เครื่องมือเครื่องใช้ในการพัฒนา

2.1 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)

- การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ซึ่งหลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด คือ

1) Actual identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

2) Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้

2.1.1 ประเภทของการพิสูจน์ตัวตน (Authentication Types)

2.1.1.1 การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords) รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ แต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

2.1.1.2 การพิสูจน์ตัวตนโดยใช้ PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

2.1.1.3 การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้างรหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password) ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัส และ อะซิงโครนัส

1) การพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ

- การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication) เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกด Token เพื่อให้ Token สร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกด Token ใส่ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเครื่องแม่ข่ายก่อน ว่ารหัสผ่านที่ใส่มีอยู่ในเครื่องแม่ข่ายจริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบ

- การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุก ๆ หนึ่งนาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการ

ตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเครื่องแม่ข่ายว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเครื่องแม่ข่ายจริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ

2) การพิสูจน์ตัวตนแบบอะซิงโครนัส (Asynchronous) หรือเรียกอีกอย่างหนึ่งว่า "challenge-response" ถูกพัฒนาขึ้น เป็นลำดับแรกๆ ของระบบการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้" ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้ต้องการจะเข้าสู่ระบบ ผู้ใช้จะต้องทำการร้องของไปยังเครื่องแม่ข่าย จากนั้นก็จะส่ง challenge string มาให้ผู้ใช้ เพื่อให้ผู้ใช้ใส่ลงใน Token ที่ผู้ใช้ถืออยู่ จากนั้น Token จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้ ผู้ใช้จึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้

2.1.1.4 การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits)

ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน

2.1.1.5 การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP)

One-Time Password ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำ ๆ กัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ

การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเครื่องแม่ข่ายจากนั้นเครื่องแม่ข่ายจะส่ง challenge string กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ challenge string และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเครื่องแม่ข่าย แล้วจะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เครื่องแม่ข่ายเองคำนวณได้ โดยเครื่องแม่ข่ายก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

2.1.1.6 การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)

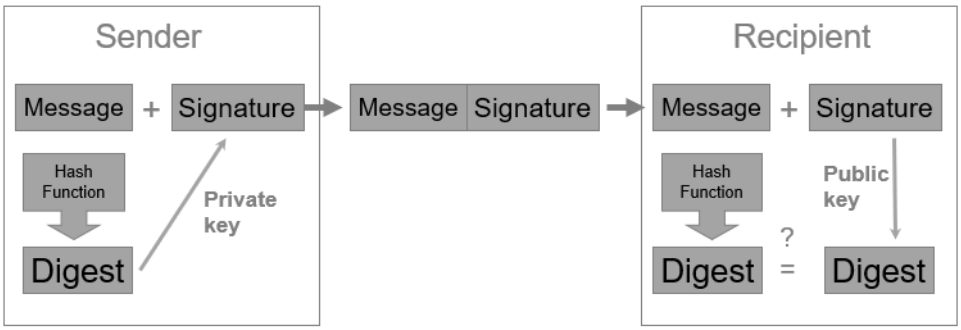
การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

1) เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชันทางคณิตศาสตร์ที่เรียกว่าแฮชฟังก์ชัน(Hash) ได้เมสเซจไดเจสต์ (Message Digest) ออกมา

2) การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

3) การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่าน Hash เพื่อคำนวณหาค่า Message Digest และถอดรหัสลายเซ็นอิเล็กทรอนิกส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูล Message Digest ที่ได้จากการถอดรหัสเท่ากันกับค่าในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง

ลายเซ็นอิเล็กทรอนิกส์นิยมนำไปใช้ในระบบรักษาความปลอดภัยในการชำระเงินผ่านระบบออนไลน์ ซึ่งในปัจจุบันนี้การทำธุรกรรมการเงินอิเล็กทรอนิกส์ได้รับความนิยมเป็นอย่างมาก



ภาพที่ 1 แสดงการวิธีการทำงานของลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)

2.1.1.7 โพรโทคอลในการพิสูจน์ตัวตน

ในระบบเครือข่ายแบบเปิดหรืออินเทอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโทคอลในการพิสูจน์ตัวตน คือโพรโทคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโทคอล ตัวอย่างของโพรโทคอลในการพิสูจน์ตัวตนได้แก่

- Secure Socket Layer (SSL) คือ โปรโตคอลรักษาความปลอดภัยอินเทอร์เน็ตที่ใช้การเข้ารหัสข้อมูลระหว่างเซิร์ฟเวอร์และเบราว์เซอร์ เพื่อป้องกันการดักฟังหรือขโมยข้อมูลสำคัญ เช่น ข้อมูลส่วนตัวและข้อมูลการเงิน แม้ว่า SSL จะถูกแทนที่ด้วย Transport Layer Security (TLS) ซึ่งเป็นเวอร์ชันที่พัฒนาขึ้นแล้ว แต่คำว่า "SSL" ยังคงถูกใช้เรียกเทคโนโลยีนี้โดยทั่วไป และเว็บไซต์ที่ใช้ SSL/TLS จะแสดง "HTTPS" ใน URL แทน "HTTP" เพื่อบ่งบอกถึงความปลอดภัยของเว็บไซต์

- Internet Security (IPSEC) ชุดโปรโตคอลที่ใช้เพิ่มความปลอดภัยให้กับเครือข่าย Internet Protocol (IP) โดยการเข้ารหัสและยืนยันตัวตนของข้อมูลที่ส่งผ่านเครือข่าย ทำให้มั่นใจว่าข้อมูลจะปลอดภัยและไม่ถูกแก้ไขหรือแอบอ้างระหว่างทาง. IPSec มักถูกใช้ในการสร้างอุโมงค์ในเครือข่ายส่วนตัวเสมือน (VPN) เพื่อสร้างช่องทางที่ปลอดภัยในการสื่อสารผ่านเครือข่ายสาธารณะอย่างอินเทอร์เน็ต.

- Kerberos คือ โปรโตคอลการตรวจสอบสิทธิ์เครือข่าย ที่ช่วยให้ผู้ใช้และเซิร์ฟเวอร์บนเครือข่ายพิสูจน์ตัวตนซึ่งกันและกันได้อย่างปลอดภัย โดยไม่ต้องส่งรหัสผ่านผ่านเครือข่าย Kerberos ใช้ ระบบตั๋ว (tickets) ที่เข้ารหัสไว้ ซึ่งออกโดย บุคคลที่สามที่เชื่อถือได้ หรือที่เรียกว่า Key Distribution Center (KDC) เพื่อให้แน่ใจว่าการสื่อสารมีความปลอดภัยและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต Kerberos เป็นโปรโตคอลการตรวจสอบสิทธิ์เริ่มต้นสำหรับโดเมน Windows มาตั้งแต่ปี 2000 และรองรับในระบบปฏิบัติการหลักๆ เช่น macOS, Linux และ Unix

2.2 วิธีการพัฒนาระบบด้วย SDLC

ในการพัฒนาระบบสารสนเทศสำหรับศูนย์ฝึกอบรม ได้ถูกออกแบบตามวงจรการพัฒนาระบบงาน (System Development Life Cycle : SDLC) ซึ่งระเบียบวิธีในการวิเคราะห์และออกแบบงานแบบวงจรการพัฒนาระบบมีการพัฒนาเป็น 7 ขั้นตอน ดังนี้

ภาพที่ 2 แสดงวงจรการพัฒนาระบบ (SDLC)

2.2.1 การนิยามปัญหา (Problem Definition)

การกำหนดปัญหาเป็นขั้นตอนของการกำหนดขอบเขตของปัญหา สาเหตุของปัญหาจากการดำเนินงานในปัจจุบันความเป็นไปได้ในการสร้างระบบใหม่ การกำหนดความต้องการ (Requirement) ระหว่างนักวิเคราะห์ระบบกับผู้ใช้งาน โดยข้อมูลเหล่านี้ได้จากการสัมภาษณ์ การรวบรวมข้อมูลจากการดำเนินงานต่างๆ เพื่อทำการสรุปเป็นข้อกำหนด (Requirement Specification) ที่ชัดเจน

2.2.2 การวิเคราะห์ระบบงาน (Analysis)

เป็นขั้นตอนที่ทำการศึกษาถึงระบบงานปัจจุบัน โดยการนำสรุปความต้องการของผู้ใช้ที่ได้มาจากขั้นตอนแรกมาวิเคราะห์ในรายละเอียดเพื่อทำการพัฒนาเป็นแบบจำลอง ลอจิคัล (Logical Model) ซึ่งประกอบด้วย แผนภาพกระแสข้อมูล (Data Flow Diagram) แผนภาพแสดงความสัมพันธ์ระหว่างข้อมูล (ER-Diagram) เป็นต้น

2.2.3 การออกแบบระบบงาน (Design)

การออกแบบเป็นขั้นตอนของการนำผลลัพธ์ที่ได้จากการวิเคราะห์ทางตรรกะมาพัฒนาเป็น Physical Model ให้สอดคล้องกันโดยการออกแบบจะเริ่มจากส่วนของอุปกรณ์และเทคโนโลยีต่างๆ และโปรแกรมคอมพิวเตอร์ที่นำมาพัฒนา การออกแบบจำลองข้อมูล การออกแบบรายงาน และการออกแบบส่วนติดต่อกับผู้ใช้งาน การจัดทำพจนานุกรมข้อมูล

2.2.4. การพัฒนาระบบงาน (Development)

ขั้นตอนนี้เป็นขั้นตอนการพัฒนาโปรแกรมด้วยการสร้างชุดคำสั่งหรือ เขียนโปรแกรมเพื่อการสร้างระบบงาน โดยโปรแกรมที่ใช้ในการพัฒนาจะต้องพิจารณาถึงความเหมาะสมกับเทคโนโลยีที่ใช้งานอยู่และพัฒนาต่อได้ง่าย

2.2.5 การทดสอบระบบ (Testing)

การทดสอบระบบงานเป็นขั้นตอนในการตรวจสอบระบบก่อนนำไปใช้ปฏิบัติงานจริง โดยการตรวจสอบระบบนี้จะทำใน 2 ส่วนด้วยกันคือ การตรวจสอบรูปแบบไวยากรณ์ภาษาเขียน (Syntax) และการตรวจสอบวัตถุประสงค์ของงานว่าตรงกับความต้องการหรือไม่

2.2.6 การติดตั้ง (Implementation)

ขั้นตอนต่อมาหลังจากได้ทำการทดสอบจนมีความมั่นใจแล้วว่าระบบสามารถทำงานได้จริงและตรงกับความต้องการของผู้ใช้ระบบ จากนั้นจึงดำเนินการติดตั้งระบบเพื่อใช้งานจริงต่อไป ซึ่งประกอบด้วยการเตรียมอุปกรณ์ฮาร์ดแวร์อุปกรณ์ทางการสื่อสารและเครือข่ายให้พร้อม หลังจากนั้นจึงลงระบบปฏิบัติการและโปรแกรมที่พัฒนาขึ้นใหม่จึงสามารถนำระบบไปใช้งานได้

2.2.7 การบำรุงรักษา (Maintenance)

การบำรุงรักษาเป็นขั้นตอนการปรับปรุงแก้ไขระบบหลังจากได้มีการติดตั้งและใช้งานแล้ว ในขั้นตอนนี้อาจเกิดจากปัญหาของโปรแกรมหรือมีความต้องการของผู้ใช้ในการทำงานด้านอื่น ๆ เพิ่มขึ้นก็สามารถพัฒนาเพิ่มได้ ซึ่งในการบำรุงรักษานี้หมายความรวมถึงการบำรุงรักษาทั้งด้านซอฟท์แวร์และฮาร์ดแวร์ด้วย

2.3. OAuth

OAuth (Open Authorization) คือ โปรโตคอลมาตรฐานเปิดสำหรับการอนุญาต ที่ช่วยให้แอปพลิเคชันหรือบริการหนึ่งได้รับอนุญาตให้เข้าถึงข้อมูลของผู้ใช้ในอีกบริการหนึ่งได้อย่างจำกัด โดยที่ผู้ใช้ไม่ต้องเปิดเผยรหัสผ่านจริงให้กับแอปพลิเคชันนั้น. OAuth มอบประสบการณ์ที่สะดวกสบายและปลอดภัยยิ่งขึ้น โดยผู้ใช้สามารถกำหนดได้ว่าต้องการให้แอปพลิเคชันนั้นเข้าถึงข้อมูลใดได้บ้างแทนที่จะให้สิทธิ์เข้าถึงบัญชีทั้งหมด.

การทำงานของ OAuth นั้น ผู้ใช้ (Resource Owner) เป็นเจ้าของข้อมูล ส่วนแอปพลิเคชันจะเป็นผู้ขอใช้ (Client) โดยแอปพลิเคชันที่ต้องการเข้าถึงข้อมูลของคุณ (เช่น Canva ที่ต้องการเข้าถึง Google account ของผู้ใช้ เซิร์ฟเวอร์ผู้ให้บริการข้อมูล (Authorization Server/Resource Server): บริการที่คุณมีบัญชีอยู่ (เช่น Google, Facebook).

ขั้นตอนพื้นฐาน

1. การขอสิทธิ์: แอปพลิเคชัน (Client) ต้องการเข้าถึงข้อมูลของคุณ จึงขออนุญาตไปยังเซิร์ฟเวอร์ผู้ให้บริการข้อมูล (Authorization Server).

2. การยินยอม: ผู้ใช้ (Resource Owner) ได้รับการแจ้งเตือน และเลือกว่าจะอนุญาตให้แอปพลิเคชันเข้าถึงข้อมูลส่วนไหนได้บ้าง.

3. การออกโทเค็น (Access Token): หากผู้ใช้ยินยอม เซิร์ฟเวอร์ผู้ให้บริการจะออก "โทเค็น" ให้กับแอปพลิเคชัน.

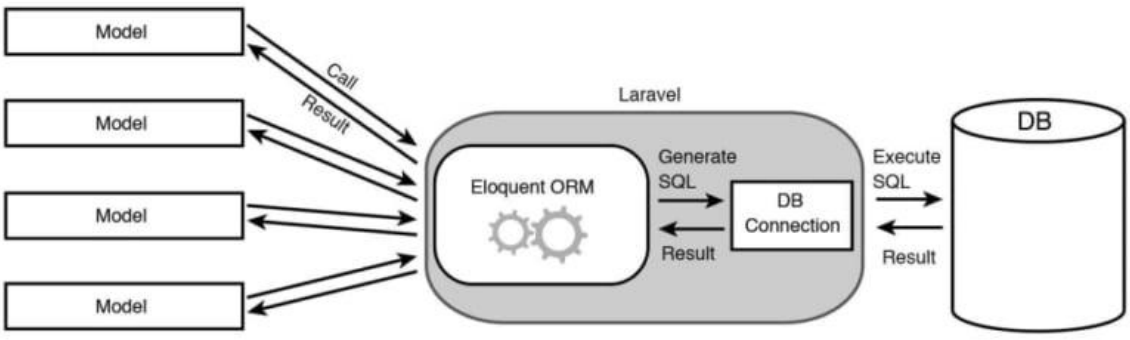
4.การเข้าถึงข้อมูล:แอปพลิเคชันใช้โทเค็นนี้เพื่อเข้าถึงข้อมูลที่ผู้ใช้ได้อนุญาตไว้ในบริการของผู้ให้บริการ โดยไม่ต้องใช้รหัสผ่านของผู้ใช้เลย

OAuth ช่วยเพิ่มความปลอดภัย โดยเฉพาะอย่างยิ่ง ข้อมูลประจำตัว (รหัสผ่าน) ของผู้ใช้จะไม่ถูกเปิดเผยให้กับแอปพลิเคชันภายนอก ทำให้ปลอดภัยมากขึ้นหากแอปนั้นถูกละเมิด และยังมีความสะดวกกับผู้ดูและระบบและผู้ใช้โดยที่ไม่ต้องสร้างบัญชีใหม่ในทุกๆ แอปพลิเคชัน เพียงแค่ใช้บัญชีที่มีอยู่แล้ว (เช่น "ลงชื่อเข้าใช้ด้วย Google") นอกจากนี้ในการควบคุมข้อมูลนั้น ผู้ใช้สามารถกำหนดขอบเขตการเข้าถึงข้อมูลได้อย่างละเอียด ทำให้รู้ว่าแอปพลิเคชันสามารถทำอะไรได้บ้าง

4. เครื่องมือเครื่องใช้ในการพัฒนา

4.1 Laravel Framework

Laravel Framework คือ เฟรมเวิร์ก (Framework) ภาษา PHP แบบโอเพนซอร์สฟรี ที่ใช้สำหรับพัฒนาเว็บแอปพลิเคชัน โดยมีเป้าหมายเพื่อให้การพัฒนาเว็บทำได้ง่าย รวดเร็ว และเป็นระบบมากขึ้น ผ่านการใช้งานสถาปัตยกรรม Model-View-Controller (MVC), เครื่องมืออย่าง Artisan CLI, การจัดการฐานข้อมูลด้วย Eloquent ORM, และระบบจัดการการรับส่งข้อมูลที่เรียกว่า Inversion of Control (IoC) Container.



ภาพที่ 3 Laravel Framework

วัตถุประสงค์หลักของ Laravel คือ ทำให้การพัฒนาเว็บง่ายและสนุก มุ่งเน้นการลดความซับซ้อนของงานที่ใช้บ่อย เช่น การจัดการสิทธิ์, การกำหนดเส้นทาง (routing), การจัดการเซสชัน, และการแคช ทำให้เหล่านักพัฒนาสามารถโฟกัสกับส่วนที่สร้างสรรค์และสำคัญของแอปพลิเคชันได้มากขึ้น สร้างเว็บแอปพลิเคชันที่ปรับขนาดได้ เฟรมเวิร์กนี้มอบเครื่องมือและทรัพยากรที่จำเป็นในการสร้างเว็บแอปพลิเคชันที่มีประสิทธิภาพและสามารถรองรับการขยายตัวในอนาคตได้ดี คุณสมบัติเด่น

สถาปัตยกรรม MVC ช่วยแบ่งโครงสร้างของแอปพลิเคชันออกเป็น 3 ส่วน คือ Model (จัดการข้อมูล), View (ส่วนแสดงผล), และ Controller (จัดการตรรกะ) ทำให้โค้ดเป็นระเบียบและดูแลรักษาง่าย นอกจากนี้จังมีส่วนสำคัญที่ช่วยในการพัฒนาระบบให้ง่ายและรวดเร็วขึ้นดังนี้

- Artisan CLI คือ ชุดคำสั่งบนบรรทัดคำสั่งที่ช่วยในการสร้างฐานข้อมูล, จัดการไฟล์, และดำเนินการต่างๆ ในโปรเจกต์ได้ง่าย

- Eloquent ORM คือ เครื่องมือช่วยในการเข้าถึงฐานข้อมูลได้อย่างง่ายดาย โดยเขียนโค้ดในภาษา PHP แทนการเขียน SQL โดยตรง

- Blade Templating คือ ระบบเทมเพลตที่ทำให้การสร้างโค้ด HTML ทำได้ง่ายขึ้น โดยอนุญาตให้นักพัฒนาแบ่งส่วนประกอบต่างๆ เช่น Header, Footer แล้วนำมาประกอบกันในภายหลังได้

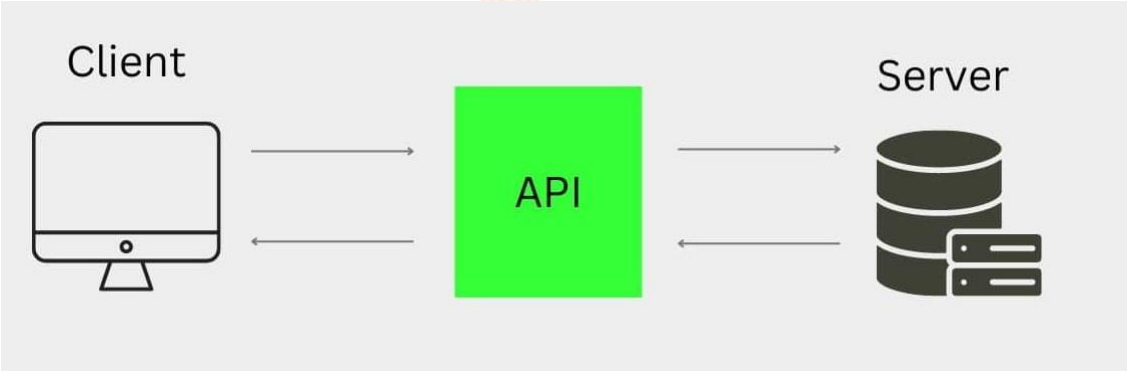
- ระบบยืนยันตัวตน (Authentication) มีความสามารถสำเร็จรูปสำหรับระบบการลงทะเบียนและเข้าสู่ระบบ

- Inversion of Control (IoC) Container คือ ระบบที่ช่วยจัดการการพึ่งพากันระหว่างคลาสต่าง ๆ ทำให้โค้ดสะอาดและจัดการได้ง่ายขึ้น

4.2 API

API (Application Programming Interface) คือส่วนต่อประสานโปรแกรมประยุกต์ เป็นชุดคำสั่ง กฎ และโปรโตคอลที่ทำหน้าที่เป็นตัวกลางให้ซอฟต์แวร์หรือระบบต่าง ๆ สามารถสื่อสาร แลกเปลี่ยนข้อมูล และทำงานร่วมกันได้อย่างเป็นระบบ โดยนักพัฒนาไม่ต้องรู้รายละเอียดการทำงาน

ภายในของอีกระบบ เพียงแต่ส่งคำขอผ่าน API และรับการตอบกลับมา เปรียบเสมือนบริกรที่รับคำสั่งจากลูกค้า (ผู้ใช้บริการ) ไปยังครัว (ผู้ให้บริการ) และนำอาหาร (ข้อมูล) กลับมาให้ลูกค้า



ภาพที่ 4 การทำงานของ API

หลักการทำงานพื้นฐานของ API คือ คำขอและการตอบกลับ (Request-Response) เมื่อแอปพลิเคชันต้องการข้อมูล จะส่งคำขอ (Request) ไปยัง API จากนั้น API จะส่งคำขอไปยังระบบที่ให้บริการ และส่งข้อมูลที่ร้องขอ (Response) กลับมายังแอปพลิเคชัน

การเชื่อมต่อ API เป็นสะพานเชื่อมที่ทำให้แอปพลิเคชันต่างๆ สามารถทำงานร่วมกันได้ เช่น แอปพลิเคชันสั่งอาหารที่เรียกใช้ API ของ Google Maps เพื่อแสดงแผนที่ร้านอาหาร นอกจากนี้การเชื่อต่อที่มีความปลอดภัย API ช่วยให้นักพัฒนาสามารถเข้าถึงข้อมูลหรือฟังก์ชันของระบบอื่นได้อย่างปลอดภัย โดยกำหนดสิทธิ์การเข้าถึงและรูปแบบการสื่อสารที่ชัดเจน

4.3 OWASP

OWASP (Open Worldwide Application Security Project) คือองค์กรไม่แสวงหาผลกำไรที่มุ่งเน้นการสร้างซอฟต์แวร์ที่ปลอดภัยและเชื่อถือได้ ผ่านการเป็นชุมชนเปิดระดับโลกในการให้ความรู้ เครื่องมือ และการทำงานร่วมกัน เพื่อช่วยองค์กรต่าง ๆ ในการออกแบบ พัฒนา จัดการ และบำรุงรักษาแอปพลิเคชันที่ปลอดภัย OWASP มีทรัพยากรฟรีมากมาย เช่น โครงการซอฟต์แวร์โอเพนซอร์ส เอกสาร แนวทางปฏิบัติที่ดีที่สุด และรายงานที่รู้จักกันอย่าง OWASP Top 10 ซึ่งรวบรวมความเสี่ยงด้านความปลอดภัยที่พบบ่อยในแอปพลิเคชันเว็บ

พันธกิจหลักในการส่งเสริมความปลอดภัยของซอฟต์แวร์ OWASP นั้นมีเป้าหมายเพื่อช่วยเหลือองค์กร นักพัฒนา และผู้เชี่ยวชาญด้านความปลอดภัยในการปกป้องเว็บแอปพลิเคชันจากการโจมตีทางไซเบอร์ ให้สามารถใช้ทรัพยากรได้ฟรี โดยองค์กรจัดเตรียมแหล่งข้อมูลฟรีที่เข้าถึงได้ง่าย เพื่อให้ทุกคนสามารถปรับปรุงความปลอดภัยของแอปพลิเคชันตนเองได้ และยังสร้างชุมชนสำหรับเป็นเวทีที่ผู้เชี่ยวชาญด้านความปลอดภัยและเทคโนโลยีสารสนเทศสามารถสร้างเครือข่าย แลกเปลี่ยนความรู้ และทำงานร่วมกันได้

4.4 การรองรับ PHP

ภาษาพีเอชพี ในชื่อภาษาอังกฤษว่า PHP ซึ่งใช้เป็นคำย่อแบบกล่าวซ้ำ จากคำว่า PHP Hypertext Preprocessor หรือชื่อเดิม Personal Home Page พีเอชพี (PHP) คือ ภาษาคอมพิวเตอร์ในลักษณะเซิร์ฟเวอร์-ไซด์ สคริปต์ โดยลิขสิทธิ์อยู่ในลักษณะโอเพนซอร์ส ภาษา PHP ใช้สำหรับจัดทำเว็บไซต์ และแสดงผลออกมาในรูปแบบ HTML โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษา ภาษาซี ภาษาจาวา และ ภาษาเพิร์ล ซึ่ง ภาษาพีเอชพี นั้นง่ายต่อการเรียนรู้ ซึ่งเป้าหมายหลักของภาษานี้ คือให้นักพัฒนาเว็บไซต์สามารถเขียน เว็บเพจ ที่มีความตอบโต้ได้อย่างรวดเร็ว

คำสั่งของ PHP สามารถสร้างผ่านทางโปรแกรมแก้ไขข้อความทั่วไป เช่น Notepad หรือ vi ซึ่งทำให้การทำงานของ PHP สามารถทำงานได้ในระบบปฏิบัติการหลักเกือบทั้งหมด โดยเมื่อเขียนคำสั่งแล้วนำมาประมวลผล Apache, Microsoft Internet Information Services (IIS) , Personal Web Server, Netscape และ iPlanet servers, Oreilly Website Pro server, Caudium, Xitami, OmniHTTPd, และอื่นๆ อีกมากมาย. สำหรับส่วนหลักของ PHP ยังมี Module ในการรองรับ CGI มาตรฐาน ซึ่ง PHP สามารถทำงานเป็นตัวประมวลผล CGI ด้วย และด้วย PHP, ทำให้มีอิสรภาพในการเลือกระบบปฏิบัติการ และ เว็บเซิร์ฟเวอร์ นอกจากนี้ยังสามารถใช้สร้างโปรแกรมโครงสร้าง สร้างโปรแกรมเชิงวัตถุ (OOP) หรือสร้างโปรแกรมที่รวมทั้งสองอย่างเข้าด้วยกัน ซึ่งตัวไลบรารีทั้งหลายของโปรแกรม และตัวโปรแกรมประยุกต์ (รวมถึง PEAR library) ได้ถูกเขียนขึ้นโดยใช้รูปแบบการเขียนแบบ OOP เท่านั้น

PHP สามารถทำงานร่วมกับฐานข้อมูลได้หลายชนิด ซึ่งฐานข้อมูลส่วนหนึ่งที่รองรับได้แก่ Oracle, dBase PostgreSQL, IBM DB2, MySQL, Informix ODBC โครงสร้างของฐานข้อมูลแบบ

DBX ซึ่งทำให้ PHP ใช้กับฐานข้อมูลอะไรก็ได้ที่รองรับรูปแบบนี้ และ PHP ยังรองรับ ODBC (Open Database Connection) ซึ่งเป็นมาตรฐานการเชื่อมต่อฐานข้อมูลที่ใช้กันแพร่หลายอีกด้วย ทำให้สามารถเชื่อมต่อกับฐานข้อมูลต่างๆ ที่รองรับมาตรฐานโลกนี้ได้

PHP ยังสามารถรองรับการสื่อสารกับการบริการใน Protocol ต่างๆ เช่น LDAP IMAP SNMP NNTP POP3 HTTP COM (บนวินโดวส์) และอื่นๆ อีกมากมาย นอกจากนี้ยังสามารถเปิด Socket บนเครือข่ายโดยตรง และ ตอบโต้โดยใช้ Protocol ใดๆ ก็ได้ PHP มีการรองรับสำหรับการแลกเปลี่ยนข้อมูลแบบ WDDX Complex กับ Web Programming อื่นๆ ทั่วไปได้ และในส่วน Interconnection, PHP มีการรองรับสำหรับ Java objects ให้เปลี่ยนมันเป็น PHP Object แล้วใช้งานในรูปแบบ CORBA เพื่อเข้าสู่ Remote Object ได้เช่นกัน

4.5 ThaiD

ThaID (ไทยดี) คือ แอปพลิเคชันที่กรมการปกครอง กระทรวงมหาดไทย พัฒนาขึ้นเพื่อใช้ในการพิสูจน์และยืนยันตัวตน (Digital ID) รวมถึงการเปรียบเทียบภาพใบหน้า (Face Verification System) ทางดิจิทัล เมื่อประชาชนเข้าไปใช้บริการจากทางภาครัฐหรือภาคเอกชนที่จำเป็นต้องมีการยืนยันตัวตน ก็สามารถเข้าสู่ระบบแอปพลิเคชัน ThaID เพื่อยืนยันตัวตนได้เลย โดยไม่ต้องกรอกข้อมูลให้เสียเวลา ถือเป็นการสร้างมิติใหม่ของการทำธุรกรรมผ่านช่องทางดิจิทัล ที่มีความสะดวก รวดเร็ว และปลอดภัยมากยิ่งขึ้น และปัจจุบันได้มีการนำมาใช้เพื่อทำการพิสูจน์ตัวตนเพื่อรับสิทธิ์ในการใช้งานระบบต่าง ๆ ของภาครัฐที่ให้บริการประชาชนได้อย่างมีประสิทธิภาพ

เนื่องจากงานวิจัยนี้มุ่งเน้นการรักษาความปลอดภัยและคุ้มครองข้อมูลส่วนบุคคล ตาม พรบ. การคุ้มครองข้อมูลส่วนบุคคล PDPA (Personal Data Protection Act) [3] ที่มีการใช้งานบนระบบสารสนเทศฯ โดยการพิสูจน์ตัวตนผ่าน ThaiD ที่พัฒนาโดยกรมการปกครองและนำมาประยุกต์ใช้กับ Active Directory ของมหาวิทยาลัย

นอกจากนี้ ปัจจุบันได้มีนักวิจัยได้หลายกลุ่มได้ทำการวิเคราะห์และได้ให้คำแนะนำเกี่ยวกับความปลอดภัย Open Web Application Security Project (OWASP) [2] โดยได้ให้คำแนะนำในการพัฒนาระบบสารสนเทศ การออกแบบเครือข่าย แบ่งเป็นการจัดอันดับ 10 ความเสี่ยงด้านความปลอดภัย ทั้งทางด้าน การโจมตีทั้งแอปพลิเคชัน จากการแนะนำของ OWASP จึงได้ศึกษาค้นคว้า

มาตรฐาน OAuth 2.0 ที่ได้รับความนิยม เป็นที่ยอมและคำแนะนำจากนักวิจัย [1] , [6] , [7] , [8] โดยปัจจุบันได้มีการใช้งานอย่างแพร่หลายใน บริษัทใหญ่ๆ เช่น Facebook, Google และ Twitter [12] นอกจากนี้ยังนำ กับ Active Directory เข้ามาประยุกต์ใช้งานในการจัดเก็บบัญชีรายชื่อ โดยเพิ่มความปลอดภัยในการจัดเก็บข้อมูลโดยมีการเข้ารหัส AES [13] ใช้เครื่องมือการพัฒนาด้วย Laravel framework จากการวิเคราะห์และคำแนะนำของนักวิจัย ได้ให้คำแนะนะ เทคนิคการพัฒนาให้เหมาะสมกับความปลอดภัยด้วย OWASP [14]

บทที่ 3
ระเบียบวิธีการวิจัย

การพัฒนาระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID จำเป็นอย่างยิ่งที่จะต้องหาข้อสรุปของระบบที่พัฒนาขึ้นใหม่ว่ามีคุณลักษณะเป็นไปตามจุดประสงค์ของการวิจัยหรือไม่ การหาประสิทธิภาพของระบบโดยวัดจากความพึงพอใจของผู้ใช้บริการระบบพิสูจน์ตัวตนจึงเป็นสิ่งจำเป็นในการสรุปผลการใช้งานระบบ ที่ออกแบบใหม่ เพื่อให้สามารถนำผลการวิจัยนำไปใช้ประโยชน์ต่อไป ซึ่งผู้วิจัยได้กำหนดหัวข้อสำคัญของการดำเนินการวิจัยต่อไปนี้

1. ประชากรและกลุ่มตัวอย่าง

ผู้ใช้งานระบบพิสูจน์ตัวตน (Users) เป็นบุคลากรและนักศึกษา มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์ จำนวน 40 คน การเลือกกลุ่มตัวอย่างที่ใช้ในการทดลองใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling)

2. เครื่องมือที่ใช้ในการวิจัย

2.1 การพัฒนาระบบพิสูจน์ตัวตน

ในการพัฒนาชระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID ต้องเตรียมการดังนี้

2.1.1 ทำหนังสือราชการขออนุญาตกรมการปกครอง ในการเข้าถึงส่วนระบบควบคุมในการเข้าใช้งาน ThaiD สำหรับผู้พัฒนาระบบ

2.1.2 ทำการศึกษา OAuth 2.0 , PDPA , Active Directory , RFC6749 , OWASP

2.1.3 พัฒนาระบบพิสูจน์ตัวตนที่มีการจัดเก็บบัญชีรายชื่อ Active Directory ให้สามารถทำงานผ่าน OAuth 2.0 และทำให้เกิดความเชื่อมโยงกับ ThaiD โดยผู้ใช้สามารถ Authorization ผ่าน ThaiD เสมือน Authorization ผ่าน Active Directory

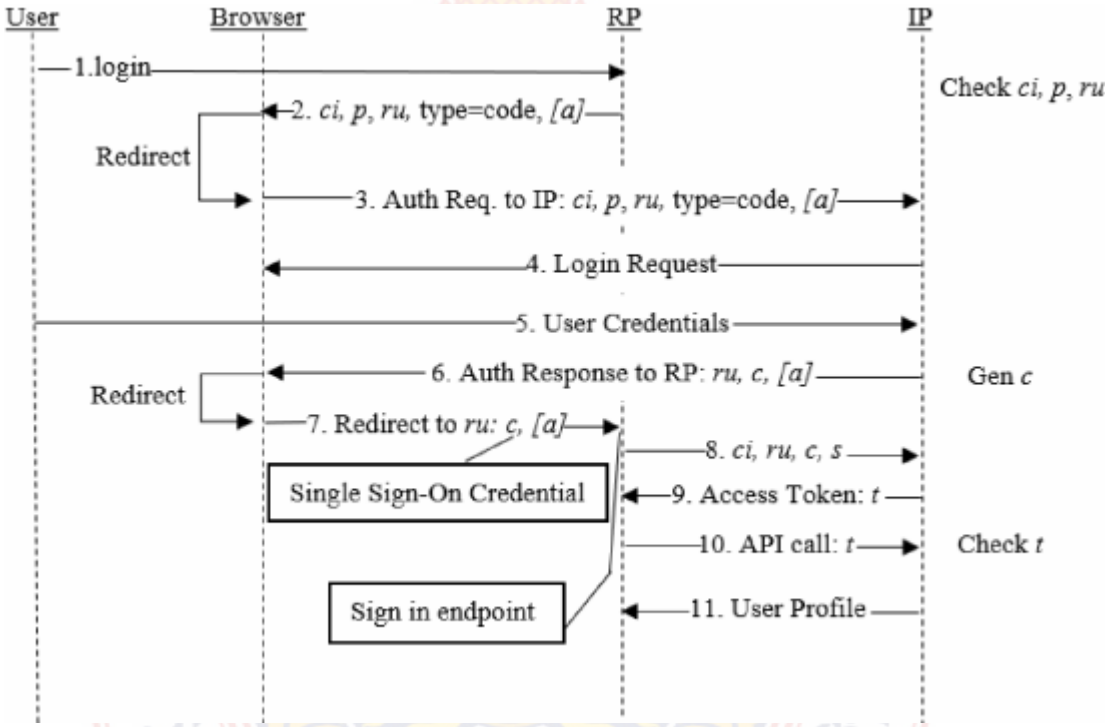
2.1.4 ปรับปรุงให้สามารถแก้ไขข้อมูลส่วนบุคคลได้ด้วยตนเอง

2.1.5 พัฒนาการกำหนดรหัสผ่านบน Active Directory ได้ด้วยตนเอง

2.1.6 สร้างลายเซ็นอิเล็กทรอนิกส์ ที่ใช้สามารถนำไปต่อยอดใช้ร่วมกับระบบสารสนเทศอื่น ๆ ได้ในอนาคต

2.1.7 ผู้วิจัยได้นำ Laravel framework ทำการพัฒนาทั้งระบบ โดยแบ่งขั้นตอนการพัฒนาแบ่งออกเป็น 2 ฝั่ง ประกอบไปด้วย

- Back-end จะเป็นส่วนที่ติดต่อกับระบบฐานข้อมูล ที่ใช้เก็บข้อมูล และเซิร์ฟเวอร์ ที่ใช้จัดการกับการส่งคำขอ และการตอบกลับ รวมถึงการประมวลผลและจัดการข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการทำงานของระบบ
- Front-End ส่วนที่ติดต่อกับผู้ใช้งาน ซึ่งเป็นส่วนที่ผู้ใช้งานสามารถมองเห็น และสื่อสารกับระบบได้โดยตรง คอยควบคุมดูแล และสร้างเว็บไซต์ให้มีส่วนต่อประสานผู้ใช้ (User Interface) และใช้งานได้ถูกต้องตามที่ออกแบบไว้
- นำ ThaiD ทำการพัฒนาระบบพิสูจน์ตัวตน เมื่อผ่านขั้นตอนของ ThaiD เรียบร้อยแล้ว ทำการพิสูจน์ตัวตนผ่าน Active Directory ให้รองรับมาตรฐาน OAuth 2.0 ที่ได้รับความนิยมในการใช้งานโดยมีกระบวนการทำงานดังภาพ



ภาพที่ 5 OAuth 2.0 Authentication Flows

จากภาพที่ 4 ผู้พัฒนาจะได้รับ Token เข้ารหัส/ถอดรหัส (Encryption) หรือการแฮช (Hashing) มาตรฐาน Hash Function ดังภาพที่ 5

```
{
  "access_token" : "U4xxxxxxxxxxxxxxxxxxxxxxxxQ2OjE1M",
  "token_type" : "bearer",
  "expires_in" : 1800 //seconds,
  "refresh_token" : "mEtZlOxxxxxxxxxxxxxxxxxxxx0LTgw"
}
```


ภาพที่ 6 Authorization Token

สำหรับผู้พัฒนาจะนำ access_token ใช้ในการเรียกใช้ API Call ในขั้นตอนที่ 10 โดยที่ขั้นตอนที่ 11 ผู้พัฒนาจะได้รับ User Profile ของผู้ใช้ไป ส่วน token ที่ได้รับนั้นค่าเริ่มต้นจะหมดอายุในเวลา 30 นาที กรณี Token หมดอายุนั้น ผู้พัฒนาจะต้องขอ Token ใหม่จาก refresh_token และจะได้ access_token ใหม่อีกครั้ง ทั้งนี้เพื่อความปลอดภัยของผู้ใช้งาน

2.2 แบบสอบถามสำหรับงานวิจัย

การสร้างเครื่องมือที่ใช้ในการวิจัยโดยใช้แบบสอบถามเพื่อหาประสิทธิภาพและความพึงพอใจในการทำงานของระบบที่พัฒนาขึ้น เป็นแบบมาตราส่วนประเมินค่า แสดงค่า 5 ระดับ (Rating Scale) โดยมีระดับความคิดเห็นดังต่อไปนี้

5 หมายถึง ระดับมากที่สุด
4 หมายถึง ระดับมาก
3 หมายถึง ระดับปานกลาง
2 หมายถึง มีระดับน้อย
1 หมายถึง น้อยที่สุด

3. การเก็บรวบรวมข้อมูล

การศึกษาวิจัยครั้งนี้ ผู้วิจัยจะใช้การรวบรวมข้อมูลจากโดยใช้แบบสอบถามเรื่อง ความพึงพอใจในการใช้งานระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID

4. การวิเคราะห์ข้อมูล

นำข้อมูลที่ได้จากการรวบรวมแบบสอบถามของกลุ่มตัวอย่างที่กำหนดไว้มาคำนวณ แล้วจึงวิเคราะห์ผล โดยมีวิธีการวิเคราะห์ข้อมูล ดังนี้

4.1 สรุปข้อมูลที่ได้รับจากแบบสอบถามแบบปลายเปิดเพื่อแสดงข้อคิดเห็นของผู้ใช้งานต่อระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID โดยการรวบรวมข้อมูลที่ได้จากแบบสอบถามมาสรุปเพื่อนำมาใช้ในการอภิปรายผลต่อไป

นำข้อมูลที่ได้รับจากแบบสอบถามแบบมาตราส่วนประมาณค่า 5 ระดับ มานำเสนอการวิเคราะห์ข้อมูลที่ได้จากแบบสอบถามซึ่งผู้วิจัยกำหนดเกณฑ์การให้คะแนน ดังนี้

4.1.1 วิเคราะห์ความพึงพอใจในประสิทธิภาพของระบบจากกลุ่มผู้ใช้ระบบระบบโดยหาค่าเฉลี่ยของความพึงพอใจรายข้อต่อประสิทธิภาพของระบบ และแปลความตามมาตราส่วนประมาณค่าที่กลุ่มตัวอย่างประมาณค่าไว้ดังนี้

ระดับคะแนน	ระดับความพึงพอใจ	หมายความว่า
4.50-5.00	ความพึงพอใจมากที่สุด	ระบบมีประสิทธิภาพดีมาก
3.50-4.49	ความพึงพอใจมาก	ระบบมีประสิทธิภาพดี
2.50-3.49	ความพึงพอใจปานกลาง	ระบบมีประสิทธิภาพปานกลาง
1.50-2.49	ความพึงพอใจน้อย	ระบบมีประสิทธิภาพพอใช้
1.00-1.49	ความพึงพอใจน้อยที่สุด	ระบบไม่มีประสิทธิภาพ ต้องปรับปรุง

5. สถิติที่ใช้ในการวิเคราะห์

สถิติที่ใช้ในการวิเคราะห์ข้อมูลสำหรับผู้ใช้บริการระบบได้แก่

5.1 สถิติที่ใช้ในการวิเคราะห์ผลสำหรับกลุ่มตัวอย่างผู้บริหารระบบ ค่าเฉลี่ย ($\bar{x}$)

$$\bar{x} = \frac{\sum_{i=1}^{N} x_i}{N}$$

เมื่อ $\bar{x}$ = ค่าเฉลี่ย

$\sum_{i=1}^{N} x_i$ = ผลรวมคะแนนทั้งหมด

N = จำนวนประชากร

ค่าส่วนเบี่ยงเบนมาตรฐาน (SD.)

$$SD. = \frac{\sqrt{n\sum_{i=1}^{n} fx_i^2 - \left(\sum_{i=1}^{n} fx_i\right)^2}}{n(n-1)}$$

เมื่อ SD. = ส่วนเบี่ยงเบนมาตรฐาน

x_i = ข้อมูลแต่ละจำนวน

f = ความถี่

n = จำนวนกลุ่มตัวอย่าง

5.2 สถิติที่ใช้ในการวิเคราะห์ ผลสำหรับประชากรผู้ใช้งาน ค่าเฉลี่ย (μ)

$$\mu = \frac{\sum_{i=1}^{N} x_i}{N}$$

เมื่อ μ = ค่าเฉลี่ย

$\sum_{i=1}^{N} x_i$ = ผลรวมคะแนนทั้งหมด

N = จำนวนประชากร

ค่าส่วนเบี่ยงเบนมาตรฐาน (σ)

$$\sigma = \frac{\sqrt{n\sum_{i=1}^{N} fx_i^2 - \left(\sum_{i=1}^{N} fx_i\right)^2}}{N}$$

เมื่อ σ = ส่วนเบี่ยงเบนมาตรฐาน

x_i = ข้อมูลแต่ละจำนวน

f = ความถี่

N = จำนวนประชากร

ข้อมูลที่ได้รับจากแบบสอบถามในข้อเสนอแนะจะนำเสนอและวิเคราะห์ข้อมูลด้วยการบรรยายและสรุปความคิดเห็น

บทที่ 4
ผลการวิจัย/ผลการวิเคราะห์ข้อมูล

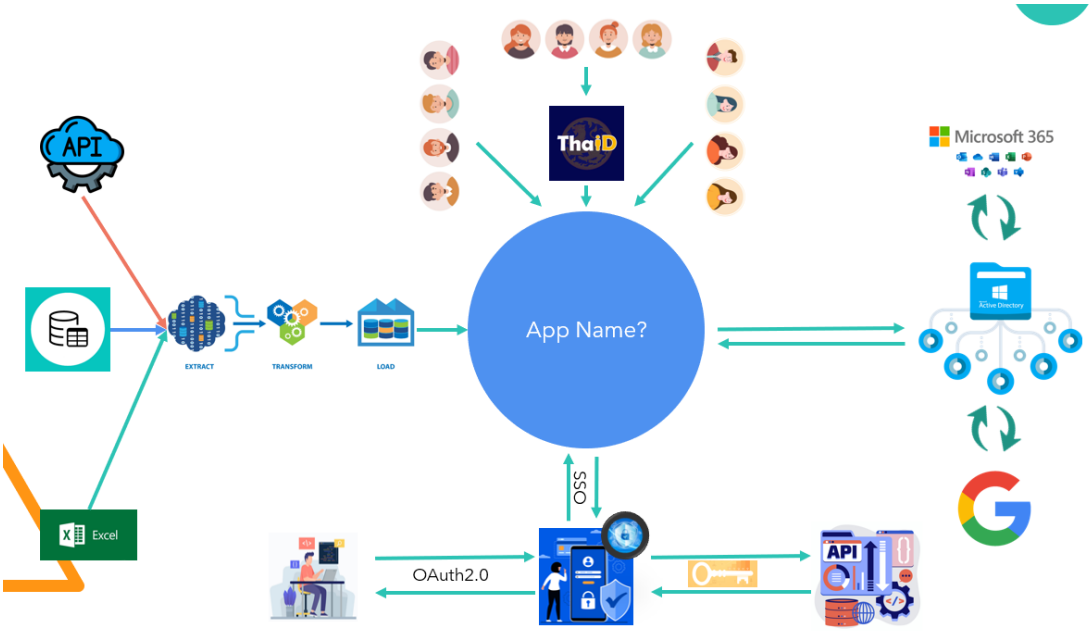
ThaiD (ไทยดี) คือ แอปพลิเคชันที่ กรมการปกครอง กระทรวงมหาดไทย พัฒนาขึ้นเพื่อใช้ในการพิสูจน์และยืนยันตัวตน (Digital ID) รวมถึงการเปรียบเทียบภาพใบหน้า (Face Verification System) ทางดิจิทัล เมื่อประชาชนเข้าไปใช้บริการจากทางภาครัฐหรือภาคเอกชนที่จำเป็นต้องมีการยืนยันตัวตน ก็สามารถเข้าสู่ระบบแอปพลิเคชัน ThaID เพื่อยืนยันตัวตนได้เลย โดยไม่ต้องกรอกข้อมูลให้เสียเวลา ถือเป็นการสร้างมิติใหม่ของการทำธุรกรรมผ่านช่องทางดิจิทัล ที่มีความสะดวก รวดเร็ว และปลอดภัยมากยิ่งขึ้น

1. ผลการพัฒนาระบบ

จากการวิเคราะห์ออกแบบ และพัฒนาระบบ App Name เป็นศูนย์กลางการทำงานระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID โดยมีความสามารถดังนี้

- ทำการตรวจสอบสร้างบัญชีรายชื่อ โดยผ่านกระบวนการ ETL
- App Name สามารถรวบรวมข้อมูลจากหลาย ๆ แหล่ง (Multiple Source)
- มี data warehouse สำหรับข้อมูลบัญชีรายชื่อบน AD (Active Directory)
- สามารถสร้าง แก้ไข บัญชีรายชื่อผ่าน SSL เสริมสร้างความปลอดภัยในการรับส่งข้อมูล
- จัดระเบียบบัญชีรายชื่อ แบ่งแยกตาม campus, คณะ/หน่วย/, ประเภทบุคลากร, ตามความเหมาะสม
- synchronize ข้อมูลบัญชีรายชื่อและทำการสร้างบน Google , Microsoft ผู้ใช้สามารถกำหนดรหัสผ่านและ สามารถเข้าถึงได้ตลอดเวลา
- พิสูจน์ตัวตนผ่าน ThaiD ของกรมการปกครองในการกำหนดรหัสผ่านได้
- ผู้ใช้งานในองค์กร สามารถ update profiles สำหรับทำไว้ใช้งานกับระบบอื่น ๆ ของมหาวิทยาลัย

ซึ่งจากความสามารถของระบบที่ออกแบบใหม่ดังกล่าวสามารถสนับสนุนการทำงานของระบบในภาพรวมโดยผู้วิจัยได้เขียนโมเดลการทำงานของระบบเป็นผังการทำงานรวมศูนย์ไว้ดังภาพ

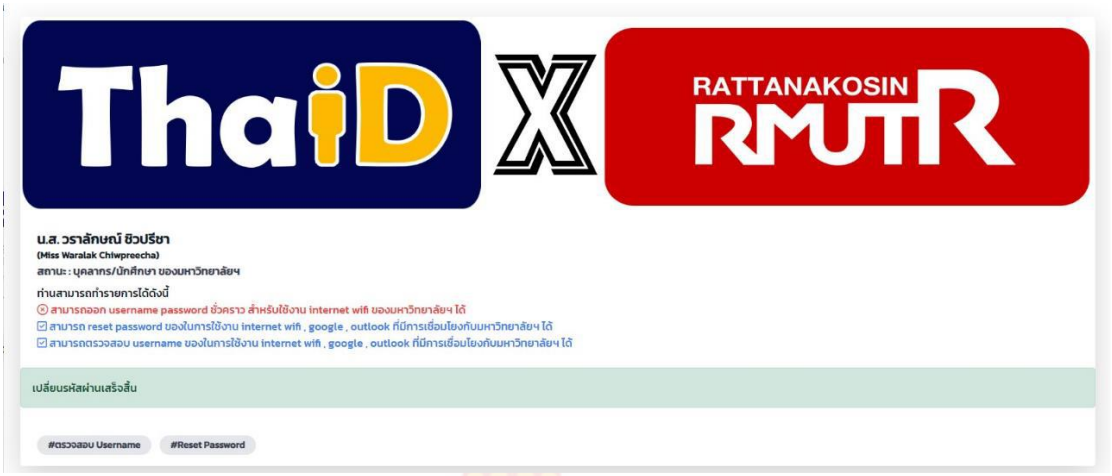


ภาพที่ 7 แสดงการทำงานของระบบพิสูจน์ตัวตน

จากภาพแสดงการทำงานของระบบ Authen ด้วย ThaiD โดยภาพรวมการให้บริการผู้ใช้จะต้องติดตั้งระบบ ThaiD ก่อน หลังจากนั้นจึงผ่านสิทธิด้วยการยืนยันตัวตนกับบัญชีอีเมลของมหาวิทยาลัย ซึ่งผู้ใช้ทุกคนจะมีบัญชีอีเมล 2 ชุด คือ xxxxx.xxx@rmutr.ac.th สาหรับ Gmail (Google G Suite) และ xxxxx.xxx@outlook.rmutr.ac.th ใช้สำหรับ Outlook บน Microsoft Office 365

ศูนย์กลางของระบบคือ app name ที่ถูกพัฒนาขึ้นใหม่เพื่อให้สามารถรวบรวมข้อมูลจากหลายๆแหล่ง โดยจะทำการตรวจสอบสร้างบัญชีรายชื่อ โดยผ่านกระบวนการ ETL และนำไปเก็บไว้ใน data warehouse สำหรับข้อมูลบัญชีรายชื่อบน AD

ผู้ใช้งานระบบสามารถนำ user จากทั้ง 2 ระบบมาพิสูจน์ตัวตนผ่าน Outh2.0 โดยตรวจสอบกับฐานข้อมูลบัตรประชาชนที่ผ่านสิทธิมาจากระบบ ThaiD ซึ่งได้ใช้ API ในการแลกเปลี่ยนข้อมูลกับเครื่องแม่ข่ายของมหาวิทยาลัยเพื่อนำทะเบียนผู้ใช้มาทำ SSO (Single Sign On) หลังจากนั้นก็จะให้สิทธิผู้ใช้ในการเข้าไปทำธุรกรรมต่าง ๆ กับ ระบบให้บริการอิเล็กทรอนิกส์(e-Service) ของมหาวิทยาลัยได้ทันที ซึ่งช่วยอำนวยความสะดวกให้กับผู้ใช้งานในระบบเป็นอย่างมาก และช่วยสร้างความเชื่อมันและความปลอดภัยในการเข้าใช้งานได้อีกด้วย



ภาพที่ 8 แสดงการให้บริการระบบ ThaiD กับระบบพิสูจน์ตัวตนของมหาวิทยาลัย

การให้บริการสำหรับ อาจารย์ บุคลากรและนักศึกษา มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์นั้น เปิดให้บริการ Reset Password via ThaiD (เปลี่ยนรหัสผ่านด้วย ThaiD) นอกจากนี้ในการให้บริการสำหรับบุคคลภายนอก สามารถเข้าใช้งานอินเทอร์เน็ตชั่วคราวได้ 1 account โดยสามารถเข้าใช้ระบบอินเทอร์เน็ตแบบไร้สาย (Wi-Fi) ภายใต้ชื่อ @RMUTR-SLY โดยมีวิธีการติดตั้งและใช้งานระบบ Reset Password Via ThaiD ตามคู่มือที่ได้เผยแพร่ในเว็บไซต์ของมหาวิทยาลัย

2. ผลการประเมินความพึงพอใจของผู้ใช้บริการระบบที่มีต่อระบบพิสูจน์และยืนยันตัวตน

ผู้วิจัยได้จัดทำแบบสอบถามเพื่อประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตน โดยใช้แบบสอบถามความพึงพอใจกับกลุ่มตัวอย่างผู้ใช้บริการระบบ โดยนำระบบพิสูจน์และยืนยันตัวตนไปให้ผู้ใช้บริการระบบทดสอบ และทำแบบสอบถามความคิดเห็นเพื่อนำมาปรับปรุงให้สมบูรณ์มากขึ้น ข้อมูลที่ได้จากแบบสอบถามได้นำมาประมวลผลตามหลักสถิติ แล้วสรุปดังตาราง ต่อไปนี้

ตารางที่ 1 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจในการประเมินประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในการติดตั้งระบบ

หัวข้อ	$\overline{x}$	SD.	ระดับความพึงพอใจ
ความพึงพอใจในด้านการติดตั้งระบบ			
• การทำงาน app name มีรูปแบบ Framework ที่เหมาะสม	4.67	0.58	มากที่สุด
• ความสะดวกในการติดตั้งระบบ ThaiD	4.33	0.58	มาก
• ความเชื่อมั่นในด้านความปลอดภัยของระบบ	4.33	0.58	มาก
• ระบบมีความยืดหยุ่นกับอุปกรณ์ที่หลากหลาย	4.00	1.00	มาก
ค่าเฉลี่ยความพึงพอใจ	4.33	0.68	มาก

จากตารางที่ 1 ในการประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านติดตั้งระบบพบว่า ผู้ใช้บริการระบบมีความพึงพอใจในด้านหน่วยแสดงผลข้อมูลโดยรวมอยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 4.33 และเมื่อพิจารณารายข้อพบว่าผู้ใช้บริการระบบมีความพึงพอใจในระดับมากที่สุด ในด้านการทำงาน app name มีรูปแบบ Framework ที่เหมาะสมและง่ายต่อการทำความเข้าใจ ที่ระดับคะแนน 4.67

ส่วนหัวข้อที่ผู้ใช้บริการระบบมีความพึงพอใจในระดับมาก ได้แก่ความสะดวกในการติดตั้งระบบThaiD 4.33 ความเชื่อมั่นในด้านความปลอดภัยของระบบ ที่ระดับคะแนน 4.33 และระบบมีความยืดหยุ่นกับอุปกรณ์ที่หลากหลายที่ระดับคะแนน 4.00 ตามลำดับ

ตารางที่ 2 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจในการประเมินประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านการนำเข้าข้อมูล

หัวข้อ	$\bar{x}$	SD.	ระดับความพึงพอใจ
ความพึงพอใจในด้านหน่วยนำเข้าข้อมูล (Input)			
• การออกแบบหน้าจอการรับข้อมูลเข้ามีรูปแบบที่เหมาะสม	4.67	0.58	มากที่สุด
• การออกแบบส่วนการนำข้อมูลเข้าให้มีความสัมพันธ์กันกับการออกแบบฐานข้อมูล	4.67	0.58	มากที่สุด
• มีการตรวจสอบความถูกต้องในการป้อนข้อมูลเข้าสู่ระบบ	4.00	1.00	มาก
• การออกแบบหน้าจอป้อนข้อมูลให้ใช้งานง่ายมีคำอธิบายในการใช้งาน	3.33	0.58	ปานกลาง
ค่าเฉลี่ยความพึงพอใจ	4.17	0.68	มาก

จากตารางที่ 2 การประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านหน่วยนำเข้าข้อมูลพบว่า ผู้ใช้บริการระบบมีความพึงพอใจในด้านหน่วยนำเข้าข้อมูลโดยรวมอยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 4.17 และเมื่อพิจารณารายข้อพบว่าผู้ใช้บริการระบบมีความพึงพอใจในระดับมากที่สุดในหัวข้อการออกแบบหน้าจอการรับข้อมูลเข้ามีรูปแบบที่เหมาะสม และการออกแบบส่วนการนำข้อมูลเข้าให้มีความสัมพันธ์กันกับการออกแบบฐานข้อมูล ที่ระดับคะแนน 4.67

ส่วนหัวข้อที่ผู้ใช้บริการระบบมีความพึงพอใจในระดับมาก ได้แก่การตรวจสอบความถูกต้องในการป้อนข้อมูลเข้าสู่ระบบ ที่ระดับคะแนน 4.00 และมีความพึงพอใจในระดับปานกลางในหัวข้อการออกแบบหน้าจอป้อนข้อมูลให้ใช้งานง่ายมีคำอธิบายในการใช้งาน ที่ระดับคะแนน 3.33

ตารางที่ 3 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจในการประเมินประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านการประมวลผล

หัวข้อ	$\overline{x}$	SD.	ระดับความพึงพอใจ
ความพึงพอใจในด้านการประมวลผล (Process)			
• การตอบสนองต่อคำสั่งของโปรแกรม ในการประมวลผลมีความรวดเร็วและได้ผลลัพธ์ที่ถูกต้อง	4.67	0.58	มากที่สุด
• การทำงานของระบบพิสูจน์และยืนยันตัวตน ถูกต้อง เชื่อถือได้	4.33	0.58	มาก
• วิธีการทำงานของระบบพิสูจน์และยืนยันตัวตน มีความยืดหยุ่นสำหรับการเพิ่ม หรือเปลี่ยนแปลงให้เหมาะสมกับการปฏิบัติงานจริงของผู้ใช้	4.33	1.15	มาก
ค่าเฉลี่ยความพึงพอใจ	4.44	0.77	มาก

จากตารางที่ 3 ในการประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านการประมวลผล พบว่า ผู้ใช้บริการระบบมีความพึงพอใจในด้านการประมวลผลโดยรวมอยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 4.44 และเมื่อพิจารณารายข้อพบว่าผู้ใช้บริการระบบมีความพึงพอใจในระดับมากที่สุดในหัวข้อการตอบสนองต่อคำสั่งของโปรแกรม ในการประมวลผลมีความรวดเร็วและได้ผลลัพธ์ที่ถูกต้อง ที่ระดับคะแนน 4.67

ส่วนหัวข้อที่ผู้ใช้บริการระบบมีความพึงพอใจในระดับมาก ได้แก่หัวข้อวิธีการทำงานของระบบพิสูจน์และยืนยันตัวตน ถูกต้อง เชื่อถือได้ ที่ระดับคะแนน 4.33 และวิธีการทำงานของระบบพิสูจน์และยืนยันตัวตน มีความยืดหยุ่น สำหรับการเพิ่ม หรือเปลี่ยนแปลงให้เหมาะสมกับการปฏิบัติงานจริงของผู้ใช้ที่ระดับคะแนน 4.33 เช่นกัน

ตารางที่ 4 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจในการประเมินประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านหน่วยจัดเก็บข้อมูล

หัวข้อ	$\overline{x}$	SD.	ระดับความพึงพอใจ
ความพึงพอใจในด้านข้อมูล			
• ระบบใช้ข้อมูลส่วนบุคคลที่จำเป็นเท่านั้นในการทำงาน	4.67	0.58	มากที่สุด
• ข้อมูลที่นำมาใช้ช่วยลดความซ้ำซ้อนในข้อมูลใน data warehouseได้ (Minimal data redundancy)	4.67	0.58	มากที่สุด
• ระบบฐานข้อมูลที่ออกแบบช่วยให้การเข้าถึงข้อมูลและการประมวลผลมีประสิทธิภาพดีขึ้น	4.33	0.58	มาก
• มีการแจ้งการปกป้องข้อมูลส่วนบุคคลตาม พรบ. PDPA	4.33	0.58	มาก
ค่าเฉลี่ยความพึงพอใจ	4.50	0.58	มากที่สุด

จากตารางที่ 4 ในการประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านหน่วยจัดเก็บข้อมูล พบว่า ผู้ใช้บริการระบบมีความพึงพอใจในด้านหน่วยจัดเก็บข้อมูลโดยรวมอยู่ในระดับมากที่สุด มีค่าเฉลี่ยเท่ากับ 4.50 และเมื่อพิจารณารายข้อ พบว่า ผู้ใช้บริการระบบมีความพึงพอใจในระดับมากที่สุดได้แก่หัวข้อระบบฐานข้อมูลถูกออกแบบอย่างถูกต้องตามหลักสถาปัตยกรรมฐานข้อมูลเชิงสัมพันธ์ ที่ระดับคะแนน4.67 และระบบฐานข้อมูลที่ออกแบบช่วยลดความซ้ำซ้อนในข้อมูลได้ ที่ระดับคะแนน 4.67

ส่วนหัวข้ออื่น ๆ ผู้ใช้บริการระบบมีความพึงพอใจในระดับมากได้แก่ข้อมูลที่นำมาใช้ช่วยลดความซ้ำซ้อนในข้อมูลใน data warehouseได้ (Minimal data redundancy) ที่ระดับคะแนน 4.33 และมีการแจ้งการปกป้องข้อมูลส่วนบุคคลตาม พรบ. PDPA ที่ระดับคะแนน 4.33 เช่นกัน

ตารางที่ 5 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจในการประเมินประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านกระบวนการทำงาน

หัวข้อ	$\bar{x}$	SD.	ระดับความพึงพอใจ
ความพึงพอใจในด้านกระบวนการทำงาน (Procedure)			
• ระบบสามารถสนับสนุนการทำงานแบบหลายผู้ใช้ได้เป็นอย่างดี	4.67	0.58	มากที่สุด
• กระบวนการทำงานของระบบเป็นลำดับขั้นตอน มีการออกแบบความสัมพันธ์กับผู้ใช้ (User Interface) ที่ง่ายต่อการทำความเข้าใจ เหมาะสมกับผู้ใช้	4.33	058	มาก
• การออกแบบระบบรักษาความปลอดภัยของจัดกลุ่มผู้ใช้งานและระบบรักษาความปลอดภัยที่ดี	4.33	0.58	มาก
• ระบบพิสูจน์และยืนยันตัวตนสามารถทำงานได้อย่างมีประสิทธิภาพและเสถียรภาพ	4.33	0.58	มาก
ค่าเฉลี่ยความพึงพอใจ	4.42	0.58	มาก

จากตารางที่ 5 ในการประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านกระบวนการทำงานพบว่าผู้ใช้บริการระบบมีความพึงพอใจในด้านกระบวนการทำงาน โดยรวมอยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 4.42 และเมื่อพิจารณารายข้อ พบว่าผู้ใช้บริการระบบมีความพึงพอใจในระดับมากที่สุดคือหัวข้อระบบสามารถสนับสนุนการทำงานแบบหลายผู้ใช้ได้เป็นอย่างดี ที่ระดับคะแนน 4.67

ส่วนในหัวข้ออื่น ๆ ผู้ใช้บริการระบบมีความพึงพอใจในระดับมากคือกระบวนการทำงานของระบบเป็นลำดับขั้นตอน มีการออกแบบความสัมพันธ์กับผู้ใช้ (User Interface) ที่ง่ายต่อการทำความเข้าใจ เหมาะสมกับผู้ใช้ ที่ระดับคะแนน 4.33 การออกแบบระบบรักษาความปลอดภัยของจัด

กลุ่มผู้ใช้งานและระบบรักษาความปลอดภัยที่ดี ที่ระดับคะแนน 4.33 และระบบพิสูจน์และยืนยันตัวตนสามารถทำงานได้อย่างมีเสถียรภาพ ที่ระดับคะแนน 4.33 เช่นกัน

ตารางที่ 6 แสดงค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับความพึงพอใจในการประเมินประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านการนำไปใช้

หัวข้อ	$\bar{x}$	SD.	ระดับความพึงพอใจ
ความพึงพอใจในด้านการนำไปใช้			
• ผู้ใช้งานสามารถยืนยันตัวตนได้อย่างถูกต้อง	4.67	0.58	มากที่สุด
• ระบบสามารถนำไปใช้ในการเข้าระบบ e-Service อื่น ๆ ของมหาวิทยาลัยได้	4.00	1.00	มาก
ค่าเฉลี่ยความพึงพอใจ	4.33	0.79	มาก

จากตารางที่ 6 ในการประเมินความพึงพอใจในประสิทธิภาพของระบบพิสูจน์และยืนยันตัวตนโดยผู้ใช้บริการระบบในด้านของบุคลากร พบว่า ผู้ใช้บริการระบบมีความพึงพอใจในด้านของบุคลากรโดยรวมอยู่ในระดับมาก มีเฉลี่ยค่าเท่ากับ 4.33 และเมื่อพิจารณารายข้อพบว่าผู้ใช้บริการระบบมีความพึงพอใจในระดับมากที่สุดได้แก่หัวข้อผู้ใช้งานสามารถยืนยันตัวตนได้อย่างถูกต้อง ที่ระดับคะแนน 4.67 และหัวข้อที่ผู้ใช้บริการระบบมีความพึงพอใจในระดับมาก คือมีระบบสามารถนำไปใช้ในการเข้าระบบ e-Service อื่น ๆ ของมหาวิทยาลัยได้ที่ระดับคะแนน 4.00

บทที่ 5
สรุปผล อภิปรายผลและข้อเสนอแนะ

จากการนำระบบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID มาใช้ทำให้บริการเมื่อผู้ใช้งานในระบบยืนยันตัวตนผ่าน ThaiD ระบบของมหาวิทยาลัยจะให้สิทธิในการเข้าใช้บริการอิเล็กทรอนิกส์ต่าง ๆ ได้ ทำให้ผู้ใช้ได้รับความสะดวกขึ้นมากด้วย โดยนำมาขยายผลโดยใช้ชื่อว่า ThaiD X RMUTR ดังภาพ

ภาพที่ 9 ระบบThaiD X RMUTR

1. สรุปผลการวิจัย

สรุปผลการประเมินความพึงพอใจของผู้ใช้บริการระบบทางด้านการพัฒนาระบบที่มีต่อระบบพิสูจน์และยืนยันตัวตน ตามกลุ่มหัวข้อคำถามในด้านต่าง ๆ สามารถแปลผลโดยเรียงลำดับจากมากไปน้อยได้ ดังนี้

1. มีความพึงพอใจมากที่สุดในด้านส่วนจัดการข้อมูล (Data Management) ค่าเฉลี่ยความพึงพอใจ 4.50 หมายความว่า ส่วนจัดการข้อมูลของระบบพิสูจน์และยืนยันตัวตนมีประสิทธิภาพดีมาก

2. มีความพึงพอใจมากในด้านการประมวลผล (Process) ค่าเฉลี่ยความพึงพอใจ 4.44 หมายความว่า การประมวลผลของระบบพิสูจน์และยืนยันตัวตนมีประสิทธิภาพดี

3. มีความพึงพอใจมากในด้านกระบวนการทำงาน (Process) ค่าเฉลี่ยความพึงพอใจ 4.42 หมายความว่ากระบวนการทำงาน ของระบบพิสูจน์และยืนยันตัวตนมีประสิทธิภาพดี

4. มีความพึงพอใจมากในด้านผลลัพธ์ (Output) ค่าเฉลี่ยความพึงพอใจ 4.33 หมายความว่าผลลัพธ์ของระบบพิสูจน์และยืนยันตัวตนมีประสิทธิภาพดี

5. มีความพึงพอใจมากในด้านการนำไปใช้ (Use Case) ค่าเฉลี่ยความพึงพอใจ 4.33 หมายความว่าระบบพิสูจน์และยืนยันตัวตนมีประสิทธิภาพดี เหมาะสมกับผู้ใช้งาน

6. มีความพึงพอใจมากในด้านการนำเข้าข้อมูล (Input) ค่าเฉลี่ยความพึงพอใจ 4.17 หมายความว่า การนำเข้าข้อมูลของระบบพิสูจน์และยืนยันตัวตนมีประสิทธิภาพดี

2. การอภิปรายผล

จากผลการวัดประสิทธิภาพโดยใช้แบบสอบถามประเมินความพึงพอใจของผู้ใช้บริการระบบทางด้านการพัฒนาระบบที่มีต่อระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID ได้คะแนนเฉลี่ยรวมทุกมิติ 4.36 แปลผลได้ว่าระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID มีประสิทธิภาพดี มีความเหมาะสมในการนำมาให้บริการในมหาวิทยาลัยได้เป็นอย่างดี

3. ข้อเสนอแนะ

การทำวิจัยครั้งนี้ เป็นระบบระบบให้บริการอิเล็กทรอนิกส์แบบรวมศูนย์ผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล DOPA -Digital ID ที่สามารถให้บริการได้ครอบคลุมความต้องการของผู้ใช้งาน อย่างไรก็ตามเพื่อให้เกิดความทันสมัยต่อเหตุการณ์และสภาพแวดล้อมทางเทคโนโลยีสมัยใหม่ ผู้วิจัยใคร่ขอเสนอแนะแนวคิดการนำผลการวิจัยไปใช้ให้เกิดประโยชน์ ดังนี้

3.1 ข้อเสนอแนะจากการทำวิจัย

- หลังจากพัฒนาระบบเสร็จเรียบร้อยแล้ว ควรนำระบบมาใช้สำหรับการจัดการทำ Single Sign On กับการให้บริการผ่านระบบอิเล็กทรอนิกส์ในหน่วยงานต่าง ๆ ภายในมหาวิทยาลัย เช่น ระบบทะเบียน ระบบจัดการงานวิจัย หรือระบบสารสนเทศอื่น ๆ

- การเพิ่มประสิทธิภาพการการพิสูจน์และยืนยันตัวตนทางดิจิทัลแบบ 2 Factor Authentications เป็นแนวทางที่เป็นที่นิยมอย่างกว้างขวาง การวิจัยและพัฒนาระบบด้านนี้จะช่วยให้ผู้ใช้ได้รับความปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์

- การศึกษาเพิ่มเติมในมุมมองของการลงทุน และการบริหารจัดการเมื่อนำระบบมาใช้จะสามารถลดการใช้วัสดุสิ้นเปลือง และเป็นการรณรงค์ด้านสิ่งแวดล้อมที่เป็นนโยบายของมหาวิทยาลัย (Green University) รวมทั้งทรัพยากรในการจัดเก็บข้อมูลพื้นฐานสำหรับเป็นหลักฐานในงานเอกสารเนื่องจากเปลี่ยนมาใช้ในลักษณะ E-Service

- หน่วยงานในสังกัดมหาวิทยาลัยฯ ได้นำไปใช้ประโยชน์ร่วมกัน โดยไม่เสียค่าใช้จ่ายในการพัฒนาอีก

บรรณานุกรม

[1]. Binduf, A., Alamoudi, H. O., Balahmar, H., Alshamrani, S., Al-Omar, H., & Nagy, N. (20182018, April). Active directory and related aspects of security. In 2018 21 21st Saudi Computer Society National Computer Conference (NCC) (pp. 4474 4479). IEEE.

[2]. Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., & Guntara, A. (20202020, October). Analysis of web security using open web application security project 10. In 2020

88th International Conference on Cyber and IT Service Management (CITSM) (pp. 1 5). IEEE.

[3].พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. (24 พฤษภาคม 2562). ราชกิจจานุเบกษา. เล่ม136 ตอนที่ 69 ก หน้า 52 95.

[4].สำนักบริหารการทะเบียน กรมการปกครอง. (14 มีนาคม 2566). ระบบ Digital ID ของกรมการปกครองใน

แอปพลิเคชัน ThaID. https://www.bora.dopa.go.th/app-thaid/

[5].สำนักงานพัฒนารัฐบาลดิจิทัล / แผนพัฒนารัฐบาลดิจิทัลของประเทศไทยปี พ.ศ.2566 25702570, /25662566, / (https://www.dga.or.th/wp-content/uploads/2023/05/แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ปี พ.ศ.2566 2570.pdf)

[6].Federico, G. D., & Barcaroli, F. (2022). Cloud Identity Patterns and Strategies: Design enterprise cloud identity models with OAuth 2.0 and Azure Active Directory. Packt Publishing.

[7]. Fotiou, N., Siris, V. A., & Polyzos, G. C. (20212021, July). Capability-based access control for multi-tenant systems using OAuth 2.0 and Verifiable Credentials. In 2021 International Conference on Computer Communications and Networks (ICCCN) (pp. 1 9). IEEE.

[8]. Hardt, D. (Ed.). (2012). Rfc 6749: The oauth 2.0 authorization framework.

[9].Fugkeaw, S., Langsanam, I., & Saviphan, H. (20232023, February). Design and Implementation of Fast and Secure SSO Authentication for Multi-Application

Services Deployed in Cloud. In 2023 15 15th International Conference on Knowledge and Smart Technology (KST) (pp. 1 6).IEEE.5ฉบับปรับปรุง พฤษภาคม 2566

[10].Chaiwut, N., & Rueangsirarak, W. (20222022, November). An Online Gap Analysis on Cyber Security Principles for Thailand Organizations Based on ISO/IEC 27001: 201327001: 2013 Standard. In 2022 62022 6th International Conference on Information Technology (InCIT) (pp. 479479--484). 484). IEEE.

[11].Pandhare, Y., Pujari, P., Bawa, A., & Save, A. (20222022, March). A Secure Authentication Protocol for Enterprise Administrative Devices. In 2022 82022 8th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 11, pp. 358358--364). 364). IEEE.

[12].Hossain, N., Hossain, M. A., Hossain, M. Z., Sohag, M. H. I., & Rahman, S. (20182018, August). OAuth-SSO: a framework to secure the OAuth-based SSO service for packaged web applications. In 2018 172018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/1212th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 15751575--1578). 1578). IEEE.

[13].Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Gómez, N. G. (2021). 2021). On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey. IEEE Access, 99, 109289109289--109319.109319.

[14].Vanderlei, I., Araujo, J., Rocha, R., Silva, G., Pacheco, F., & Dantas, J. (20212021, June). Analysis of Laravel Framework Security Techniques Against Web Application Attacks. In 2021 162021 16th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 11--7). 7). IEEE.

ภาคผนวก ก

คู่มือการใช้งาน

ขั้นตอนการกำหนดรหัสผ่านระบบยืนยันตัวตน (Reset Password) สำหรับนักศึกษา

ระบบยืนยันตัวตน (Reset Password) นักศึกษาทุกท่านจะมี Account สำหรับเข้าใช้งานอินเทอร์เน็ตและอีเมลมหาวิทยาลัย รวมถึงเข้าใช้งานระบบสารสนเทศต่างๆของมหาวิทยาลัย โดยจะสามารถเข้าใช้งานได้นักศึกษาต้องทำการกำหนดรหัสผ่านด้วยตนเอง มีวิธีการกำหนดรหัสผ่าน ดังนี้

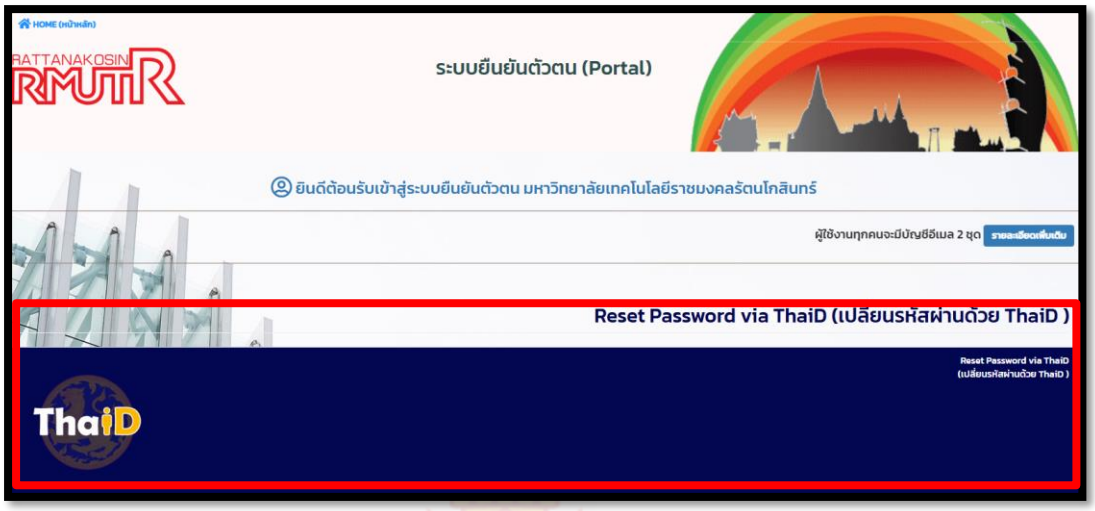
วิธีการติดตั้งและใช้งานระบบ Reset Password Via ThaiD

ThaiD (ไทยดี) คือ แอปพลิเคชันที่ กรมการปกครอง กระทรวงมหาดไทย พัฒนาขึ้นเพื่อใช้ในการพิสูจน์และยืนยันตัวตน (Digital ID) รวมถึงการเปรียบเทียบภาพใบหน้า (Face Verification System) ทางดิจิทัล เมื่อประชาชนเข้าไปใช้บริการจากทางภาครัฐหรือภาคเอกชนที่จำเป็นต้องมีการยืนยันตัวตน ก็สามารถเข้าสู่ระบบแอปพลิเคชัน ThaID เพื่อยืนยันตัวตนได้เลย โดยไม่ต้องกรอกข้อมูลให้เสียเวลา ถือเป็นการสร้างมิติใหม่ของการทำธุรกรรมผ่านช่องทางดิจิทัล ที่มีความสะดวก รวดเร็วและปลอดภัยมากยิ่งขึ้น

- **สำหรับ อาจารย์ บุคลากรและนักศึกษา มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์**
  เปิดให้บริการ Reset Password via ThaiD (เปลี่ยนรหัสผ่านด้วย ThaiD)
- **สำหรับบุคคลภายนอก**
  สามารถเข้าใช้งานอินเทอร์เน็ตชั่วคราวได้ 1 account โดยสามารถเข้าใช้ระบบอินเทอร์เน็ตแบบไร้สาย (Wi-Fi) ภายใต้ชื่อ @RMUTR-SLY

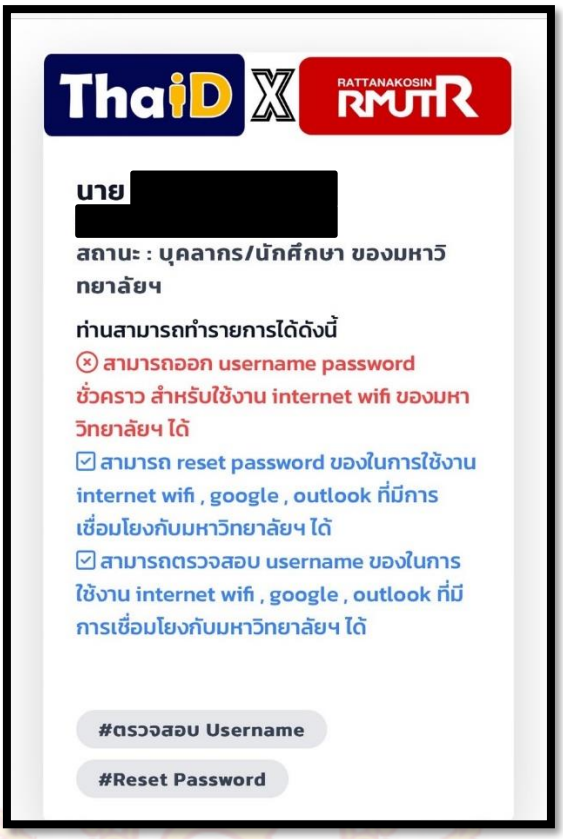
วิธีการติดตั้งและใช้งานระบบ Reset Password Via ThaiD

1. ดาวน์โหลดแอปพลิเคชัน ThaiD ลงในโทรศัพท์มือถือของตนเอง ใช้ได้ทั้งระบบ iOS และระบบแอนด์ดรอย (Android) ลิงก์คู่มือการติดตั้ง https://www.bora.dopa.go.th/app-thaid/
2. เข้าหน้าเว็บไซต์ portal.rmutr.ac.th จากนั้นเลือก Reset Password via ThaiD



3. ระบบจะแสดงป๊อปอัพ เพื่อเข้าสู่แอพพลิเคชั่น ThaiD

4. ระบบจะแสดงข้อมูลเบื้องต้นของท่าน
   กรณีต้องการตรวจสอบ Username เลือก **#ตรวจสอบ Username**
   กรณีต้องการ Reset Password เลือก **#Reset Password**



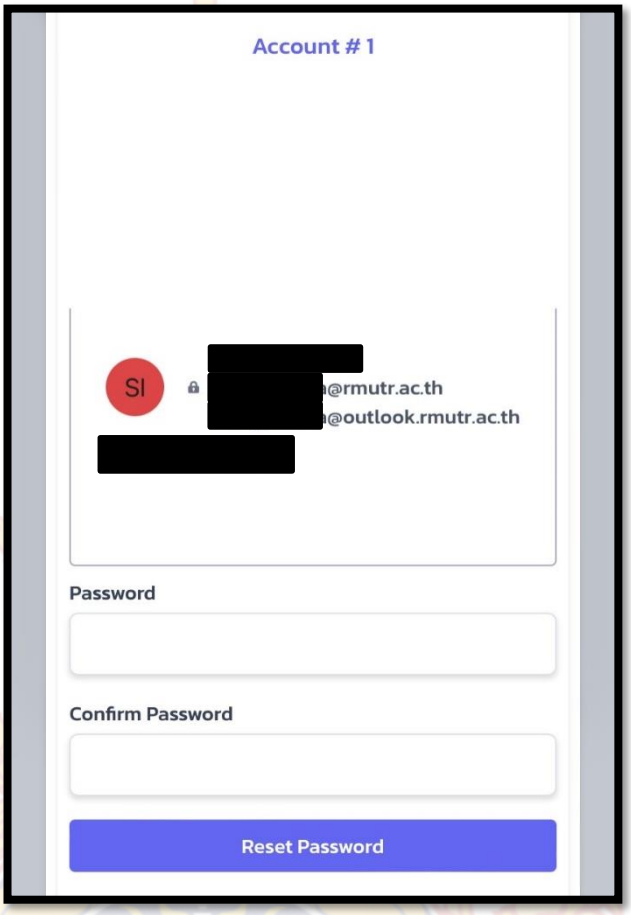
5. กรณีต้องการตรวจสอบ Username เลือก **#ตรวจสอบ Username** ระบบจะแสดงข้อมูลดังนี้

5.1 Username (สำหรับเข้าใช้งานอินเทอร์เน็ต และระบบสารสนเทศของมหาวิทยาลัย)

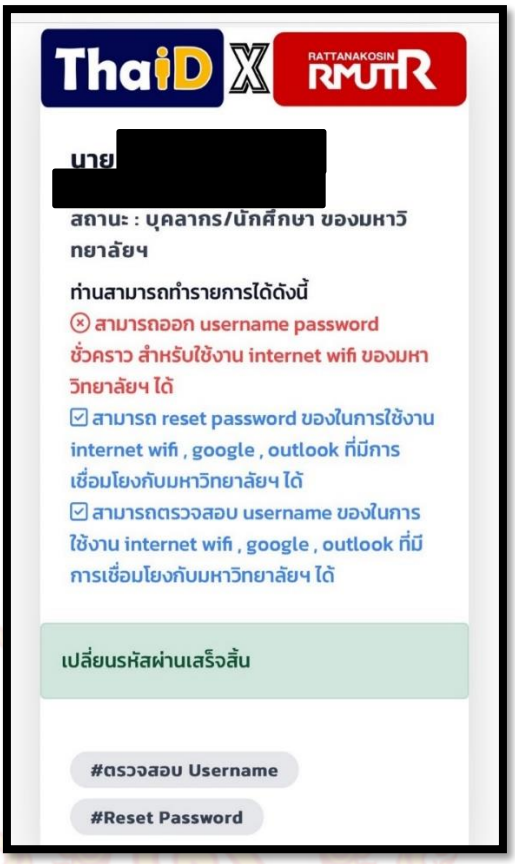
5.2 Email username@rmutr.ac.th (สำหรับเข้าใช้งานผ่าน Gmail)

5.3 Email username@outlook.rmutr.ac.th (สำหรับเข้าใช้งานผ่าน office.com)

6. กรณีต้องการเปลี่ยนรหัสผ่าน เลือก **#Reset Password** ระบบจะแสดงข้อมูลของท่าน จากนั้นกำหนดรหัสผ่านที่ต้องการ โดยต้องใส่รหัสผ่าน 8 หลักขึ้นไป



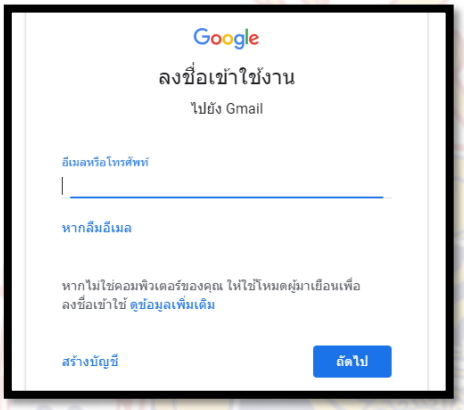
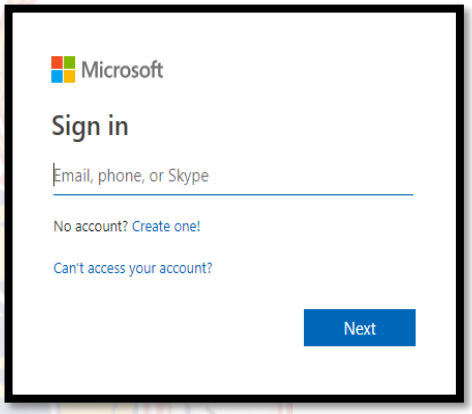
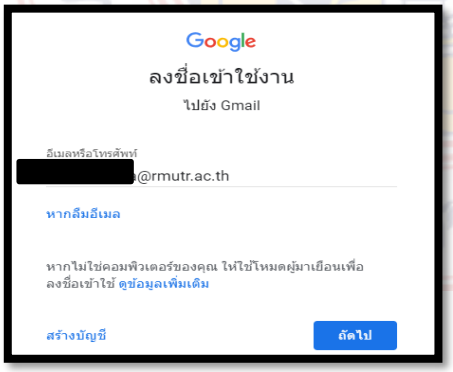
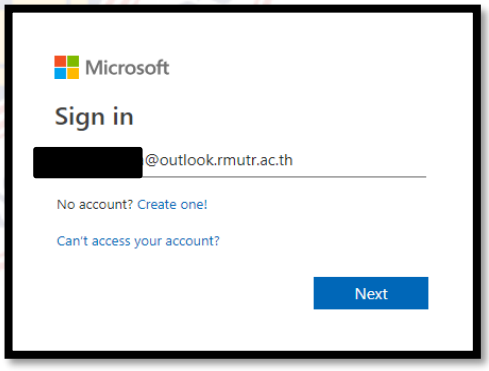
7. หลังจากกำหนดรหัสผ่านเรียบร้อยแล้ว รอ 5 นาที นักศึกษาสามารถเข้าใช้งานระบบอินเทอร์เน็ต และอีเมลของมหาวิทยาลัยได้

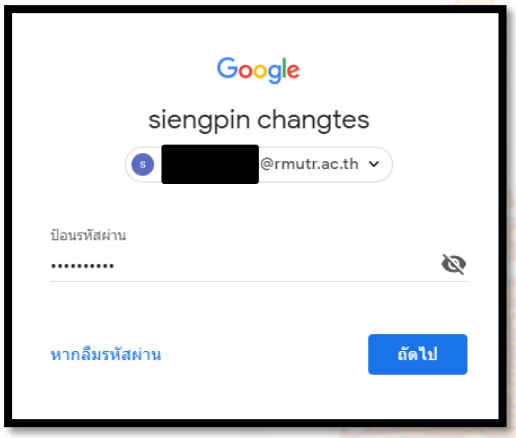
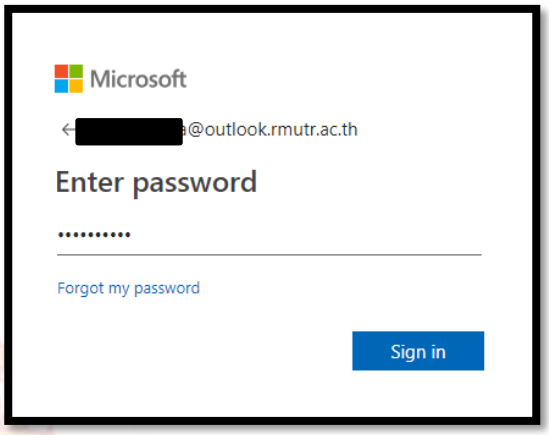
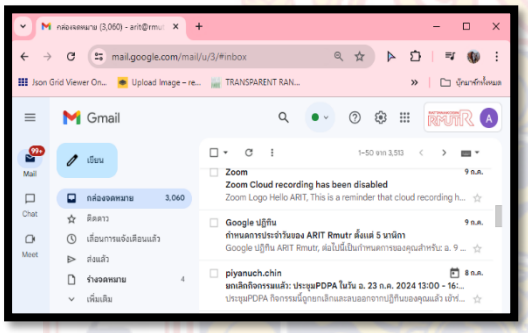
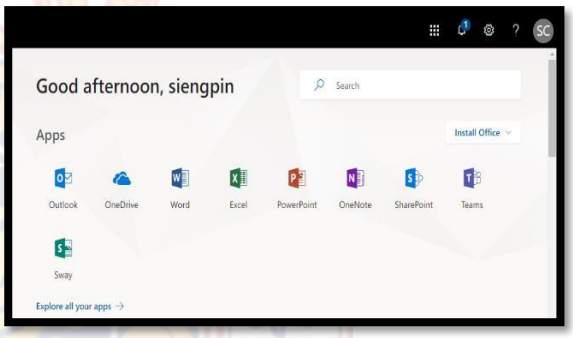


** หลังจากกำหนดรหัสผ่านเรียบร้อยแล้ว รอ ประมาณ 5 นาที สามารถเข้าใช้งานได้ในส่วนของอินเทอร์เน็ต อีเมลมหาวิทยาลัยและระบบสารสนเทศต่างๆของมหาวิทยาลัย

ขั้นตอนการใช้งานอีเมลมหาวิทยาลัย

ผู้ใช้งานทุกคนจะมีบัญชีอีเมล 2 ชุด คือ xxxxx.xxx@rmutr.ac.th สำหรับ Gmail (Google G Suite) และ xxxxx.xxx@outlook.rmutr.ac.th ใช้สำหรับ Outlook บน Microsoft Office 365 เข้าผ่าน office.com

Gmail (@rmutr.ac.th)	Office 365 (@outlook.rmutr.ac.th)
สำหรับอีเมลโดเมน @rmutr.ac.th Login Information Username: xxxxx.xxx@rmutr.ac.th Password: รหัสผ่านของคุณ **(username , password เหมือนใช้งานอินเทอร์เน็ตมหาวิทยาลัย)**	สำหรับอีเมลโดเมน @outlook.rmutr.ac.th Login Information Username: xxxxxxxx@outlook.rmutr.ac.th Password: รหัสผ่านของคุณ **(username , password เหมือนใช้งานอินเทอร์เน็ตหาวิทยาลัย)**
1. URL : https://gmail.com 	1. URL : office.com 
2. จากนั้นใส่ที่อยู่อีเมลมหาวิทยาลัยคลิก “ถัดไป” 	2. จากนั้นใส่ที่อยู่อีเมลมหาวิทยาลัย คลิก “**Next**” 

Gmail (@rmutr.ac.th)	Office 365 (@outlook.rmutr.ac.th)
3. ใส่ Password จากนั้น คลิก “ถัดไป” 	3. ใส่ Password จากนั้น คลิก “**Sign in**” 
4. เมื่อลงชื่อเข้าใช้งานสำเร็จ หน้าจอจะเข้าสู่ส่วนของ Gmail ซึ่งจะแสดงจดหมาย e-mail ขาเข้าทั้งหมด และ ส่วนการใช้งานอื่นๆ ดังภาพ 	4. เข้าสู่อีเมลของคุณ โดยมีแถบเครื่องมือเพื่อการใช้งาน Outlook, Calendar, Ms Teams , People, Newsfeed, Skydrive และ Sites 

ภาคผนวก ข

แบบสอบถามงานวิจัย

แบบสอบถามสำหรับผู้ใช้บริการ

กรุณาขีดเครื่องหมาย ✓ ในช่องระดับความพึงพอใจที่ท่านต้องการ

ลำดับที่	หัวข้อ	ระดับความพึงพอใจ				
		5	4	3	2	1
	การติดตั้งระบบ (Install)					
1.	การทำงาน app name มีรูปแบบ Framework ที่เหมาะสม					
2.	ความสะดวกในการติดตั้งระบบ ThaiD					
3.	ความเชื่อมั่นในด้านความปลอดภัยของระบบ					
4	ระบบมีความยืดหยุ่นกับอุปกรณ์ที่หลากหลาย					
	การนำข้อมูลเข้า (Input)					
5.	การออกแบบหน้าจอการรับข้อมูลเข้ามีรูปแบบที่เหมาะสม					
6.	การออกแบบส่วนการนำข้อมูลเข้ามีสัมพันธ์กันกับการออกแบบฐานข้อมูล					
7.	การออกแบบหน้าจอป้อนข้อมูลให้ใช้งานง่ายมีคำอธิบายในการใช้งาน					
8.	มีการตรวจสอบความถูกต้องในการป้อนข้อมูลเข้าสู่ระบบ					
	การประมวลผล (Process)					
9.	วิธีการทำงานของระบบพิสูจน์และยืนยันตัวตน ถูกต้อง เชื่อถือได้					

10.	วิธีการทำงานของระบบพิสูจน์และยืนยันตัวตน มีความยืดหยุ่น สำหรับการเพิ่ม หรือเปลี่ยนแปลงให้เหมาะสมกับการปฏิบัติงานจริงของผู้ใช้					
11.	การตอบสนองต่อคำสั่งของโปรแกรม ในการประมวลผลมีความรวดเร็วและได้ผลลัพธ์ที่ถูกต้อง					
	ส่วนจัดการข้อมูล (Data Management)					
12.	ระบบใช้ข้อมูลส่วนบุคคลที่จำเป็นเท่านั้นในการทำงาน					
13.	ระบบฐานข้อมูลที่ออกแบบช่วยให้การเข้าถึงข้อมูลและการประมวลผลมีประสิทธิภาพดีขึ้น					
14.	ข้อมูลที่นำมาใช้ช่วยลดความซ้ำซ้อนในข้อมูลใน data warehouseได้ (Minimal data redundancy)					
15.	มีการแจ้งการปกป้องข้อมูลส่วนบุคคลตาม พรบ. PDPA					
	กระบวนการทำงาน(Procedure)					
16.	กระบวนการทำงานของระบบเป็นลำดับขั้นตอน มีการออกแบบความสัมพันธ์กับผู้ใช้ (User Interface) ที่ง่ายต่อการทำความเข้าใจเหมาะสมกับผู้ใช้					
17.	การออกแบบระบบรักษาความปลอดภัยของจัดกลุ่มผู้ใช้งานและระบบรักษาความปลอดภัยที่ดี					
18.	ระบบสามารถสนับสนุนการทำงานแบบหลายผู้ใช้ได้เป็นอย่างดี					
19.	ระบบพิสูจน์และยืนยันตัวตนสามารถทำงานได้อย่างมีประสิทธิภาพและเสถียรภาพ					
	การนำไปใช้ (Use Case)					

20.	ผู้ใช้งานสามารถยืนยันตัวตนได้อย่างถูกต้อง					
21.	ระบบสามารถนำไปใช้ในการเข้าระบบ e-Service อื่น ๆ ของมหาวิทยาลัยได้					

ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

.....

.....

.....

ประวัติผู้วิจัย

1. ชื่อ สกุล **อาจารย์** ดร.วัชรินทร์ วรินทักษะ

2. ตำแหน่งปัจจุบัน ผู้อำนวยการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

3. หน่วยงานที่สามารถติดต่อได้

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
96 หมู่3 ต.ศาลายา อ.พุทธมณฑล จ.นครปฐม 73170
โทรศัพท์ 02-441-6050
Watcharin.W@rmutr.ac.th

4. ประวัติการศึกษา

ปริญญาเอก มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ พ.ศ.2559

ปริญญาโท มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
ครุศาสตร์อุตสาหกรรมมหาบัณฑิต สาขาวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ พ.ศ.2545

ปริญญาตรี สถาบันราชภัฏจันทรเกษม
ครุศาสตร์บัณฑิต สาขาวิชาคอมพิวเตอร์ศึกษา พ.ศ.2538

5. สาขาวิชาการที่มีความชำนาญพิเศษ

วิทยาการข้อมูล
เครือข่ายคอมพิวเตอร์

6. ประสบการณ์ที่เกี่ยวข้องกับการบริหารงานวิจัย

- การพัฒนาระบบสารสนเทศสำหรับการฝึกอบรม
- องค์ประกอบของระบบจัดการองค์ความรู้โดยใช้ระบบเทคโนโลยีสารสนเทศเป็นหลักในการพัฒนา
- การพยากรณ์ปริมาณน้ำฝนในเขตพื้นที่บางนาโดยใช้วิธีวิเคราะห์อนุกรมเวลา

- M-Learning system to support multi-user perspective.
- Determining appropriate of Data Classification with Multi-Layer Perceptron, Support Vector Machines and Radial Basis Function
- Components and Processes of Knowledge Management System in the information technology services at Higher Education.
- The Synthesis Model of Knowledge Management System using Rapid Application Software Development.
- A study of the factors of cloud computing for the education management.
- Examining Spurious Information through Text Categorization Methods (IEEE)
- Determinants Affecting the Adoption of Individualized Marketing Technology in Blended Medical Education (ACM)
- The System Transformation for Customer Relationship Management Application: Rebranding (IEEE)
- Exploring Acceptance Factors of the One Stop Service Application through Sentiment Analysis for Integrative Thai Medicine Clinic (IEEE)
- Examining Patterns of Alternative Medicine Service Utilization for Innovative Appointment Scheduling System.(ACM)