ปีที่ 4 ฉบับที่ 1 (2024) : มกราคม – มิถุนายน 2567
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology LOEI RAJABHAT UNIVERSITY

การยืนยันตัวตนสำหรับเว็บแอปพลิเคชันแบบพหุปัจจัย

Two-factor Authentication for Web Application

วุฒิพงษ์ พันธุมนันท์[1] และ ชัยนันท์ สมพงษ์[1*]
Vutthipong Puntumnunt[1] and Chaiyanan Sompong[1*]
[1]สาขาวิชาคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสกลนคร จังหวัดสกลนคร 47000
[1]Department of Computer, Faculty of Science and Technology, Sakon Nakhon Rajabhat University, Sakon Nakhon Province, 47000
[*]Corresponding author E-mail: chaiyanan@snru.ac.th
Received 16 February 2024, Accepted 13 May 2024, Published 17 May 2024

บทคัดย่อ

การล็อกอินเข้าสู่ระบบเว็บแอปพลิเคชันด้วยวิธีการใช้รหัสผ่านเป็นวิธีที่พบเห็นทั่วไปในระบบสารสนเทศต่างๆ สำหรับเว็บแอปพลิเคชันที่ต่างกันการจำรหัสผ่านหลายรหัสในการเข้าสู่ระบบยังคงเป็นปัญหาที่เกิดขึ้นกับผู้ใช้ที่มีโอกาสในการลืมรหัสผ่าน ทำให้เกิดการปัญหามากมายจนนำไปสู่ช่อง นอกจากนี้การให้ผู้อื่นยืมรหัสผ่านจะทำให้เกิดปัญหาการถูกขโมยรหัสผ่านจากผู้ไม่ประสงค์ดี นับเป็นช่องโหว่สำคัญที่จะนำปสู่การถูกโจมตีทางไซเบอร์ อย่างไรก็ตามนักพัฒนาระบบสารสนเทศได้นำการยืนยันตัวตนแบบพหุปัจจัยเข้ามาใช้เพื่อให้เกิดความปลอดภัยในการใช้มากขึ้น แต่ยังคงมีข้อจำกัดในด้านค่าใช้จ่ายและความสะดวกสบายในการใช้งาน ดังนั้นงานวิจัยนี้มีวัตถุประสงค์เพื่อสร้างระบบการยืนยันตัวตนสำหรับเว็บแอปพลิเคชันแบบสองขั้นตอนด้วยคิวอาร์โค้ด โดยการใช้เทคโนโลยีการยืนยันตัวตนแบบไม่มีการเก็บสถานะ (Stateless Authentication) ด้วยเทคโนโลยี JSON Web Token (JWT) ซึ่งออกแบบในการเข้าใช้ระบบสารสนเทศหรือเว็บแอปพลิเคชันสองขั้นตอนได้แก่ 1) การยืนยันตัวตนของผู้ใช้เพื่อรับ user_token และ 2) การเข้าสู่เว็บแอปพลิเคชันด้วยการสแกนคิวอาร์โค้ด ผลการทดสอบจำลองการใช้งานด้วยผู้ใช้จำนวน 30 ถึง 240 บัญชี พร้อมกันพบว่ามีประสิทธิภาพด้านเวลาในการตอบสนอง (Response Time) ที่เหมาะสมในการใช้งานรองรับผู้ใช้ที่ 90 บัญชี ที่เวลาเฉลี่ย 4 วินาที ในขณะที่ผู้ใช้ 240 บัญชีเข้าระบบพร้อมกันมีความเร็วเฉลี่ยประมาณ 8 วินาที ส่วนด้านประสิทธิภาพพบว่าได้รับการประเมินจากผู้เชี่ยวชาญที่คะแนนเฉลี่ย 4.50 อยู่ในระดับมากที่สุด

คำสำคัญ: การให้ยืมรหัสผ่าน การยืนยันตัวตนแบบพหุปัจจัย การยืนยันตัวตนแบบไม่มีการเก็บสถานะ คิวอาร์โค้ด

ABSTRACT

Web application login based on password is commonly to apply in information system. For various applications, a numerous password memorization is still a problem for users that have a chance to forget a password. Moreover, a password lending cause a leak password that is stolen a password from a malicious person. It is a major cyber vulnerability that leads to a cyber attack. However, a researcher develop a multi-factor authentication to increase a security for application login. This approach is still a limitation of cost and

JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY

comfortable using. Therefore, this research aims to develop the two-step authentication for web application. The proposed method applies a stateless authentication based on JSON Web Token (JWT) technology. It divides to two steps consisting of 1) user authentication to obtain a user_token and 2) web login using QR code scanning. The experiment result to simulate a scenario for 30-240 user accounts login simultaneously found that the performance of a response time is an average at 3-7 second in case of 240 user accounts, which depends on a network traffic. The performance assessment found that obtains a score at 4.53 that means excellent level.

Keywords: Password Lending, Multi-factor Authentication, Stateless Authentication, QR Code

บทนำ

การให้บริการระบบสารสนเทศผ่านเว็บแอปพลิเคชันส่วนใหญ่จำเป็นต้องมีการยืนยันตัวตนเพื่อเข้าใช้งานระบบ (Login) ซึ่งผู้ให้บริการนอกจากจะต้องคำนึงถึงความปลอดภัยของการเข้าถึงข้อมูลแล้วยังต้องมีความสะดวกต่อการใช้งาน โดยการยืนยันตัวตนที่นิยมใช้กันมากที่สุดคือการใช้ระบบรหัสผ่าน (Password) ซึ่งในฝั่งของแอปพลิเคชันรหัสผ่านจะถูกกระบวนการเข้ารหัส (Password encryption) ด้วยการเข้ารหัสในด้วยฟังก์ชันแฮช (Hash function) เช่น MD5, SHA-2, SHA-3 หรือ SHA256 ซึ่งเป็นการป้องกันการเปิดเผยรหัสผ่านจากการดักจับข้อมูลระหว่างการส่งข้อมูลไปยังเซิร์ฟเวอร์ยืนยันตัวตน ส่วนในฝั่งของผู้ใช้ (User) การยืนยันตัวตนด้วยการใช้รหัสผ่านในสถานะการณ์จริงส่วนมากจะใช้หนึ่งรหัสผ่านต่อหนึ่งแอปพลิเคชัน ในทำนองเดียวกันถ้าผู้ใช้มีการใช้งานหลายแอปพลิเคชันจำเป็นต้องมีการยืนยันตัวตนด้วยรหัสผ่านหลายรหัส (Multi point authentication) (Chaimueng et al., 2012) ทำให้ผู้ใช้ต้องจำรหัสผ่านหลายชุด โดยทางปฏิบัติที่ง่ายที่สุดสำหรับผู้ใช้ คือ การตั้งรหัสผ่านเหมือนกันทุกๆ แอปพลิเคชัน อีกทั้งยังพบว่ามีการใช้คำง่ายๆ ในการตั้งรหัสผ่าน เช่น “password”, “123456” หรือ “aaaaaa” เป็นต้น จากการศึกษากลุ่มคนอายุ 10-24 ปี (Titiakarawongse and Boonkrong, 2023) พบว่า กลุ่มคนเหล่านี้มีความตระหนักมากขึ้นในการตั้งรหัสผ่าน ทั้งด้านวิธีการ ความซับซ้อน และความยาวของรหัสผ่าน ซึ่งมีโอกาสที่ผู้ใช้จะลืมรหัสผ่านที่มีความยาวและซับซ้อน จนทำให้เกิดการบันทึกรหัสผ่านลงบนกระดาษ หรือสื่อภายนอก จากปัญหาที่กล่าวมาข้างต้น เป็นการนำไปสู่การเกิดจุดอ่อนของระบบความปลอดภัยในการยืนยันตัวตน เช่น การเดารหัสผ่าน การแอบดูรหัสผ่าน การขโมยรหัสผ่านได้ หรือแม้กระทั่งการให้ยืมรหัสผ่านระหว่างกัน เป็นต้น

การแก้ไขปัญหาที่กล่าวมาข้างต้นมีแนวคิดในการจัดการปัญหารหัสผ่านหลายชุดด้วยการยืนยันตัวตน ณ จุดเดียว (Single Sign-On: SSO) โดยการเข้าสู่ระบบครั้งเดียวด้วยรหัสผ่านชุดเดียว แล้วสามารถเข้าใช้ทรัพยากรต่างๆ ได้หลายแอพลิเคชัน ซึ่งการใช้รหัสผ่านเดียวก็ยังคงมีความเสี่ยงต่อการรั่วไหลของรหัสผ่านในกรณีของการขโมย หรือแอบดูรหัสผ่าน (Shoulder Surfing) โดยที่ Sarawan (2018) นำเสนอการใช้รหัสผ่านเสมือนด้วยการเข้ารหัสของรหัสผ่านแบบตารางสุ่มอักษรก่อนการเข้าสู่ระบบเพื่อป้องกันการแอบดูจากผู้ไม่ประสงค์ดี แม้ว่าจะช่วยให้ผู้ใช้ได้ป้อนรหัสผ่านโดยไม่ต้องกังวลใจ แต่ก็ทำให้ผู้ใช้ต้องยุ่งยากในการถอดรหัสของตารางสุ่มอักษรในการป้อนรหัสผ่าน ดังนั้นจึงมีการนำเสนอวิธีการยืนยันตัวตนแบบพหุปัจจัย (Two-factor Authentication: 2FA) โดยใช้รหัสผ่านครั้งเดียว (One time Password: OTP) (Chaimueng, Puangpronpitag, and Pongsiri, 2012; Thumsiraruk and Puangpronpitag, 2015) เข้ามาเป็นปัจจัยที่สองในการยืนยันตัวตน นอกจากนี้ยังมีการนำเสนอการใช้ชีวมาตร (Biometric) (Thumsiraruk and Puangpronpitag, 2015; Sainui, Jankaew, and U-seng, 2021) การใช้ลายเซ็นดิจิทัล (Digital Signature) (Bunaramrueang and Kowpatanakit, 2023) หรือ การใช้อุปกรณ์ร่วม (Mutual Authentication) (Rukpakavong, Subsomboon, and Nilpanich, 2022) เป็นพหุปัจจัยในการเพิ่มความน่าเชื่อถือและความปลอดภัยของระบบ

JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY

อีกทั้งให้ผู้ใช้มีความสะดวกสบายไม่ต้องกังวลกับการโดนโจมตี แต่เทคโนโลยีที่กล่าวมาจะต้องมีการขอรับบริการกับผู้ให้บริการที่มาพร้อมกับค่าใช้จ่าย เช่น SMS, SSL, OTP Token หรือ Mobile Token

การยืนยันตัวตนแบบพหุปัจจัยได้รับความนิยมในการใช้งานอย่างแพร่หลาย เนื่องจากมีความน่าเชื่อถือกับระบบที่ต้องการความมั่นคงปลอดภัยสูง เช่น ระบบธนาคาร หรือระบบการชำระเงิน เป็นต้น ซึ่ง Vongsingthong et al. (2023) ได้มีการนำเสนอวิธีการนำ Biometric โดยใช้ใบหน้า (Face) ลายนิ้วมือ (Fingerprint) และม่านตา (Iris) เพื่อยืนยันตัวตนก่อนเข้าใช้ระบบ ขณะที่ Chaimueng et al. (2012) นำเสนอการใช้ 2FA สำหรับ SSO บนเทคโนโลยี LDAP โดยใช้ร่วมกับ OTP โดยการส่ง SMS ซึ่งผลการพัฒนาระบบดังกล่าวสามารถแก้ปัญหาการรั่วไหลของรหัสผ่านได้ นอกจากนี้ Rukpakavong et al. (2022) ได้พัฒนาระบบการยืนยันตัวตันแบบใช้อุกรณ์ร่วมกันกับระบบเครื่องกดเงินอัตโนมัติ (ATM) โดยการใช้โทรศัพท์มือถือยืนยันตัวตนในครั้งแรกและใช้การสแกนรหัสคิวอาร์ในการทำธุรกรรม จะเห็นได้ว่าการการยืนยันตัวตนแบบพหุปัจจัยมีความปลอดภัยกับปัญหาการรั่วไหลของรหัสผ่าน

ระบบสารสนเทศในมหาวิทยาลัยราชภัฏสกลนครได้ดำเนินการพัฒนาระบบแบบเว็บแอปพลิเคชัน ซึ่งมีการนำมาใช้งานกับทั้งนักศึกษาและบุคลากรหลากหลายระบบ เช่น ระบบงานทะเบียนนักศึกษา บุคลากร หรือระบบงานวิจัย เป็นต้น ทำให้พบปัญหาการใช้ระบบการยืนยันตัวตนที่ต้องใช้หลายรหัสผ่าน จนนำไปสู่ปัญหาดังที่กล่าวในข้างต้น ดังนั้นผู้วิจัยจึงได้เสนอการพัฒนาการยืนยันตัวตนแบบพหุปัจจัย โดยใช้วิธีการยืนยันตัวตนแบบไม่มีการเก็บสถานะ (Stateless Authentication) ด้วยเทคโนโลยี JSON Web Token หรือ JWT ซึ่งในขั้นแรกเป็นการยืนยันตัวตนของผู้ใช้เพื่อรับ user_token และเมื่อต้องการเข้าสู่เว็บไซต์หรือแอปพลิเคชันจะใช้คิวอาร์โค้ดในการเข้าสู่ระบบและจะใช้ user_token ขอรับสิทธิ์ในการเข้าสู่ระบบ เป็นขั้นที่สองและรับ web_token เพื่อนำไปใช้ในการเข้าถึงทรัพยากรของเว็บไซต์หรือแอปพลิเคชันต่อไป

การวิจัยนี้จะทำให้ผู้ใช้มีความสะดวกสบายมากขึ้นในการใช้งานระบบสารสนเทศ โดยลดการจำรหัสผ่าน และยากต่อการโดยขโมยและการเดารหัสผ่านมากขึ้น โดยใช้โทรศัพท์มือถือซึ่งนับได้ว่าเป็นอุปกรณ์ที่เป็นของเฉพาะตัวบุคคลนั้นๆ นอกจากนี้ระบบที่พัฒนาขึ้นสามารถพัฒนาใช้กับระบบ SSO ให้ผู้ใช้สามารถเข้าถึงทรัพยากรสารสนเทศที่ต่างระบบกันในองค์กรด้วยโทรศัพท์มือถือเพียงเครื่องเดียวได้ แต่ยังคงความปลอดภัยในระบบสารสนเทศได้อีกด้วย

เอกสารและงานวิจัยที่เกี่ยวข้อง

1. JSON Web Token (JWT)

JWT เป็นมาตรฐานอุตสาหกรรมแบบเปิด RFC 7519 (Jones, Bradley, and Sakimura, 2015) ที่ใช้ในการร้องขอการสื่อสารระหว่างกันบน URL โดยที่ JSON Object จะมีการเข้ารหัสข้อมูลด้วยลายเซ็นดิจิทัล (Digital Signature) ด้วยอัลกอริทึม SHA256 ซึ่งมีความปลอดภัยระดับสูง (Saetang and Boonkrong, 2017) ในการสื่อสารผ่านโปรโตคอล http อีกทั้งยังสามารถร้องขอให้มีการตรวจสอบลายเซ็นสำหรับการยืนยันตัวตนได้อีกด้วย โดยข้อมูล JSON ที่ถูกเข้ารหัสจะเรียกว่า Token โดยสามารถศึกษาได้จากเว็บไซต์ JWT.io ที่ให้บริการการเข้าและถอดรหัสสำหรับตรวจสอบ JWT โดยข้อความจำถูกเข้ารหัส (Encoded) ไปเป็น Token เมื่อนำ Token ไปทำการถอดรหัส (Decoded) จะได้ข้อมูลก่อนการเข้ารหัส ซึ่งแบ่งข้อมูล JSON เป็นสามส่วนได้แก่ 1) Header เป็นส่วนของการอธิบาย (Metadata) ข้อมูลของการสร้าง Token 2) ส่วนของข้อมูล (Playload) เป็นส่วนใช้ในการเก็บข้อมูลที่ต้องการ และ 3) Signature เป็นส่วนที่เก็บรหัสลับ (Secret key) ที่ใช้ในการเข้ารหัส Header และ Playload เข้าด้วยกัน จะสังเกตได้ว่าจะมีรหัสลับซึ่งใช้ในการเข้ารหัส ถ้าการถอดรหัสถูกต้องเว็บไซต์จะตรวจสอบการเข้ารหัสได้ว่า Signature Verified ดังนั้น JWT จึงนิยมนำมาใช้ในการยืนยันตัวตนเนื่องจากมีความน่าเชื่อถือ และปลอดภัย อีกทั้งยังแก้ปัญหา

ของการสื่อสารระหว่าง ไคลเอนต์ (Client) และ เซิร์ฟเวอร์ (Server) ที่ฝั่งของ Server ต้องจดจำการร้องขอสิทธิ์การเข้าถึงทรัพยากรของ Server ซึ่งหน่วยความจำของ Server มีโอกาสเต็มได้ถ้ามีผู้ใช้จำนวนมาก

2. การยืนยันตัวตนแบบ Stateless (Stateless Authentication)

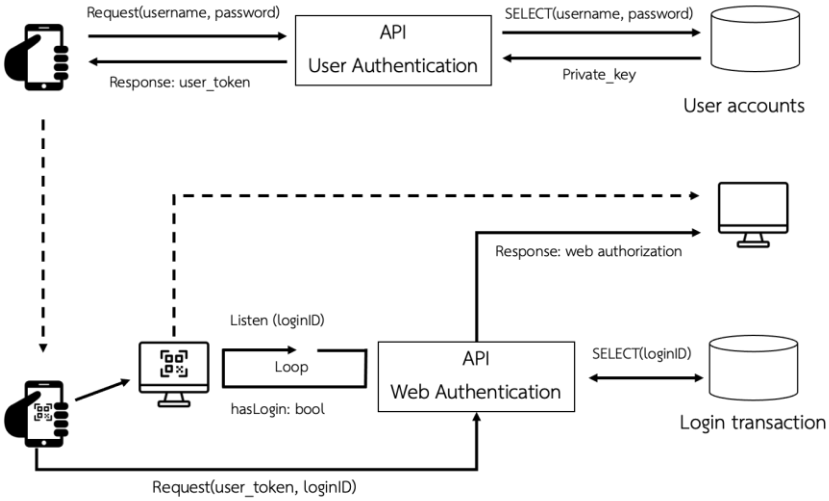
การพัฒนาแอปพลิเคชันจำเป็นจะระบุถึงตัวบุคคลที่กำลังใช้งาน ซึ่งโดยขั้นพื้นฐานผู้ใช้การยืนยันตัวตนด้วย username และ password บนแอปพลิเคชันฝั่ง Client หลังจากผู้ใช้ได้ยืนยันตัวตนแล้ว ระบบจะสร้าง Token ส่งกลับไปให้ Client เก็บไว้ เมื่อผู้ใช้ต้องการเข้าถึงทรัพยากรต่างๆ ของแอพพลิเคชัน Client จะส่ง Token ไปที่แอปพลิเคชันฝั่ง (Server) เพื่อขอรับการอนุญาต (Authorization) ซึ่งโดยวิธีการมาตรฐานทั่วไปจะมีการยืนยันตนสองแบบ ได้แก่ มีการเก็บสถานะ (Stateful) และ ไม่มีการเก็บสถานะ (Stateless) (Mitchell, 2013) โดยวิธี Stateful หลังจากยืนยันตัวตนแล้ว Server จะสร้าง Session ลงในหน่วยความจำเพื่อจดจำผู้ใช้ที่เข้าสู่ระบบ และจะส่ง Token ซึ่งอาจเป็น Cookies กลับมาที่ Client เพื่อใช้ในการร้องขอทรัพยากรของแอปพลิเคชันต่อไป ขณะที่วิธี Stateless ฝั่งของ Server จะไม่มีการจดจำการเข้าสู่ระบบ แต่จะมีมิดเดิลแวร์ (Middleware) ขั้นกลางทำหน้าที่การสร้าง Token พร้อมการเข้ารหัสด้วยคีย์สาธารณะ (Public key) ในรูปแบบ JWT ส่งกลับไปให้ Client เก็บไว้ เมื่อมีการร้องขอ (Request) ทรัพยากรของแอปพลิเคชัน Client จะส่งคำขอพร้อม Token ไปตรวจสอบที่ Middleware หากได้รับอนุญาตจึงจะสามารถเข้าถึงทรัพยากรต่างๆ ได้

การทำให้สถานะของการยืนยันตัวตนที่ผ่านมามีความพยายามทำให้มีขนาดที่เล็กลงเพื่อให้ Server รองรับผู้ใช้จำนวนมาก (Aura and Nikander, 1997) อย่างไรก็ตามเทคโนโลยีในปัจจุบันไม่ได้จำกัดการทำงานกันเพียงระบบ Client-Server โดยเฉพาะเทคโนโลยีเว็บเซอร์วิส (Web services) ซึ่งมีการพัฒนาระบบที่รองรับการสื่อสารขนาดเบา เช่น REST (Representation state transfer) หรือ SOAP (Simple Object Access Protocol) (Lee, Jo, and Kim, 2018) ทำให้มีการใช้การยืนยันตัวตนบนพื้นฐานของ Token ที่มีการเข้ารหัสใช้งานอย่างกว้างขวาง โดยเฉพาะ JWT ได้ถูกนำมาใช้ในการทำการยืนยันตัวตนแบบ Stateless ซึ่งสามารถใช้ได้กับแอปพลิเคชันหลายแพล็ตฟอร์ม และรองรับกับการขยายระบบผู้ใช้จำนวนมาก แต่ก็มีข้อเสียคือต้องมีการตรวจสอบสิทธิ์ทุกครั้ง ซึ่งทำให้ทำงานช้ากว่าการยืนยันตัวตนแบบ Stateful ที่สถานะของ Client ถูกบันทึกไว้ที่ Session ของ Server อย่างไรก็ตามแอปพลิเคชันในปัจจุบันมีหลากหลายแพล็ตฟอร์ม เช่น เว็บแอปพลิเคชัน (Web Application) ไอโอที (IoT) หรือโมบายแอปพลิเคชัน (Mobile Application) ที่ถูกแบ่งการทำงานเป็นส่วนหน้าบ้าน (Front-end) และส่วนหลังบ้าน (Back-end) การใช้การยืนยันตัวตนแบบ Stateful จึงไม่เหมาะสมกับงานดังกล่าว (Lee, Jo, and Kim, 2018; Rahmatullo, Aldya, and Arifin, 2019) ดังนั้นในงานวิจัยนี้จึงเลือกใช้การยืนยันตัวตนแบบ Stateless เป็นพื้นฐานของการระบบการยืนยันตัวตนสองขั้นตอนด้วยคิวอาร์โค้ด

วิธีการวิจัย

การออกแบบระบบการยืนยันตัวตนสองขั้นตอนด้วยคิวอาร์โค้ด แบ่งออกเป็นสองส่วนคือ 1) การยืนตันตัวตนของผู้ใช้งาน และ 2) การยืนตันตัวตนและการอนุญาตสิทธิ์การเข้าเว็บไซต์ แสดงภาพรวมของระบบได้ดังภาพที่ 1

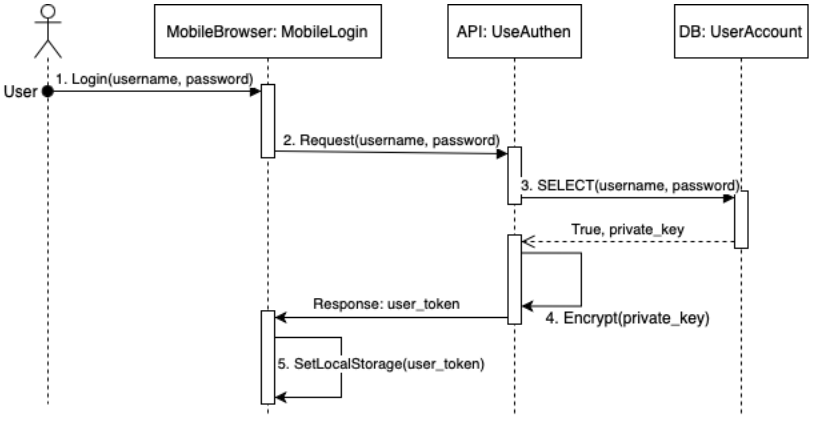
JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY



ภาพที่ 1 ภาพรวมของระบบการยืนยันตัวตนสองขั้นตอนด้วยคิวอาร์โค้ด

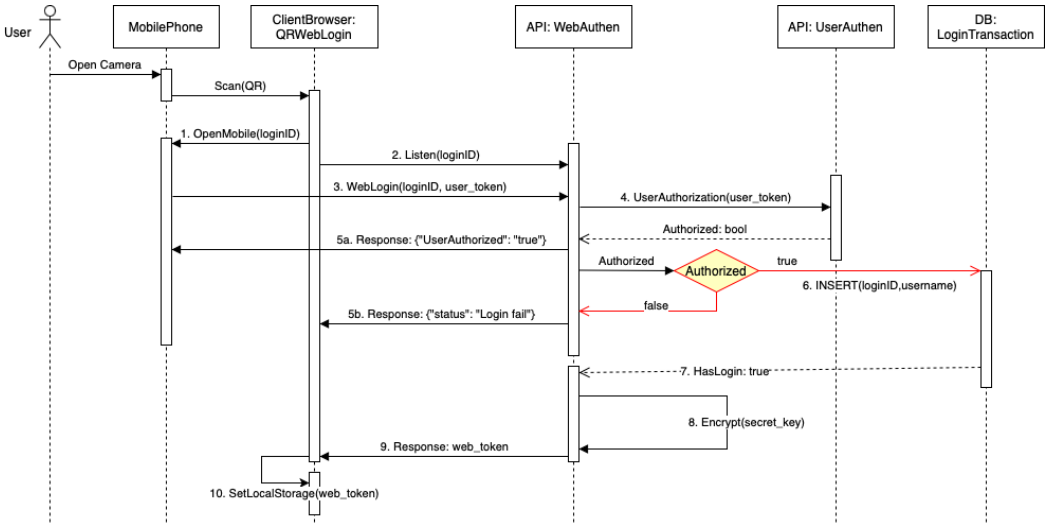
1. การออกแบบการยืนยันตัวตนผู้ใช้ (User Authentication Design)

การยืนยันตัวตนผู้ใช้คือการใช้กระบวนการเข้าสู่ระบบ (1. Login(username, password)) ของผู้ใช้ผ่านอุปกรณ์เคลื่อนที่บนโปรแกรมเบราเซอร์ของอุปกรณ์ (MobileBrowser) ซึ่งในงานวิจัยนี้ใช้วิธีการยืนยันตัวตนแบบ Stateless Authentication (2. Request(username, password)) จากนั้นระบุตัวตนด้วยรหัสผู้ใช้และรหัสผ่านจากฐานข้อมูล (3. SELECT(username and password)) เพื่อขอรับกุญแจส่วนตัว (Private Key) ของผู้ใช้เพื่อนำไปเข้ารหัสข้อมูลแบบ SHA256 (4. Encrypt(private_key)) และส่งข้อมูลกลับให้ผู้ใช้เป็น user_token ตามมาตรฐาน JWT โดย user_token จะถูกจัดเก็บไว้หน่วยความจำภายใน (5. setLocal Storage(user_token)) ของ MobileBrowser โดยการทำงานของขั้นตอนนี้แสดงในแผนภาพลำดับ (Sequence Diagram) ในภาพที่ 2



ภาพที่ 2 แผนภาพลำดับการทำงานของการยืนยันตัวตนผู้ใช้

JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY



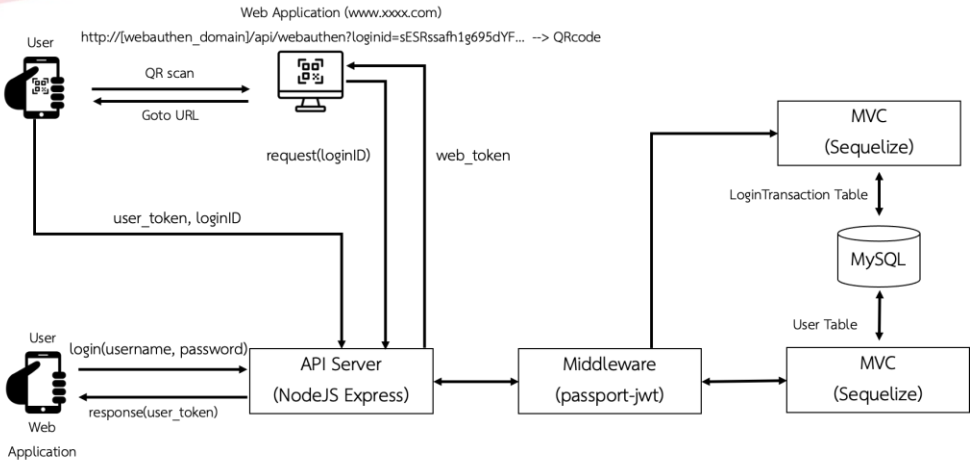
ภาพที่ 3 แผนภาพลำดับการทำงานของการยืนยันตัวตนตัวตนและการอนุญาตบนเว็บไซต์

2. การออกแบบการยืนยันตัวตนและการอนุญาตบนเว็บไซต์ (Web Authentication and Authorization Design)

ในขั้นตอนนี้ผู้ใช้จะใช้กล้องจากอุปกรณ์เคลื่อนที่ในการสแกนรหัสคิวอาร์ที่หน้าเว็บไซต์ที่ต้องการล็อกอิน (ClientBrowser) โดยที่รหัสคิวอาร์ดังกล่าวเป็นการสุ่มค่า loginID จำนวน 30 ตัวอักษร (1. OpenMobile(loginID)) และอุปกรณ์ดังกล่าวต้องทำการยืนยันตัวตนผู้ใช้และได้รับ user_token จากขั้นตอนก่อนหน้า ในขณะเดียวกัน ClientBrowser จะทำการร้องของว่า loginID นี้มีการดำเนินการหรือยัง (2. Listen(loginID)) ซึ่งจะทำการร้องขอทุกๆ 2 วินาที จนกระทั่งมีการดำเนินการยืนยันและอนุญาตแล้วจึงหยุดการร้องขอ จากนั้นจะทำการเปิดหน้าเว็บไซต์พร้อมส่ง loginID และ user_token (3. WebLogin(loginID, user_token)) ไปยัง API เพื่อตรวจสอบการได้รับอนุญาตของผู้ใช้ (4. UserAuthorization(user_token))

กระบวนการถัดมาหลังจากการตรวจสอบผู้ใช้ ถ้าผู้ใช้ได้รับอนุญาต (5a. Authorized: true) จะทำการเพิ่มข้อมูลการล็อกอินลงในฐานข้อมูล LoginTransaction (6. INSERT (loginID, username)) ถ้าไม่ได้รับอนุญาตระบบจะปฏิเสธการร้องขอ (5b. Response ({“status”: “Login Fail”})) และระหว่างที่ ClientBrowser ร้องขอการดำเนินการ ถ้าพบว่ามีข้อมูลการล็อกอินด้วย loginID จากการสแกน (7. HasLogin: true) จะมีการสร้าง JWT โดยการเข้ารหัสด้วยกุญแจลับ (8. Encrypt (Secret Key)) แล้วจะส่ง web_token (9. Response: web_token) กลับพร้อมบันทึก web_token (10. setLocalStorage (web_token)) ลงหน่วยความจำของ ClientBrowser เพื่อไปใช้ในการขออนุญาตในการเข้าใช้เว็บไซต์ต่อไป โดยขั้นตอนทั้งหมดอธิบายดังภาพที่ 3

JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY



ภาพที่ 4 ภาพรวมของการบวนการพัฒนาระบบ

3. กระบวนการในการพัฒนาระบบยืนยันตัวตน

การพัฒนาระบบการยืนยันตัวตนแบบพหุปัจจัยแบ่งออกเป็นการพัฒนา 2 ส่วนได้แก่ ระบบยืนยันตัวตนผู้ใช้ และระบบยืนยันตัวตนและการอนุญาตบนเว็บไซต์ โดยในภาพที่ 4 แสดงขั้นตอนการการพัฒนามีรายละเอียดดังนี้

3.1 การพัฒนาระบบยืนยันตัวตนผู้ใช้ ผู้วิจัยใช้ NodeJS เป็นภาษาในการพัฒนาโปรแกรม โดยมีไลบารี Express สำหรับสร้าง API และใช้ฐานข้อมูล MySQL โดยมีรายละเอียดดังนี้

1) พัฒนาระบบส่วนหน้าบ้าน (Front-end) แบบ Web Application สำหรับการเข้าสู่ระบบ

2) พัฒนาระบบ API ด้วย NodeJS Express เป็นหลังบ้าน (Back-end) เพื่อติดต่อโปรแกรมฝั่งผู้ใช้ในข้อ 1)

3) พัฒนาระบบส่วนติดต่อฐานข้อมูลแบบ MVC (Model View Controller) ด้วยไลบารี Sequelize เพื่อเป็นการตรวจสอบบัญชีผู้ใช้ (login)

4) พัฒนาระบบมิดเดิลแวร์ (Middleware) สำหรับการตรวจสอบและอนุญาตให้เข้าถึงระบบฐานข้อมูลด้วยไลบารี passport-JWT

3.2 การพัฒนาระบบยืนยันตัวตนและการอนุญาตบนเว็บไซต์ เป็นส่วนของระบบการ login ของระบบสารสนเทศที่ต้องการใช้ระบบการยืนยันตัวตนแบบพหุปัจจัย โดยมีขั้นตอนดังนี้

1) พัฒนาระบบ Web Application ที่มีการยืนยันตัวตนแบบพหุปัจจัย โดยหน้า login ให้มีการสร้างรหัส loginID ด้วยการสุ่มตัวอักษรภาษาอังกฤษและตัวเลข จำนวน 30 หลัก เช่น sESRssafh1g695dYF... และให้ส่งไปยัง API ที่ทำการ login เช่นhttp://[webauthen_domain]/api/webauthen?loginid=sESRssafh1g695dYF... จากนั้นนำ URL ที่ได้สร้างเป็นคิวอาร์โค้ด ในขณะเดียวกันก็ให้ Web Application ทำการร้องขอเพื่อรับ (GET) จาก LoginTransaction โดยให้มีการ GET ทุกๆ 2 วินาที

2) เมื่อผู้ใช้นำกล้องของโทรศัพท์มือถือสแกนคิวอาร์โค้ด จะเป็นการลิงก์ไปยัง URL (API) ในข้อ 1) พร้อมทั้งส่ง Token ที่ได้รับจากการ login ไปตรวจสอบสิทธิ์การได้รับอนุญาต

3) พัฒนาระบบมิดเดิลแวร์ (Middleware) เพื่อตรวจสอบการยืนยันตัวตนและการได้รับอนุญาตในการเข้าเว็บไซต์ด้วย passport-jwt จากข้อ 2) จะเป็นการตรวจสอบ Token ของผู้ใช้ (user_token)

JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY

4) พัฒนาระบบ LoginTransaction เพื่อเก็บสถานะการที่ผู้ใช้ login ในข้อ 1) ซึ่งจากข้อ 3) ถ้า user_token ได้รับอนุญาตจะมีการเพิ่มข้อมูลลงในฐานข้อมูล LoginTransaction

5) สอดคล้องกับข้อ 1) ถ้าการร้องขอ LoginTransaction ด้วย loginID และพบว่ามี LoginTransaction ที่เกิดขึ้นจากข้อ 4) ระบบมิดเดิลแวร์จะทำ web_login และสร้าง web_token ด้วยรหัสลับของผู้ใช้ ส่งกลับมายัง Web Application เพื่อนำไปใช้ในระบบ Web Application ต่อไป

4. การออกแบบการทดลองและการวัดประสิทธิภาพ

4.1 การออกแบบการทดลอง

ในงานวิจัยนี้จะทำการวัดประสิทธิภาพการตอบสนองต่อการสื่อสารกันระหว่างผู้ใช้และระบบ API ในการยืนยันตัวตนและการอนุญาตบนเว็บไซต์ โดยการจำลองสถาณการณ์ผู้ใช้จำนวน 30 บัญชี ซึ่งจะทำการเข้าระบบใช้การเข้าสู่ระบบพร้อมกันเพื่อหาเวลาการตอบสนอง (Response Time) ของระบบ มีหน่วยเป็นมิลลิวินาที (ms) โดยทดสอบจำนวน 5 ครั้ง แล้วนำเวลาตอบสนองมาหาค่าเฉลี่ย จากนั้นทำการเพิ่มจำนวนการล็อกอินของผู้ใช้ครั้งละ 30 บัญชี จนถึง 240 บัญชี โดยในการทดลองสนใจเวลาการตอบสนองเป็น 3 ส่วนได้แก่

1) เวลาตอบสนองของการเข้าสู่ระบบของผู้ใช้ (User Login) หมายถึงเวลาตั้งแต่ผู้ใช้ส่ง username และ password เพื่อเข้าสู่ระบบจนถึงเวลาที่ผู้ใช้ได้รับ user_token กลับคืน

2) เวลาตอบสนองของการตรวจสอบการได้รับอนุญาติ (User Authorization) หมายถึง เวลาตั้งแต่ผู้ใช้สแกนรหัส QR เพื่อล็อกอินเข้าสู่เว็บไซต์ จนถึงเวลาที่เพิ่มข้อมูล loginID ลงฐานข้อมูล LoginTransaction เรียบร้อย

3) เวลาตอบสนองการสแกนเข้าสู่ระบบของเว็บไซต์ (Web Login) หมายถึงเวลาตั้งแต่ผู้ใช้สแกนรหัส QR บนหน้าเว็บไซต์ จนถึงเวลาที่เว็บไซต์ได้รับ web_token กลับคืน

4.2 การวัดประสิทธิภาพ

การพัฒนาระบบยืนยันตัวตนสำหรับเว็บแอปพลิเคชันแบบสองขั้นตอนด้วยคิวอาร์โค้ดในงานวิจัยนี้ได้พัฒนาเป็นระบบต้นแบบโดยมีกลุ่มเป้าหมายคือ นักพัฒนาโปรแกรม และนักวิชาการคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏสกลนคร ที่มีหน้าที่ในการพัฒนาระบบสารสนเทศให้กับมหาวิทยาลัยราชภัฏสกลนคร จำนวน 6 คน แบบเจาะจง โดยมีการดำเนินการดังนี้

1) ติดตั้งระบบการยืนยันตัวตนแบบพหุปัจจัยบนเครื่องแม่ข่ายของมหาวิทยาลัย

2) ให้ผู้เชี่ยวชาญข้างต้นทดลองใช้ระบบต้นแบบที่ผู้วิจัยได้พัฒนาขึ้น

3) ให้ผู้เชี่ยวชาญพัฒนาระบบยืนยันตัวตนแบบพหุปัจจัยกับกรณีศึกษาของมหาวิทยาลัย

ในการนี้ทางผู้วิจัยได้ทำการวัดประสิทธิภาพของระบบ ได้แก่ 1) ด้านการออกแบบระบบ 2) ด้านการนำไปประยุกต์ใช้งาน 3) ด้านความเหมาะสมต่อผู้ใช้งาน โดยใช้เครื่องมือแบบสอบถามประเมินประสิทธิภาพของระบบ และวิเคราะห์ด้วยค่าสถิติ ได้แก่ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน โดยนำผลที่ได้ไปเทียบกับเกณฑ์การประเมินของชูศรี วงศ์รัตนะ (2560) ใช้เกณฑ์เดียวกันทั้งการประเมินประสิทธิภาพและความพึงพอใจ ดังนี้

4.50-5.00 หมายถึง ระดับมากที่สุด

3.50-4.49 หมายถึง ระดับมาก

2.50-3.49 หมายถึง ระดับปานกลาง

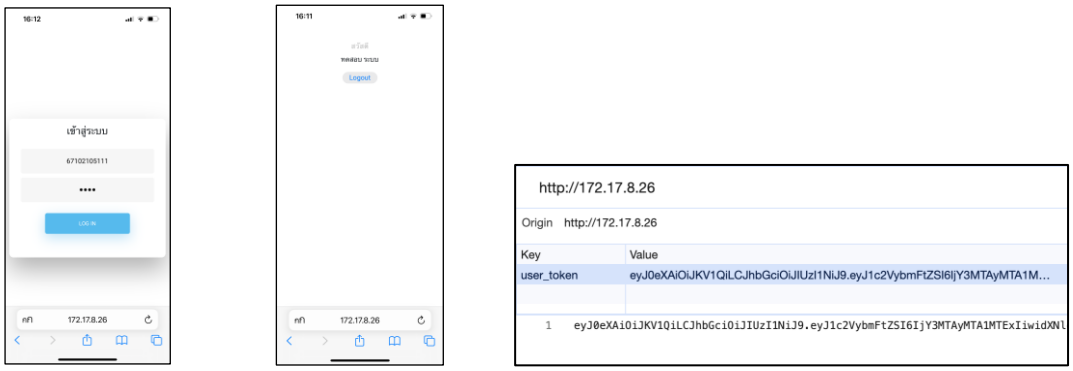
1.50-2.49 หมายถึง ระดับน้อย

1.00-1.49 หมายถึง ระดับน้อยที่สุด

ผลการวิจัย

1. ผลการพัฒนาระบบยืนยันตัวตนผู้ใช้

การยืนยันตัวตนของผู้ใช้จะเกิดขึ้นกรณีที่ผู้ใช้ยังไม่เคยเข้าสู่ระบบมาก่อน ดังนั้นเมื่อผู้ใช้สแกนคิวอาร์โค้ดเพื่อเข้าสู่ระบบเว็บไซต์ ระบบจะเปิดมายังหน้าเข้าสู่ระบบของผู้ใช้ (User Login) ก่อน ดังภาพที่ 5(ก) เมื่อผู้ใช้ป้อนรหัสผู้ใช้ และรหัสผ่าน จะเป็นการยืนยันตัวตนในครั้งแรก หลังจากนั้นจะแสดงหน้าจอที่บอกถึงการยืนยันตัวตนเรียบร้อย (ภาพที่ 5(ข)) แล้วระบบจะส่ง user_token กลับมาให้ผู้ใช้และบันทึกลงหน่วยความจำของบราวสเซอร์ ดังภาพที่ 5(ค)



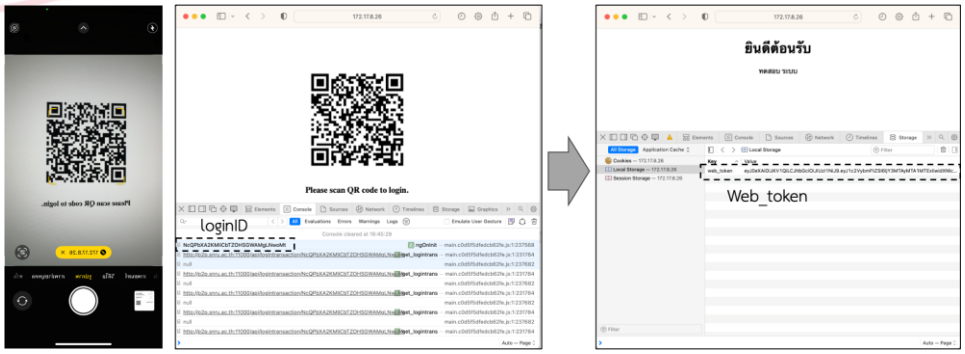
(ก) (ข) (ค)

ภาพที่ 5 ตัวอย่างหน้าจอ User Login (ก) หน้าสำหรับผู้ใช้ล็อกอิน (ข) หน้าจอเมื่อล็อกอินสำเร็จ และ (ค) ผู้ใช้ได้รับ

2. ผลการพัฒนาระบบยืนยันตัวตนและการอนุญาตบนเว็บไซต์

เมื่อผู้ใช้ทำการยืนยันตัวตนในขั้นแรกแล้วจะได้รับ user_token มาเก็บไว้ที่เครื่องแล้ว ผู้วิจัยได้จำลองเว็บไซต์โดยใช้การล็อกอินแบบ Stateless โดยมีเพจแรกเป็นเพจสำหรับการล็อกอินแบบคิวอาร์โค้ด ดังภาพที่ 6 หลังจากนั้นผู้ใช้จะต้องทำการล็อกอินโดยใช้โทรศัพท์สแกนคิวอาร์โค้ดดังกล่าวซึ่งคิวอาร์โค้ดจะมีข้อมูล loginID จากนั้นฝั่งของผู้ใช้จะส่ง loginID พร้อมทั้ง user_token ไปยัง WebAuthen API เพื่อตรวจสอบการได้รับอนุญาติ (Authorization) ของผู้ใช้ ถ้าผู้ใช้ได้รับอนุญาต ระบบจะสร้าง web_token ส่งกลับมาให้เว็บไซต์ เพื่อนำไปใช้งานใช้ในเว็บไซต์ต่อไป

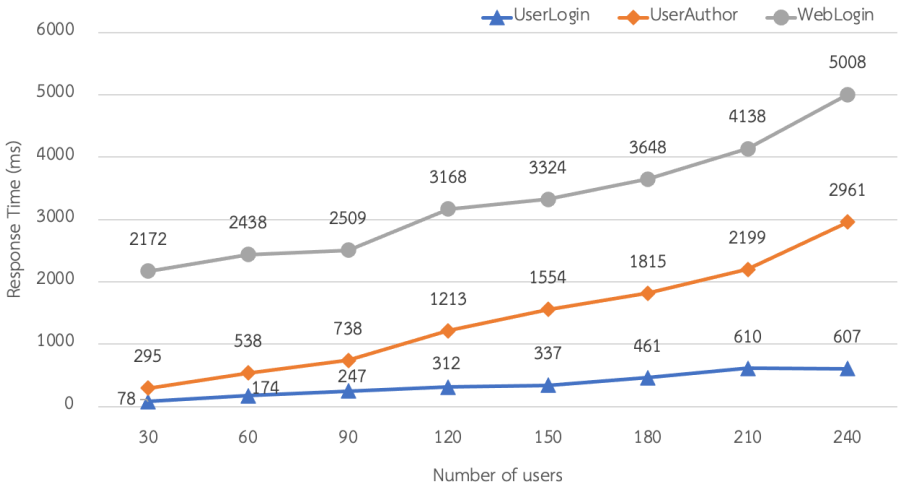
JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY



ภาพที่ 6 ตัวอย่างการเข้าสู่ระบบโดยด้วยคิวอาร์โค้ด

3. ผลการการทดสอบระบบ

3.1 การทดสอบเพื่อหาค่าเวลาตอบสนองของระบบ ภาพที่ 7 แสดงถึงเวลาตอบสนองเฉลี่ยของหนึ่งบัญชีมีหน่วยเป็นมิลิวินาที จากภาพเป็นผลเฉลี่ยของการทดสอบจำนวน 5 ครั้ง โดยมีการล็อกอิน 30 ถึง 240 บัญชี ผลที่ได้แสดงให้เห็นเวลาของการทำ User Login จะใช้เวลาน้อยที่สุด โดยเฉลี่ยหนึ่งบัญชีไม่เกิน 1 วินาที เนื่องจากขั้นตอนนี้ระบบทำงานเพียงแค่หน้าที่เดียว คือ การล็อกอินแล้วสร้าง user_token ส่งกลับ ในขณะที่ของ User Authorization จะมีการทำงานหลายขั้นตอนมากกว่า ได้แก่ การตรวจสอบสิทธิผู้ใช้ และการเพิ่มข้อมูล loginID ลงฐานข้อมูล โดยเวลาที่ใช้ได้จะสังเกตได้ว่าเมื่อมีผู้ใช้มากขึ้น เวลาตอบสนองมีแนวโน้มการเติบโตแบบเอ็กซ์โพเนนเชียล (Exponential) ในทำนองเดียวกันกับเวลาตอบสนองของ Web Login จะเห็นได้ว่าใช้เวลาตอบสนองนานที่สุดเนื่องจากระบบออกแบบไว้ให้รอ เพื่อสอบถาม loginID (Linster(loginID)) จากฐานข้อมูล LoginTransaction ทุกๆ 2 วินาที ทำให้อัตราการเติบโตของเวลาตอบสนองเพิ่มมากขึ้นเช่นเดียวกับการทำ User Authorization



ภาพที่ 7 ผลการทดสอบเวลาตอบสนอง (Response Time) ของระบบ

4. ผลประเมินประสิทธิภาพ

ผลการประเมินจากแบบสอบถามจากผู้เชี่ยวชาญซึ่งเป็นโปรแกรมเมอร์และมีหน้าที่ในการพัฒนาระบบสารสนเทศให้กับมหาวิทยาลัย จำนวน 6 คน โดยการประเมินประสิทธิภาพของระบบระบบยืนยันตัวตนสำหรับเว็บแอปพลิเคชันแบบพหุปัจจัยได้ผลการประเมินดังตารางที่ 1 ซึ่งในด้านการออกแบบระบบ ประเมินเกี่ยวกับความเข้าใจ ประสิทธิภาพของการนำไปใช้จริง และความปลอดภัยของระบบ พบว่ามีผลคะแนนเฉลี่ยที่ 4.44 คะแนน อยู่ในระดับมาก ในด้านที่สองการนำไปประยุกต์ใช้งาน ซึ่งเกี่ยวกับความเหมาะสม และความยาก-ง่าย ต่อนักพัฒนาระบบสานสนเทศนำไปปรับใช้กับงานจริง พบว่ามีผลคะแนนที่ 4.38 คะแนน อยู่ในระดับมาก และด้านความเหมาะสมต่อผู้ใช้งานสอบถามเกี่ยวกับความเห็นของผู้เชี่ยวชาญว่าเมื่อมีการนำระบบที่พัฒนาขึ้นไปใช้จริงจะมีความเหมาะสมหรือความสะดวกสบายต่อผู้ใช้ระบบเพียงใด ผลการประเมินพบว่ามีคะแนนเฉลี่ยที่ 4.67 คะแนน อยู่ในระดับมากที่สุด ซึ่งประสิทธิภาพโดยรวมที่ระดับคะแนน 4.50 อยู่ในระดับมากที่สุด

5. การวิเคราะห์และการอภิปรายผลการทดลอง

การทดสอบประสิทธิภาพของระบบที่พัฒนาขึ้นได้จำลองสถานการณ์ให้มีการใช้งานของผู้ใช้พร้อมกันซึ่งอาจเกิดขึ้นได้จำนวนมากภายในช่วงเวลาหนึ่ง ซึ่งทางผู้วิจัยได้การทดสอบระบบโดยใช้การเขียนโปรแกรมด้วยภาษา JavaScript ที่ทำงานแบบ Synchronous โดนแต่ละคำสั่งในการเรียกใช้ API ไม่ต้องรอให้เสร็จแต่จะทำไปพร้อมๆ กัน ดังนั้นในการทดสอบผู้ใช้ในการใช้งานระบบจึงมีความใกล้เคียงกับสถานการณ์จริงมากที่สุด โดยผลทดสอบเป็นเวลาเฉลี่ยต่อ 1 ผู้ใช้ ซึ่งจะเห็นได้ว่าเวลาตอบสนองจะเพิ่มตามจำนวนผู้ใช้ที่เข้าระบบพร้อมๆ กัน จากภาพที่ 7 จะเห็นได้ว่ากราฟทั้ง 3 เส้น หลังจากผู้ใช้ที่มากกว่า 90 บัญชี จะมีแนวโน้มเติบโตแบบเอ็กซ์โพเนนเชียล ผู้วิจัยจึงวิเคราะห์ได้ว่าระบบที่พัฒนาขึ้นสามารถรองรับผู้ใช้ที่เหมาะสมได้ถึง 90 บัญชีพร้อมๆ กัน โดยใช้เวลาเฉลี่ยต่อ 1 ผู้ใช้ ในทั้ง 3 ขั้นตอนประมาณ 4 วินาที

การประเมินประสิทธิภาพของระบบที่พัฒนาขึ้นโดยการให้ผู้เชี่ยวชาญทั้ง 6 คน ได้ทดลองใช้ระบบต้นแบบ อีกทั้งได้ประยุกต์ใช้ระบบการยืนยันตัวตนแบบพหุปัจจัยที่พัฒนาขึ้นเพื่อนำไปใช้กับระบบสารสนเทศของมหาวิทยาลัย ซึ่งผลที่ได้จะเห็นได้น่าจะแก้ปัญหาของการต้องจำรหัสผ่านหลายรหัสที่มีความเหมาะสมต่อผู้ใช้ถึง 4.67 คะแนน อยู่ในระดับมากที่สุด ขณะที่ความเห็นของการนำไปประยุกต์ใช้อยู่ที่ 4.38 คะแนน เนื่องจากวิธีการยืนยันตัวตนที่นำเสนอยังเป็นวิธีการที่ยังไม่ได้นำมาใช้กับระบบสารสนเทศของมหาวิทยาลัย

ตารางที่ 1 ผลการประเมินประสิทธิภาพ

รายการประเมินประสิทธิภาพ	$\overline{X}$	*SD*	ผลการประเมิน
ด้านการออกแบบระบบ	4.44	0.49	มาก
ด้านการนำไปประยุกต์ใช้งาน	4.38	0.46	มาก
ด้านความเหมาะสมต่อผู้ใช้งาน	4.67	0.57	มากที่สุด
เฉลี่ย	4.50	0.51	มากที่สุด

สรุปผลการวิจัย

ระบบยืนยันตัวตนสำหรับเว็บแอปพลิเคชันแบบพหุปัจจัยที่พัฒนาพัฒนาขึ้น เป็นระบบที่ช่วยแก้ปัญหาผู้ใช้ของผู้ใช้ที่มักจะลืมรหัสผ่าน และป้องกันการขโมยรหัสผ่านเข้าระบบ โดยใช้โทรศัพท์มือถือซึ่งเป็นอุปกรณ์ส่วนบุคคลในการยืนยันตัวตนชั้นแรก และใช้การสแกนรหัส QR เพื่อล็อกอินเข้าสู่เว็บไซต์เป็นการยืนยันตนชั้นที่สอง โดยผลของการทดสอบเวลาตอบสนองของระบบที่พัฒนาขึ้น แสดงให้เห็นถึงการรองรับปริมาณการใช้งานพร้อมๆ กันได้หลายคน แม้ว่าการทดสอบเพื่อหาเวลาในการตอบสนองของระบบจะขึ้นอยู่กับปัจจัยหลายอย่าง เช่น ความเร็วของอินเทอร์เน็ต สภาพการจราจรของระบบเครือข่ายคอมพิวเตอร์ หรือฮาร์ดแวร์และซอฟต์แวร์ของระบบ API และ ระบบฐานข้อมูล เป็นต้น แต่ผลการทดสอบแสดงให้เห็นถึงแนวโน้มของความเร็วในการตอบสนองในการล็อกอินของผู้ใช้ได้พร้อมกันจำนวนมากๆ ในขณะที่ผลการประเมินจากแบบสอบถามที่สนใจกลุ่มของโปรแกรมเมอร์และนักพัฒนาระบบสารสนเทศของมหาวิทยาลัยราชภัฏสกลนครจำนวน 6 คน พบว่าประสิทธิภาพของการออกแบบและการเหมาะสมกับผู้ใช้อยู่ในระดับมากที่สุด และประสิทธิภาพของการนำไปประยุกต์ใช้งานอยู่ในระดับมาก

ข้อเสนอแนะ

ระบบยืนยันตัวตนแบบสองขั้นตอนด้วยคิวอาร์โค้ดเพื่อใช้กับการล็อกอินเข้าสู่เว็บไซต์ยังคงมีข้อจำกัดในการที่หน้าเว็บไซต์ที่ต้องการล็อกอินจำเป็นต้องร้องขอ Login Transaction รอทุกๆ 2 วินาที อาจเป็นผลทำให้เกิดความหนาแน่นของการการจราจรบนระบบเครือข่ายหากมีผู้ใช้จำนวนมากๆ ขณะรอเพื่อสแกนเข้าสู่ระบบ ผู้เชี่ยวชาญจึงมีข้อเสนอแนะให้มีการกำหนดเวลาของ loginID ซึ่งเมื่อหมดเวลาระบบจะหยุดร้องขอ Login Transaction และให้ผู้ใช้ขอ loginID ใหม่อีกครั้ง นอกจากนี้ในการนำไปใช้งานจริงในมหาวิทยาลัยราชภัฏสกลนคร มีแนวโน้มความเป็นไปได้ที่จะนำระบบนี้มาประยุกต์ใช้กับระบบสารสนเทศใหม่ๆ ของมหาวิทยาลัย เนื่องจากผู้เชี่ยวชาญมีความเห็นสอดคล้องไปในเชิงบวก ซึ่งผู้วิจัยจะผลักดันให้มีการนำไปใช้งานจริงต่อไป

เอกสารอ้างอิง

ชูศรี วงศ์รัตนะ. (2560). **เทคนิคการใช้ สถิติเพื่อการวิจัย.** กรุงเทพฯ: อมรการพิมพ์.

Aura, T., and Nikander, P. (1997). Stateless connections. Lecture Notes in Computer Science, 1334. **Springer**, Berlin, Heidelberg.

Bunaramrueang, P., and Kowpatanakit, P. (2023). Digital identity and authentication. **Thammasa Law Journal**, 52(4), pp. 1035-1097.

Chaimueng C., Puangpronpitag, S., and Pongsiri, V. (2012) Single point authentication by multiple factor authentication. **Journal of information science and technology**, 3(1), pp. 53–62.

Jones, M., Bradley, J., and Sakimura, N. (2015). JSON Web Token (JWT). **RFC 7519**, DOI 10.17487/RFC7519.

Lee, S., Jo, J. Y., and Kim, K. (2018). Authentication System for Stateless RESTful Web Service. **Journal of Computational Methods in Sciences and Engineering**, 17, pp. 1-14, DOI: 10.3233/JCM-160677.

Mitchell, C. (2013). A Novel Stateless Authentication Protocol. **Lecture Notes in Computer Science**, vol 7028. Springer, Berlin, Heidelberg.

JSET LRU
วารสารวิทยาศาสตร์ วิศวกรรมศาสตร์ และเทคโนโลยี
มหาวิทยาลัยราชภัฏเลย
Journal of Science, Engineering and Technology
LOEI RAJABHAT UNIVERSITY

Rahmatullo, A., Aldya, A. P., and Arifin, M. N. (2019). Stateless authentication with JSON Web Tokens using RSA-512 Algorithm. **INFOTEL**, 11(2), pp. 36-42, DOI: 10.20895/infotel.v11i2.427

Rukpakavong, W., Subsomboon, K., and Nilpanich, S. (2022). Mutual authentication for cardless ATM withdrawal using location factor. **SNRU Journal of Science and Technology**, 14(2), pp. 1-8, DOI: https://doi.org/10.55674/snrujst.v14i2.245396

Sainui, J., Jankaew, N., and U-seng, H. (2021). A prototype of seminar registration system using face authentication. **Journal of Applied Information Technology**, 7(2), pp. 40-50.

Sarawan, K. (2018). Improving Web application security by virtual password Authentication. **TNI Journal of Engineering and Technology**, 6(1), pp. 19-23.

Saetang, W., and Boonkrong, S. (2017). Effectiveness Analysis and hash function. **Journal of Food Health and Bioenvironment Science**, 10(2), pp. 81-94.

Titiakarawongse, C., and Boonkrong, S. (2023). A Study of password management behaviors of young People. **Applied Science and Engineering Progress**, 16(4), pp. 1-16, DOI: 10.14416/j.asep.2023.01.001.

Thumsiraruk, P., and Puangpronpitag, S. (2015). Problem analysis and security testing of one time password. **Technology**, (37)1, pp. 10-24.

Vongsingthong, S., Paiboonsak, J., and Nakaresruengsak, S. (2023). Machine learning in biometric authentication. **Science and technology journal Mahasarakham university**, 42(4), pp 97-107.