Table of Contents

[1 บทที่ 1 บทนำ 1](#_Toc418961938)

[1.1 หลักการและเหตุผล 1](#_Toc418961939)

[1.2 วัตถุประสงค์ของโครงงาน 2](#_Toc418961940)

[1.3 ประโยชน์ที่จะได้รับจากการศึกษาเชิงประยุกต์และ/หรือ เชิงทฤษฏี 2](#_Toc418961941)

[1.4 ขอบเขตของโครงงาน/วิธีการวิจัย 2](#_Toc418961942)

[1.4.1 ขอบเขตของสถาปัตยกรรม 2](#_Toc418961943)

[1.4.2 ขอบเขตของระบบงาน 2](#_Toc418961944)

[1.4.3 ขอบเขตของข้อมูล 2](#_Toc418961945)

[2 บทที่ 2 หลักการและทฤษฏีที่เกี่ยวข้อง 3](#_Toc418961946)

[2.1 ทีแอลเอส (TLS) หรือชื่อเดิม เอสเอสแอล 3](#_Toc418961947)

[2.2 เรเดียส (RADIUS) 5](#_Toc418961948)

[2.3 คำสั่งบนเทอร์มินอลที่จำเป็นสำหรับลินุกซ์ 5](#_Toc418961949)

[2.3.1 คำสั่งจัดการกับไฟล์ 5](#_Toc418961950)

[2.3.2 คำสั่งทำงานกับข้อมูลอักขระภายในไฟล์ 6](#_Toc418961951)

[2.3.3 คำสั่งทำงานกับระบบปฏิบัติการ 7](#_Toc418961952)

[2.3.4 คำสั่งเสริมที่จำเป็น 8](#_Toc418961953)

[2.4 ซิงเกิลไซน์ออน (Single Sign-on) 8](#_Toc418961954)

[2.4.1 รูปแบบของซิงเกิลไซน์ออน 8](#_Toc418961955)

[**รูปที่ 2.2 การส่ง-ผ่านข้อมูลของเครื่องแม่ข่ายโปรแกรม ผู้ใช้ และ ศูนย์กลางกระจายกุญแจ** 9](#_Toc418961956)

[**รูปที่ 2.3 การส่งผ่านข้อมูลของ ผู้ใช้ ผู้ให้บริการ และ ผู้ให้บริการตรวจสอบยืนยันตัวตน** 10](#_Toc418961957)

[**รูปที่ 2.4 การส่งข้อมูลของซิงเกิลไซน์ออนบนพื้นฐานรวมของแซมแอล และเคอร์เบอร์รอส** 11](#_Toc418961958)

[**2.5 เทคโนโลยีการยืนยันตัวตนนักศึกษา ที่มีใช้งานในมหาวิทยาลัยเชียงใหม่** 11](#_Toc418961959)

[**2.5.1** **เรเดียส ( RADIUS )** 11](#_Toc418961960)

[**รูปที่ 2.5 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและบริการเรเดียสของสำนักบริการเทคโนโลยี** 12](#_Toc418961961)

[**2.5.2** **เอพีไอ ( API )** 12](#_Toc418961962)

[โดยค่าของ ticket จะได้ก็ต่อเมื่อการร้องขอสำเร็จคือ ค่าของ success เป็นจริง 14](#_Toc418961963)

[**รูปที่ 2.6 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและเอพีไอของสำนักบริการเทคโนโลยี** 15](#_Toc418961964)

[2.5 15](#_Toc418961965)

รูปที่ 2.1 แสดงการส่งข้อมูลบนทีแอลเอสระหว่างลูกข่ายและแม่ข่าย 4

รูปที่ 2.2 การส่ง-ผ่านข้อมูลของเครื่องแม่ข่ายโปรแกรม ผู้ใช้ และ ศูนย์กลางกระจายกุญแจ 9

รูปที่ 2.3 การส่งผ่านข้อมูลของ ผู้ใช้ ผู้ให้บริการ และ ผู้ให้บริการตรวจสอบยืนยันตัวตน 10

รูปที่ 2.4 การส่งข้อมูลของซิงเกิลไซน์ออนบนพื้นฐานรวมของแซมแอล และเคอร์เบอร์รอส 11

รูปที่ 2.5 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและบริการเรเดียสของสำนักบริการเทคโนโลยี 12

รูปที่ 2.6 แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและเอพีไอของสำนักบริการเทคโนโลยี 15

ตารางที่ 2.1ตารางแสดงคำสั่งบนโปรแกรม Vi 7

# บทที่ 1 บทนำ

โมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ ช่วยจัดการการเข้าใช้งานของนักศึกษา อาจารย์ แต่ละผู้ใช้จะมีข้อมูลส่วนตัวที่ไม่เหมือนกัน สามารถใช้ยืนยันตัวตนผู้ใช้กับระบบได้ เช่น นักศึกษา มี รหัสนักศึกษาของแต่ละคน ชื่อผู้ใช้ของอีเมลโดเมนของมหาวิทยาลัยเชียงใหม่ ส่วนอาจารย์ มีชื่อผู้ใช้งานของแต่ละคน ซึ่งในบทนี้จะกล่าวถึงภาพรวมของการจัดทำโครงงานดังนี้ ได้แก่ หลักการและเหตุผล วัตถุประสงค์ของโครงงาน ขอบเขต ประโยชน์ของการทำโครงงานนี้ และแผนการดำเนินงานและระยะเวลาดำเนินงานในการจัดทำระบบ

## หลักการและเหตุผล

ระบบสารสนเทศสำหรับส่งการบ้านปฏิบัติการของภาควิชาวิทยาการคอมพิวเตอร์ เป็นระบบช่วยการเรียนการสอนปฏิบัติการเพื่อ เพิ่มความสะดวกแก่การทำงานกับเอกสารอิเล็กทรอนิกส์ ในแต่ละวิชาผู้สอนสามารถให้ นักศึกษาทำงานแต่ละปฏิบัติการ ส่งภายในระหว่างการเรียน หรือนอกเวลา ช่วยจัดเก็บเพิ่มความสะดวกต่อการตรวจงานของอาจารย์ และ การจัดการเอกสารภายในระบบ

แต่เดิมระบบส่งการบ้านสำหรับปฏิบัติการ ของภาควิชาวิทยาการคอมพิวเตอร์ ใช้การแจกรหัสตัวเลขเฉพาะให้นักศึกษา และอาจารย์แต่ละคนเพื่อเข้าใช้งานระบบ ปัญหาที่เกิดคือ นักศึกษาบางคนลืมรหัส หรือ การขโมยรหัสเข้าใช้งานเพื่อสร้างความเสียหายเปลี่ยนแปลงข้อมูลบนระบบของเจ้าของรหัส

ด้วยเหตุนี้โครงงานจึงได้มุ่งเน้นที่จะปรับปรุงระบบให้นักศึกษาเข้าใช้ระบบโดยใช้ บัญชีผู้ใช้ไอที (IT Account) ที่มีโดเมนของมหาวิทยาลัยเชียงใหม่ และรหัสผ่านของบัญชีผู้ใช้ไอทีเพื่อนักศึกษาจำได้ง่าย ไม่ต้องจดจำรหัสเพิ่มซึ่งการที่จะเชื่อมต่อยืนยันตัวตนกับระบบ แบบใช้บัญชีผู้ใช้ไอทีนั้นมีความจำเป็นที่จะต้องแลกเปลี่ยนข้อมูลระหว่าง เรเดียสเซิร์ฟเวอร์ (RADIUS Server) หรือ เอพีไอ(API) กับทางสำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่ โดยทางระบบจะต้องส่งข้อมูลเข้าที่จำเป็นเช่น อีเมลและรหัสผ่าน และ ข้อมูลที่คาดหวังกลับมา เช่น การยืนยันว่านักศึกษาได้ให้อีเมลและรหัสผ่านถูกต้อง ข้อมูลนักศึกษาที่จำเป็น เช่น ชื่อ-นามสกุล ไทย อังกฤษ รหัสนักศึกษา สถานะ และข้อมูลอื่นที่จำเป็น นอกจากนั้น ยังต้องเพิ่มเพิ่มความปลอดภัยต่อการเข้าสู่ระบบและส่งผ่านข้อมูล โดยใช้โครงสร้างพื้นฐานในการส่งข้อมูลที่มีความปลอดภัย เอสเอสแอล(SSL)

## วัตถุประสงค์ของโครงงาน

จัดทำโมดูลยืนยันตัวตนของระบบจัดการการส่งการบ้านปฏิบัติการ โดยยืนยันตัวตนผู้ใช้งานจาก บัญชีผู้ใช้ไอที ที่เป็นโดเมนของมหาวิทยาลัยเชียงใหม่ และรหัสผ่านเดียวกันกับส่วนกลาง

## ประโยชน์ที่จะได้รับจากการศึกษาเชิงประยุกต์และ/หรือ เชิงทฤษฏี

- การติดตั้ง ตั้งค่าปรับแต่งเครื่องแม่ข่ายบนระบบลินุกซ์โครงสร้างพื้นฐานด้านการส่งข้อมูลที่มีความปลอดภัยของระบบจัดการสารสนเทศสำหรับส่งการบ้านปฏิบัติการที่ใช้อยู่

- ความรู้การเชื่อมต่อเพื่อยืนยันตัวตนโดยใช้ เรเดียสเซอร์วิส (RADIUS service) และ เอพีไอ

- การส่งผ่านข้อมูลแบบปลอดภัยผ่านเครือข่ายอินเทอร์เน็ตประสานระหว่างผู้ใช้งาน

## ขอบเขตของโครงงาน/วิธีการวิจัย

### ขอบเขตของสถาปัตยกรรม

ระบบที่ทำการทดลองใช้งานก่อนติดตั้งจริงทำงานบนระบบอินเทอร์เน็ต

1. ฮาร์ดแวร์ (Hardware) ที่ใช้ในการพัฒนาระบบประกอบด้วย

- เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เฮชพี (HP) ใช้เป็นเครื่องแม่ข่าย

- หน่วยประมวลผล (CPU) อินเทลคอร์ 2 ควอด 2.00 กิกะเฮิร์ตซ์ (Intel Core 2 Quad 2.00 GHz)

- ฮาร์ดดิสก์ (Harddisk) ขนาดความจุ 250 กิกะไบต์

1. ซอฟต์แวร์ (Software) ที่ใช้ในการพัฒนาระบบประกอบด้วย

- เครื่องแม่ข่ายติดตั้ง ระบบปฏิบัติการลินุกซ์ อุบุนตุ ระบบทำงานผ่านอินเทอร์เน็ต

- การเข้าสู่ระบบและส่งผ่านข้อมูลเพื่อความปลอดภัยโดยใช้เอสเอสแอล

### ขอบเขตของระบบงาน

- ติดตั้งปรับแต่งระบบความปลอดภัยสำหรับเครื่องแม่ข่ายระบบจัดการสารสนเทศสำหรับปฏิบัติการ

- ติดตั้งโครงสร้างพื้นฐานความปลอดภัยในการส่งข้อมูล

- ทำการเชื่อมต่อกับระบบจัดการการส่งการบ้านปฏิบัติการเพื่อพิสูจน์ตัวตนผ่านระบบ บัญชีผู้ใช้ไอทีเดียวกันกับของมหาวิทยาลัยเชียงใหม่

### ขอบเขตของข้อมูล

- บัญชีผู้ใช้อีเมล ที่เป็นโดเมนมหาวิทยาลัยเชียงใหม่ และรหัสผ่านจากนักศึกษาผู้ใช้งานระบบ

- ข้อมูลจากผู้ดูแลระบบ และคณาจารย์ภาควิชาวิทยาการคอมพิวเตอร์

- รายละเอียดของนักศึกษา ข้อมูลนักศึกษาได้มาจาก สำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่ ผ่านทาง เรเดียสเซอร์วิส และเอพีไอ

# บทที่ 2 หลักการและทฤษฏีที่เกี่ยวข้อง

การปรับปรุงโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ โดยการปรับปรุงใหม่นั้นจำเป็นต้องใช้บัญชีผู้ใช้ไอทีของทางมหาวิทยาลัย ทำให้ต้องปรับปรุงทางด้านความปลอดภัยต่อการใช้งานของนักศึกษา อาจารย์ และ ผู้ดูแลระบบโดยการใช้เอสเอสแอล (SSL) ในการแลกเปลี่ยนข้อมูล เพื่อความปลอดภัยสูง ตรวจความถูกต้องของบัญชีผ่านเครื่องแม่ข่ายเรเดียส (RADIUS) และรับข้อมูลรายละเอียดนักศึกษาได้รับจากเอพีไอ (API) ของทางสำนักบริการเทคโนโลยีสารสนเทศมหาวิทยาลัยเชียงใหม่

## ทีแอลเอส (TLS) หรือชื่อเดิม เอสเอสแอล

เอสเอสแอลโพรโทคอลรักษาความปลอดภัย เพื่อให้โปรแกรมบนเครื่องแม่ข่ายและเครื่องลูกข่ายเชื่อมต่อส่งผ่านข้อมูลระหว่างเครือข่ายอย่างปลอดภัย โดยถูกออกแบบมาเพื่อป้องกันการถูกดักจับข้อมูล การใช้งานจริง ทีแอลเอส หรือ เอสเอสแอล ถูกนำมาประยุกต์กับโพรโทคอลในชั้นสื่อสารทรานสปอร์ต (Transport Layer Protocols) ห่อหุ้มโพรโทคอลที่ใช้งาน เช่น เฮสทีทีพี (HTTP) เอฟทีพี (FTP) เอสเอมทีพี (SMTP) โดยปกติมักถูกใช้บนเว็บที่ต้องการความปลอดภัยเข้าใช้งานของผู้ใช้งาน และเว็บซื้อขายบนอินเทอร์เน็ต เครื่องแม่ข่ายและลูกข่ายจะสามารถใช้เอสเอสแอล ได้เมื่อมีการตกลงที่จะใช้เหมือนกัน คือ วิธีการจับมือกัน (Handshake) โดยระหว่างการจับมือทั้งเครื่องแม่ข่ายและลูกข่ายต้องตกลงกันในแต่ละเงื่อนไขเพื่อความปลอดภัยของการเชื่อมต่อโดยมีขั้นตอนดังนี้

1. เครื่องลูกข่ายส่ง หมายเลขรุ่นของเอสเอสแอล รายละเอียดการตั้งค่าเข้ารหัส (Cipher Settings) ข้อมูลของช่องสื่อสาร (Session) ที่ได้รับ และข้อมูลจำเป็นอื่นที่แม่ข่ายต้องใช้ติดต่อกับเครื่องลูกข่ายผ่านเอสเอสแอล
2. เครื่องแม่ข่ายส่ง หมายเลขรุ่นของเอสเอสแอล รายละเอียดการตั้งค่าเข้ารหัส ข้อมูลของช่องสื่อสาร ที่ส่งไป ข้อมูลอื่นที่ลูกข่ายต้องใช้ติดต่อกับเครื่องแม่ข่ายผ่านเอสเอสแอล ทั้งส่งหนังสือรับรอง (Certificate) ของแม่ข่าย และถ้าหากเครื่องลูกข่ายร้องขอทรัพยากรของแม่ข่ายเพื่อการยืนยันตัวตนบนระบบ เครื่องแม่ข่ายจะร้องขอหนังสือรับรอง จากเครื่องลูกข่ายด้วย
3. เครื่องลูกข่ายใช้ข้อมูลที่ได้มาจากแม่ข่ายเพื่อยืนยันตัวตนเครื่องแม่ข่าย ยกตัวอย่างเช่น เว็บเบราว์เซอร์(Web Browser) เชื่อมต่อกับเครื่องแม่ข่าย ตรวจสอบหนังสือรับรองที่ได้รับว่าชื่อแม่ข่ายตรงกับที่ได้รับเชื่อถือหนังสือรับรองได้หรือไม่ หนังสือรับรองหมดอายุแล้วหรือไม่ ถ้าไม่สามารถยืนยันเครื่องแม่ข่ายได้จึงเตือนผู้ใช้ว่าเชื่อมต่อไม่ได้ หรือ สามารถยืนยันแม่ข่ายได้ถูกต้องก็ดำเนินการขั้นต่อไป
4. จากข้อมูลทั้งหมดในกระบวนการจับมือ เครื่องลูกข่ายต้องสร้างรหัสลับพื้นฐาน (Pre-master secret) สำหรับช่องสื่อสารปัจจุบัน เข้ารหัสด้วยกุญแจสาธารณะ (Public Key) ที่ได้จากเครื่องแม่ข่ายในขั้นตอนที่ 2 จากนั้นจึงส่งรหัสลับพื้นฐานที่ถูกเข้ารหัสให้กับแม่ข่าย
5. (กรณีเครื่องแม่ข่ายร้องขอการยืนยันตัวตนจากลูกข่าย) เครื่องลูกค่ายต้องสร้างข้อมูลอื่นซึ่งจะเป็นที่เด่นชัดว่าเป็นเครื่องที่ควรส่งข้อมูลหากันอยู่จริง ซึ่งกรณีนี้เครื่องลูกข่ายต้องส่งเอกสารใหม่ พร้อมใบรับรองเครื่อง และส่งรหัสลับพื้นฐานที่ถูกเข้ารหัสให้กับแม่ข่าย
6. (กรณีเครื่องแม่ข่ายร้องขอการยืนยันตัวตนจากลูกข่าย) เครื่องแม่ข่ายยืนยันลูกข่ายว่าเข้าใช้งานได้
   1. ถ้าไม่สามารถยืนยันตัวตนของลูกข่ายให้ทำการปิดช่องสื่อสารกับลูกข่าย
   2. ถ้ายืนยันลูกข่ายได้สำเร็จ เครื่องแม่ข่ายทำการถอดรหัสลับพื้นฐานโดยใช้กุญแจลับ(Private Key) ที่มีเฉพาะเครื่องแม่ข่าย และทำงานพร้อมเครื่องลูกข่ายเพื่อสร้าง รหัสลับหลัก(Master Secret)
7. ทั้งเครื่องแม่ข่ายและลูกข่ายใช้รหัสลับหลักเพื่อสร้าง กุญแจสื่อสาร (Session Key) ซึ่งเป็นกุญแจใช้ร่วมกันของแม่ข่ายและลูกข่าย เพื่อการเข้ารหัสและถอดรหัสข้อมูลสื่อสารแลกเปลี่ยนระหว่างช่วงเปิดเอสเอสแอล และเพื่อยืนยันความเป็นบูรณภาพของข้อมูล
8. เครื่องลูกข่ายส่งข้อความให้แก่เครื่องแม่ข่ายเพื่อบอกว่าในอนาคตข้อมูลจะถูกส่งโดยถูกเข้ารหัสด้วยกุญแจสื่อสาร จากนั้นจึงบอกว่าการจับมือด้านเครื่องลูกข่ายได้เสร็จสิ้น
9. เครื่องแม่ข่ายส่งข้อความให้แก่เครื่องลูกข่ายเพื่อบอกว่าในอนาคตข้อมูลจะถูกส่งโดยถูกเข้ารหัสด้วยกุญแจสื่อสาร จากนั้นจึงบอกว่าการจับมือด้านเครื่องแม่ข่ายได้เสร็จสิ้น



รูปที่ . แสดงการส่งข้อมูลบนทีแอลเอสระหว่างลูกข่ายและแม่ข่าย

หมายเหตุ

* ถึงขั้นตอนสุดท้ายถือเป็นการเสร็จสิ้นของการจับมือของเอสเอสแอล และเริ่มการเปิดช่องการสื่อสาร ทั้งสองด้านใช้กุญแจสื่อสารเข้ารหัสและแกะรหัสข้อมูล
* ถ้ามีขั้นตอนด้านบนขั้นตอนใดล้มเหลว จะไม่มีการเชื่อมต่อระหว่างสองฝั่ง

## เรเดียส (RADIUS)

เรเดียส ย่อมาจาก Remote Access Dial In User Service เป็นโพรโทคอลเครือข่ายที่ให้การตรวจสอบ, อนุมัติ และการจัดการการบัญชี (AAA) จากส่วนกลาง สำหรับคอมพิวเตอร์ที่เชื่อมต่อและใช้บริการเครือข่าย   
 เรเดียสเป็นโพรโทคอลแบบไคลเอ็นต์/เซิร์ฟเวอร์ที่วิ่งในชั้นแอพพลิเคชัน ใช้ยูดีพีเป็นช่องทางขนส่ง  
หลักการของเอเอเอ

เอเอเอ ย่อมาจาก การตรวจสอบ (Authentication),การอนุมัติ (Authorization) และการจัดการการบัญชี (Accounting) เป็นโครงสร้างความปลอดภัยสำหรับระบบที่กระจายการบริการใช้งานเพื่อควบคุมผู้ใช้ที่จะเข้าใช้งาน  
 การตรวจสอบ คือ การที่ผู้ใช้ที่เข้าใช้ระบบนั้นเป็นผู้ใช้จริงหรือไม่

การอนุมัติ คือ การอนุญาตว่าผู้ใช้แต่ละคนสามารถใช้ทรัพยากรได้อย่างไร ใช้ระบบได้นานเท่าไหร่ ฯลฯ

การจัดการการบัญชี คือ การเก็บข้อมูลการใช้งานของผู้ใช้ เวลาเริ่มใช้งาน เวลาที่เลิกใช้งาน จำนวนทรัพยากร ระยะเวลา ระหว่างที่ใช้งานระบบ

## คำสั่งบนเทอร์มินอลที่จำเป็นสำหรับลินุกซ์

[ ] = ไม่จำเป็นต้องมีก็ได้ เป็นส่วนเสริมเพิ่มกับคำสั่ง

### คำสั่งจัดการกับไฟล์

1. เปลี่ยนที่อยู่โฟลเดอร์กำลังทำงาน
2. **cd [*options(s)*] [*directory*]**

เช่น cd /etc เข้าไปยังโฟลเดอร์หลักชื่อ etc

1. แสดงไฟล์ในไดเรคทอรี่ (Directory) ปัจจุบัน

**ls [*option(s)*] [*file(s)*]**

เช่น ls –a แสดงไฟล์ทั้งหมดในไดเรคทอรี่ปัจจุบันรวมทั้งไฟล์ที่ซ่อนไว้

1. ทำการลบไฟล์ในระบบ

**rm [*option(s)*] *file(s)***

เช่น rm text.txt ทำการลบไฟล์ที่ชื่อว่า text.txt

1. คัดลอกไฟล์บนระบบ

**cp [*option(s)*] *sourcefile targetfile***

เช่น cp ./myfolder/thisfile /etc/ คัดลอกไฟล์จาก myfolder ชื่อไฟล์ thisfile ไปยังโฟลเดอร์ etc

1. ย้ายไฟล์บนระบบ

**mv [*option(s)*] *sourcefile targetfile***

1. สร้างโฟล์เดอร์บนระบบ

**mkdir [*option(s)*] *directoryname***

เช่น mkdir newfolder สร้างโฟลเดอร์ใหม่ชื่อ newfolder

1. ลบโฟล์เดอร์บนระบบ

**rmdir [*option(s)*] *directoryname***

เช่น rmdir newfolder ลบโฟลเดอร์ชื่อ newfolder

1. โอนย้ายความเป็นเจ้าของไฟล์ให้ผู้ใช้

**chown [*option(s)*] *username.group file(s)***

เช่น chown wwwdata config.conf โอนย้ายให้ผู้ใช้ wwwdata สามารถใช้ไฟล์ config.conf ได้

1. เปลี่ยนการอนุญาตเข้าใช้งานไฟล์

**chmod [*options*] *mode file(s)***เช่น chmod u=rw,g=r,o= internalPlan.txt ผู้ใช้เจ้าของไฟล์แก้ไขและอ่านไฟล์ได้ กลุ่มสามารถอ่านได้นอกเหนือจากนั้นไม่สามารถเข้าถึงไฟล์ได้

### คำสั่งทำงานกับข้อมูลอักขระภายในไฟล์

1. แสดงรายละเอียดภายในไฟล์

**cat [*option(s)*] *file(s)***

1. โปรแกรมเพื่อใช้เปิดดูไฟล์

**less [*option(s)*] *file(s)***

PgUp - PgDown เลื่อนดูข้อความที่ละครึ่งจอ ขึ้น-ลง

Space เพื่อเลื่อนลงเต็มจอ

Home – End เลื่อนไปที่บนสุด – ท้ายสุดของไฟล์

Q เพื่อออกโปรแกรม

1. การค้นหาคำเฉพาะในไฟล์

**grep [*option(s)*] *searchstring filenames***

ผลลัพธ์ที่ได้คือข้อความทั้งบรรทัดที่มีคำเฉพาะนั้นอยู่ สามารถค้นหาโดยใช้นิพจน์ปกติ (Regular Expression) สามารถใช้ค้นหาหลังจากได้ผลลัพธ์จากคำสั่งอื่น เช่น cat studentname.txt | grep suchat โดยระบบจะใช้ข้อความนำเข้าแทนไฟล์นำเข้า

1. เปรียบเทียบข้อมูลอักขระภายในไฟล์

**diff [*option(s)*] *file1 file2***

ผลลัพธ์ที่ได้คือการแสดงอักขระในบรรทัดที่ไม่เหมือนกัน

1. โปรแกรมสำหรับแก้ไขไฟล์

**vi *filename***

โปรแกรม Vi ทุกชื่อโหมดการทำงานไม่สามารถใช้พิมพ์ใหญ่แทนพิมพ์เล็ก หรือเล็กแทนใหญ่ก็ไม่ได้ โดยแสดงที่กำลังทำงานอยู่ในโหมดทางด้านล่างซ้าย การบันทึกและออกจากไฟล์ให้ใช้: (semi-colon) นำหน้าคำสั่งนั้น

|  |  |
| --- | --- |
| ESC | ออกจากทุกโหมดที่กำลังทำงาน |
| i | เข้าสู่โหมดแก้ไขข้อความในไฟล์ |
| u | ย้อนกลับการแก้ไขล่าสุด |
| dd | ลบทั้งบรรทัดที่ตำแหน่งตัวชี้อยู่ |
| :q! | ออกจากไฟล์โดยไม่สนใจการเปลี่ยนแปลงใดๆ |
| :w [*filename*] | บันทึกไฟล์ |
| :x | บันทึกการแก้ไขล่าสุดและออกจากโปรแกรม |

ตารางที่ 2.1 ตารางแสดงคำสั่งบนโปรแกรม Vi

### คำสั่งทำงานกับระบบปฏิบัติการ

1. แสดงข้อมูล รายละเอียดของหน่วยความจำสำรอง

**df [*option(s)*] [*directory*]**

เมื่อใช้โดยไม่เติม พารามิเตอร์จะเป็นการแสดงพื้นที่ทั้งหมด ส่วนที่ถูกใช้ และส่วนที่ว่างต่อการใช้งาน

1. แสดงข้อมูลโปรแกรมที่กำลังทำงาน หน่วยประมวลผลทำงานที่อยู่

**top [*options(s)*]**

1. แสดงข้อมูลโปรแกรมที่กำลังทำงาน หน่วยประมวลผลทำงานที่อยู่ อย่างละเอียด

**ps [*option(s)*] [*process ID*]**

1. การปิดโปรแกรมที่ไม่สามารถปิดด้วยวิธีธรรมดา

**kill [*option(s*)] *process ID***

**killall [*option(s)*] *processname***

โดย process ID หาได้จากการเรียก ps ส่วนการเรียกโดย killall จะใช้ชื่อโปรแกรมที่ต้องการหยุดโดยทุกหน่วยที่มีชื่อตาม processname จะถูกหยุดทำงานทั้งหมด

1. การทดสอบการเชื่อมต่อของเครือข่าย

**ping [*option(s)*] *host name*** *|* ***IP address***

โดยใช้ชื่อเครื่องเป้าหมาย หรือหมายเลขไอพี เพื่อทดสอบการเชื่อมต่อ ถ้าไม่ใส่ค่าจำนวนครั้งจะไม่หยุดการทำงานจนกว่าจะกด Ctrl+C

### คำสั่งเสริมที่จำเป็น

1. การเปลี่ยนรหัสเข้าใช้งาน

**passwd [*option(s)*] [*username*]**

ผู้ใช้งานที่เรียกคำสั่งสามารถเปลี่ยนรหัสเฉพาะของตัวเองเท่านั้น แต่สิทธิผู้ดูแลระบบ root สามารถเปลี่ยนรหัสให้กับผู้ใช้ทุกคน

1. การเปลี่ยนการใช้งานเป็นผู้ใช้งานอื่น

**su [*option(s)*] [*username*]**

โดยสามารถเรียกได้จากผู้ใช้ทุกคน ถ้าไม่มีการใส่ username จะเป็นการเรียกใช้ผู้ดูแลระบบ root โดยจะต้องมีรหัสเข้าใช้งาน root เท่านั้น

1. คำสั่งหยุดการใช้งานระบบ

**halt [*option(s)*]**

เพื่อป้องกันความเสียหายต่อข้อมูล halt จะช่วยปิดโปรแกรมและหยุดระบบเพื่อปิดใช้งานเครื่องด้วยให้เติม –p เพื่อให้ปิดกระแสไฟในเครื่องอัตโนมัติ

1. คำสั่งให้เครื่องเริ่มต้นทำงานใหม่

**reboot [*option(s)*]**

1. การลบทุกอักขระบนหน้าจอผู้ใช้

**clear**

1. การเรียกคำสั่งโดยผู้ใช้ที่ไม่ใช่ผู้ดูแลระบบ แต่ต้องใช้สิทธิผู้ดูแลระบบ

**sudo [*commands*]**

ผู้ใช้ที่สามารถเรียก sudo ต้องมีการบันทึกชื่อไว้ภายในไฟล์ /usr/local/etc/sudoers (บางครั้ง /etc/sudoers) โดยปกติจะใช้รหัสของผู้ใช้ที่เรียก แต่สามารถเปลี่ยนให้ใช้รหัสผู้ดูแลระบบเท่านั้นได้โดยเติมคำสั่ง Defaults rootpw

1. แสดงตำแหน่งที่อยู่เต็มของโปรแกรม

**which [ *options* ] *programname***

โดย programname เป็นชื่อโปรแกรมที่ได้ติดตั้งในระบบแล้ว

## ซิงเกิลไซน์ออน (Single Sign-on)

### รูปแบบของซิงเกิลไซน์ออน

#### ซิงเกิลไซน์ออนแบบดั้งเดิม

การพิสูจน์ตัวจริงแบบดั้งเดิมที่ใช้ในระบบเก่ามีดังนี้

1. ผู้ใช้ใส่ข้อมูลผู้ใช้งาน
2. ระบบยืนยันความถูกต้อง ถ้าผ่านข้อมูลถูกจัดเก็บไว้ในคุกกี้
3. เมื่อผู้ใช้ลงบันทึกเข้า ข้อมูลผู้ใช้ที่เก็บไว้ในคุกกี้ถูกตรวจสอบ

อย่างไรก็ตามซิงเกิลไซน์ออน ต้องทำให้มั่นใจว่าข้อมูลผู้ใช้เป็นเอกลักษณ์กับแต่ละระบบ ทำให้เป็นการสิ้นเปลืองทรัพยากรระบบ และเกิดช่องโหว่ความปลอดภัยเมื่อข้อมูลภายในคุกกี้ถูกอ่านได้

#### ซิงเกิลไซน์ออนบนพื้นฐานเคอร์เบอร์รอส (Kerberos-based SSO)

เคอร์เบอร์รอส เป็นมาตรฐานส่งผ่านกุญแจ นิยามโดยคณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต (IETF) โดยซิงเกิลไซน์ออนบนพื้นฐานเคอร์เบอร์รอส ถูกนำมาใช้งานจริงโดยมี ศูนย์กลางกระจายกุญแจ (KDC) ที่ทำหน้าที่กระจาย ตั๋วและ พิสูจน์ตัวจริงผู้ใช้ โดยแกนหลักการทำงานคือ ตั๋ว และหลักการทำงาน คือ

1. ผู้ใช้พิสูจน์ตัวจริงโดยส่งข้อมูลผู้ใช้ให้ ศูนย์กลางกระจายกุญแจ ถ้าผู้ใช้ลงทะเบียนเป็นครั้งแรก บัตรผ่านแรก (Ticket-granting Ticket, TGT) ถูกส่งไปให้ผู้ใช้
2. เมื่อศูนย์กลางกระจายกุญแจ ได้รับการร้องขอ บัตรผ่านขอใช้บริการ (Service Ticket , ST) พร้อมรับ บัตรผ่านแรกจากผู้ใช้จึงส่ง บัตรผ่านขอใช้บริการให้ผู้ใช้
3. สุดท้ายผู้ใช้ขอรับการบริการจากเครื่องแม่ข่ายโปรแกรมประยุกต์โดยเสนอบัตรผ่านขอใช้บริการ ให้แก่เครื่องแม่ข่าย

****

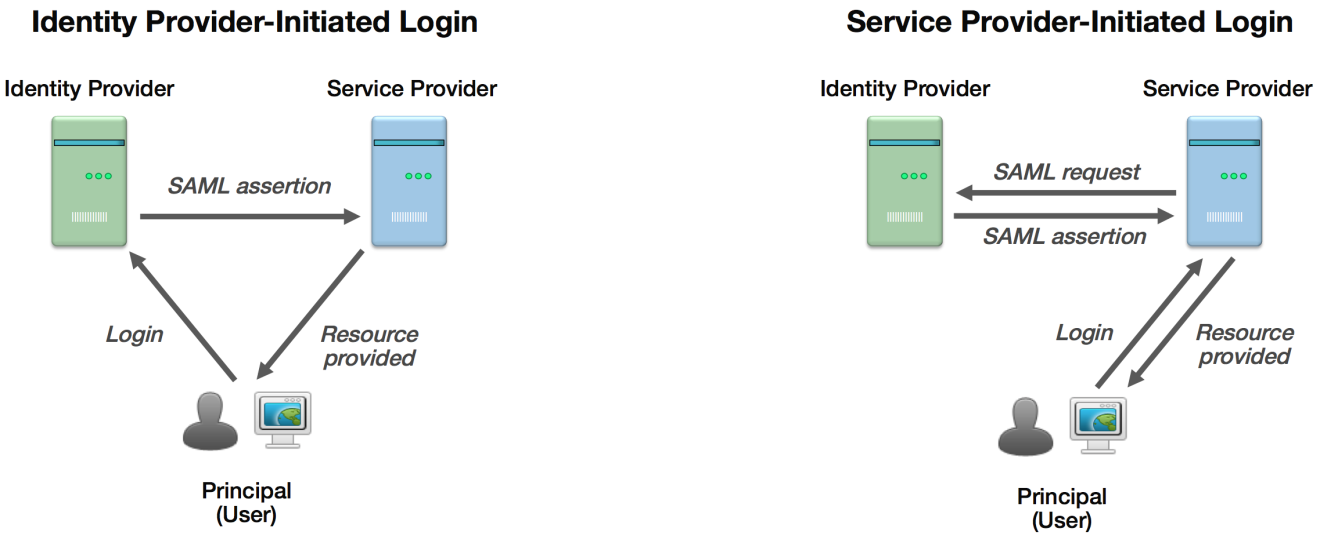
รูปที่ . การส่ง-ผ่านข้อมูลของเครื่องแม่ข่ายโปรแกรม ผู้ใช้ และ ศูนย์กลางกระจายกุญแจ

#### ซิงเกิลไซน์ออนบนพื้นฐานแซมแอล (SAML-based SSO)

โอเอซิส (OASIS) ได้ยอมรับการพัฒนาของแซมแอล ซึ่งเป็นภาษาที่ต่อยอดจากเอกซ์เอ็มแอล (XML) ซึ่งแซมแอล มีคุณสมบัติที่ไม่ขึ้นกับ โพรโทคอล (Protocol) และ แพลตฟอร์ม (Platform) เพื่อควบคุมการเข้าถึงทรัพยากรสำหรับการพิสูจน์ตัวตน

ข้อความยืนยัน เป็นหัวใจหลักของแซมแอล ซึ่งประกอบด้วย การพิสูจน์ตัวจริง คุณลักษณะ และ การอนุญาต ผู้ให้บริการ (Services Provider) ส่งข้อมูลผู้ใช้สำหรับการพิสูจน์เอกลักษณ์ เมื่อผู้ใช้เข้าถึงส่วนบริการซึ่งถูกสร้างขึ้นด้วยผู้ให้บริการผ่านเบราว์เซอร์

ผู้ให้บริการตรวจสอบยืนยันตัวตน (Identity Provider) และ ผู้ให้บริการทำการแลกเปลี่ยนข้อมูล เมื่อผู้ใช้ร้องขอการบริการ ผู้ให้บริการตรวจสอบยืนยันตัวตนจึงสร้างข้อความแซมแอล และส่งข้อความไปยังผู้ให้บริการ จากนั้นผู้ให้บริการยืนยันความถูกต้องของแซมแอล เพื่อให้การบริการ



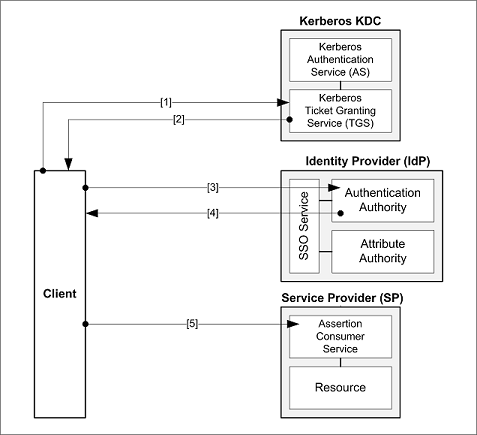
รูปที่ . การส่งผ่านข้อมูลของ ผู้ใช้ ผู้ให้บริการ และ ผู้ให้บริการตรวจสอบยืนยันตัวตน

#### ซิงเกิลไซน์ออนบนพื้นฐานรวมของแซมแอล และเคอร์เบอร์รอส

การจัดการพิสูจน์ตัวจริงแบบรวม และความสามารถในการพิสูจน์ตัวจริงสองทิศทางเป็นความสามารถของ ซิงเกิลไซน์ออนบนพื้นฐานของเคอร์เบอร์รอส ซึ่งช่วยลดปัญหาการบำรุงรักษาระบบ และเพิ่มความปลอดภัยอย่างมาก แต่ว่ายังมีข้อเสียกับการส่งผ่านของข้อมูลตั๋ว การเข้ารหัสและถอดรหัสของตั๋วยังมีความยุ่งยากอยู่มาก นอกจากนั้นข้อมูลผู้ใช้ยังเล็ดลอดได้ง่ายถ้ามีการส่งผ่านระหว่างเบราว์เซอร์และเครื่องแม่ข่ายรุ่นเก่า

แซมแอล เป็นภาษาที่ดั้งเดิมมาจากเอกซ์เอ็มแอล มีคุณลักษณะไม่ขึ้นกับแพลตฟอร์มและภาษาใด ทำงานได้กับระบบที่ไม่เข้ากัน เพื่อให้ง่ายต่อการส่งข้อมูล ผู้ใช้พิสูจน์ตัวจริงกับระบบในรูปแบบข้อความยืนยัน สร้างความปลอดภัยเพราะข้อความถูกใช้แค่ครั้งเดียวจึงถูกลบ แต่มีข้อเสียที่ระบบถูกโจมตีได้ง่ายเพราะขาดการพิสูจน์ตัวจริงแบบสองด้าน (Mutual Authentication)

แผนการสร้างระบบซิงเกิลไซน์ออนโดยการรวมจุดเด่นของเคอร์เบอร์รอส และแซมแอล ช่วยเพิ่มประสิทธิภาพ โดยการรวมความสามารถของแต่ละรูปแบบ เช่น การพิสูจน์แบบสองทางของเคอร์เบอร์รอส ช่วยเพิ่มความปลอดภัยแก่ซิงเกิลไซน์ออน ที่ทำงานกับแซมแอล และแซมแอล ช่วยเป็นตัวกลางสำหรับการส่งตั๋ว นอกจากนั้นการหลุดลอดของข้อมูลยังสามารถถูกแก้ไขโดยการใช้ข้อความยืนยันของแซมแอล



รูปที่ . การส่งข้อมูลของซิงเกิลไซน์ออนบนพื้นฐานรวมของแซมแอล และเคอร์เบอร์รอส

## เทคโนโลยีการยืนยันตัวตนนักศึกษา ที่มีใช้งานในมหาวิทยาลัยเชียงใหม่

### เรเดียส (RADIUS)

#### การเชื่อมต่อกับการบริการเรเดียส

การเชื่อมต่อกับส่วนบริการเรเดียส ของมหาวิทยาลัยเชียงใหม่มีความต้องการ คือ เครื่องแม่ข่ายใช้ไอพีสาธารณะ การส่งข้อมูลยืนยันใช้อีเมล รหัสผ่าน ที่อยู่ของผู้ให้บริการเรเดียส และรหัสลับเข้าใช้งาน โดยสามารถเชื่อมต่อผ่านพีเฮชพี โดยการใช้คลังโปรแกรมของ พีอีซีแอลเรเดียส (PECL Radius)

โดย 2 ค่าที่ได้กลับมาคือ Access-Accept ระบบยืนยันว่ามีผู้ใช้ และ Access-Reject คือการยืนยันตัวตนไม่สำเร็จ



รูปที่ . แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและบริการเรเดียสของสำนักบริการเทคโนโลยี

### เอพีไอ (API)

#### คำสั่งเพื่อทำงานกับเอพีไอ

1. การยืนยันตัวตนนักศึกษา

https://account.cmu.ac.th/v1/api/validateUser?appId={AppID}&appSecret={AppSecret}&user={UserName}&pw={Password}

การยืนยันตัวตนแบบเกท (GET) ตามยูอาร์แอล (URL) มี พารามิเตอร์ (Parameter) ดังนี้

1. เลขโปรแกรม (AppId) คือ หมายเลขเอพีไอที่กำลังเรียกฟังก์ชัน validateUser
2. เลขรหัสโปรแกรม ( AppSecret ) คือ รหัสลับเพื่อเข้าใช้งานเอพีไอ
3. ชื่อผู้ใช้ (Userame) ที่ใช้เป็นชื่อผู้ใช้จากอีเมลของมหาลัยเชียงใหม่ โดยไม่ใส่ @cmu.ac.th
4. รหัสผ่าน (Password) ใช้รหัสผ่านเดียวกับของมหาวิทยาลัยเชียงใหม่
5. การร้องขอข้อมูลนักศึกษา

https://account.cmu.ac.th/v1/api/Students/{userName}?appId={AppID}&appSecret={AppSecret}&accees\_token={access\_token}

การขอข้อมูลนักศึกษาแบบเกท ตามยูอาร์แอลมี พารามิเตอร์ ดังนี้

1. ชื่อผู้ใช้ (Username) เป็นของนักศึกษาที่ยืนยันตัวตนสำเร็จ
2. เลขโปรแกรม
3. เลขรหัสโปรแกรม
4. โทเค็นผ่าน (Access Token) เป็นสายอักขระที่ได้รับหลังยืนยันตัวตนนักศึกษาสำเร็จ

#### ตัวอย่างรูปแบบข้อมูล เจสัน (JSON) ที่ได้จากเอพีไอ

1. ข้อมูลเจสันที่ได้มาจากการยืนยันตัวนักศึกษาสำเร็จ

{

"success": true,

"ticket": {

"access\_token": "zMbjvFfRCD",

"expires\_in": 1800,

"userName": "siwaphol\_boonpan",

"issued": "19/11/2557 16:18:12",

"expires": "19/11/2557 16:48:12"

}

}

1. ข้อมูลเจสันที่ได้มาจากการร้องขอข้อมูลนักศึกษา

{

"success": true,

"ticket": {

"success": true,

"ticket": {

"access\_token": "26ggzJGG1f",

"expires\_in": 1800,

"userName": "siwaphol\_boonpan",

"issued": "19/11/2557 16:20:41",

"expires": "19/11/2557 16:50:41"

}

},

"student": {

"id": "540510828",

"personType": {

"th\_TH": "นักศึกษาปัจจุบัน",

"en\_US": "Present Student"

},

"prefix": {

"th\_TH": "ศิวพล",

"en\_US": "siwaphol"

},

"firstName": {

"th\_TH": "ศิวพล",

"en\_US": "SIWAPHOL"

},

"lastName": {

"th\_TH": "บุญปั๋น",

"en\_US": "BOONPAN"

},

"level": null,

"citizen\_id": "1579900428149",

"faculty": {

"code": "05",

"th\_TH": "คณะวิทยาศาสตร์",

"en\_US": "Faculty of Science"

},

"image": null

}

}

โดยค่าของตัวแปร ticket จะถูกสร้างก็ต่อเมื่อการร้องขอสำเร็จคือ ค่าของ success เป็นจริง



รูปที่ . แผนภาพการส่งข้อมูลระหว่างผู้ขอบริการและเอพีไอของสำนักบริการเทคโนโลยี

# บทที่ 3 การวิเคราะห์และออกแบบระบบ

บทนี้กล่าวถึงการวิเคราะห์และออกแบบระบบงาน โดยจะทำการศึกษาลักษณะการทำงานของระบบเดิม โดยจะทำการศึกษาลักษณะของระบบใช้งานเดิมว่ามีคุณสมบัติการทำงานเป็นอย่างไร มีปัญหาอะไร และทำการสำรวจความต้องการในการพัฒนาระบบเดิมจากคุณถนอม กองใจ ผู้ดูแลระบบส่งงานของภาควิชาวิทยาการคอมพิวเตอร์ เพื่อศึกษารายละเอียดงานของระบบเดิมเพื่อทำการออกแบบและปรับปรุงระบบบริการผ่านเว็บใหม่ให้เกิดการเข้าใช้งานที่สะดวกขึ้น โดยมุ่งเน้นรายละเอียดในการยืนยันตัวตนของระบบโดยทำการออกแบบในลักษณะโมดูลที่สามารถรองรับการขยายเพื่อการใช้งานกับระบบอื่นในอนาคต

## การศึกษาระบบงานเดิม

การศึกษาระบบงานเดิมทั่วไป เป็นการศึกษารายละเอียดของขั้นตอนการยืนยันตัวตนของระบบส่งการบ้านเดิมที่ใช้งานอยู่ ซึ่งมีการยืนยันตัวตนกับระบบผ่านเว็บเพจหน้าพีเอชพี (PHP)โดยมีการยืนยันตัวตนผ่านเลขรหัสประจำตัวนักศึกษาและรหัสผ่านเป็นลักษณะเลขสุ่มจำนวน 4 หลักเพื่อยืนยันตัวตนกับฐานข้อมูลในระบบ ส่วนอาจารย์และผู้ดูแลระบบใช้ชื่อและรหัสเลขสุ่มสี่ตัวเพื่อเข้าระบบ เพื่อเข้าสู่ระบบสารสนเทศส่งการบ้านแต่ละตอนของกระบวนวิชาต่างๆ ส่วนอาจารย์และผู้ดูแลระบบเข้าเรียกดูการส่งการบ้านของนักศึกษาโดยตรงจากไดเรกทอรี (Directory)ของกระบวนวิชานั้น เพื่อการตรวจและให้คะแนนฐานข้อมูลมีการจัดเก็บข้อมูลนักศึกษาประกอบไปด้วย รหัสนักศึกษาเป็นกุญแจหลัก ชื่อ-นามสกุลรหัสเลขสุ่มจำนวน 4 หลักในฐานข้อมูลของอาจารย์และผู้ดูแลระบบประกอบไปด้วย ไอดี ชื่อ-นามสกุล และเลขสุ่ม 4 หลักจึงนำข้อมูลมาวิเคราะห์หาปัญหา เพื่อที่จะนำมาพัฒนาระบบใหม่

### ลักษณะระบบงานเดิม

ลักษณะการทำงานของระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ในส่วนของการยืนยันตัวตนของนักศึกษา มีการกรอกเลขรหัสนักศึกษาเก้าตัว และรหัสคือเลขสุ่ม 4 หลักที่จัดเก็บไว้ในฐานข้อมูลเพื่อเข้าใช้งานภายในระบบ ส่วนของอาจารย์เป็นการกรอกไอดีและ รหัสผ่านเลขสุ่ม 4 หลัก

### ปัญหาของระบบงานเดิม

จากการวิเคราะห์ระบบงานเดิม พบว่ามีปัญหาในการกำหนดให้ใช้รหัสผ่านเลขสุ่มสี่ตัวในการยืนยันตัวตนกับระบบของนักศึกษา เกิดการจำรหัสผ่านเพิ่มเติม ทำให้นักศึกษาลืมรหัสผ่านที่ตัวเองได้รับไป และรหัสผ่านที่ถูกแอบมอง ดักจับ ซึ่งปัญหาของระบบงานเดิมมีดังนี้

1. การกำหนดรหัสผ่านให้แก่นักศึกษา เนื่องจากเป็นตัวเลขสุ่มสี่ตัว เพิ่มภาระการจำให้แก่นักศึกษา ทำให้เกิดการลืมและความผิดพลาดในการจำตัวเลขได้
2. ความปลอดภัยของรหัสเข้าใช้งาน ที่อาจถูกแอบมอง และดักจับ
3. ขั้นตอนของการสร้าง และแจกรหัสผ่านแก่นักศึกษายังมีความยุ่งยาก

## การวิเคราะห์ความต้องการของระบบ (System Requirement)

### ความต้องการของผู้ใช้

จากการวิเคราะห์ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ และข้อมูลความต้องการจากคุณถนอม กองใจ ผู้ดูแลระบบ และคำแนะนำจากอาจารย์ ดร.รัศมีทิพย์วิตา จึงนำความต้องการที่ได้มาปรับปรุงโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ ประกอบไปด้วยส่วนหลัก ดังนี้

|  |  |  |
| --- | --- | --- |
| **กลุ่มผู้ใช้งาน** | **รูปแบบการยืนยันตัวตน** | **หน้าที่การทำงาน** |
| ผู้ดูแลระบบ | ไอดีคือ ชื่อภาษาอังกฤษ และรหัสผ่านผู้ใช้กำหนดเอง | 1. จัดการข้อมูลผู้ใช้ในโมดูล การเพิ่ม แก้ไข และลบข้อมูล 2. จัดการการเชื่อมต่อระหว่างโมดูลและผู้ให้บริการอื่น |
| คณาจารย์ | ไอดีคือ ชื่อภาษาอังกฤษ และรหัสผ่านผู้ใช้กำหนดเอง | 1. ทำการยืนยันตัวตนในระดับคณาจารย์ |
| นักศึกษา | ใช้อีเมลที่เป็นโดเมนมหาวิทยาลัยเชียงใหม่ และรหัสผ่านเดียวกับส่วนกลาง | 1. ทำการยืนยันตัวตนระดับนักศึกษา |

ตารางที่ . ตารางแสดงรูปแบบการยืนยันตัวตนของผู้ใช้ และหน้าที่การทำงานกับโมดูลยืนยันตัวตน

### การเปรียบเทียบบริการยืนยันตัวตนจากสำนักบริการเทคโนโลยีเพื่อใช้กับโมดูล

การยืนยันตัวตนของโมดูลจากการให้บริการของสำนักบริการเทคโนโลยีมีดังนี้

1. เรเดียสยืนยันตัวตนของสำนักบริการเทคโนโลยี มีความต้องการ ระบบที่เรียกใช้ต้องมี ไอพีภายนอก เพื่อความปลอดภัยต่อการส่งข้อมูล

ใช้อีเมลผู้ใช้ รหัสผ่านผู้ใช้ยูอาร์แอลผู้ให้บริการเรเดียส และรหัสลับ ในการร้องขอแต่ละครั้ง

1. เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี (ITSC Authentication API) มีความต้องการ การเรียกแบบ GETผ่านยูอาร์แอล ของสำนักบริการเทคโนโลยี พร้อมพารามิเตอร์ที่ส่งไปพร้อมกัน เช่นอีเมลผู้ใช้โดยไม่ใส่ส่วนโดเมน รหัสผ่านผู้ใช้ เลขที่โปรแกรม และรหัสของโปรแกรม โทเคนที่ได้หลังยืนยันตัวตนสำเร็จ

|  |  |  |
| --- | --- | --- |
| คุณสมบัติ | เรเดียสยืนยันตัวตนของสำนักบริการเทคโนโลยี | เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี |
| สามารถยืนยันตัวตนนักศึกษา | 🗸 | 🗸 |
| ส่งข้อมูลนักศึกษา | 🗴 | 🗸 |
| ใช้ได้บนเอสเอสแอล | 🗸 | 🗸 |
| ทำงานได้กับพีเฮชพี | 🗸 | 🗸 |
| ข้อมูลที่ได้เป็นแบบเจสัน | 🗴 | 🗸 |
| การกำหนดใช้กับไอพีภายนอก | 🗸 | 🗴 |

ตารางที่ . ตารางเปรียบเทียบคุณสมบัติของเรเดียสยืนยันตัวตน และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี

จากการวิเคราะห์แล้ว พบว่าการใช้เอพีไอยืนยันตัวตนมีความเหมาะสมที่สุดเพราะฟังก์ชันที่มีให้ตรงความต้องการ สามารถยืนยันตัวตน และให้ข้อมูลนักศึกษาต่อคน ไม่มีการใช้ไอพีภายนอก ทำให้โมดูลสามารถนำไปใช้ได้บนทุกระบบปฏิบัติการ ไม่ขึ้นอยู่กับระบบใดระบบหนึ่ง

## แผนภาพยูเอ็มแอล(UML)

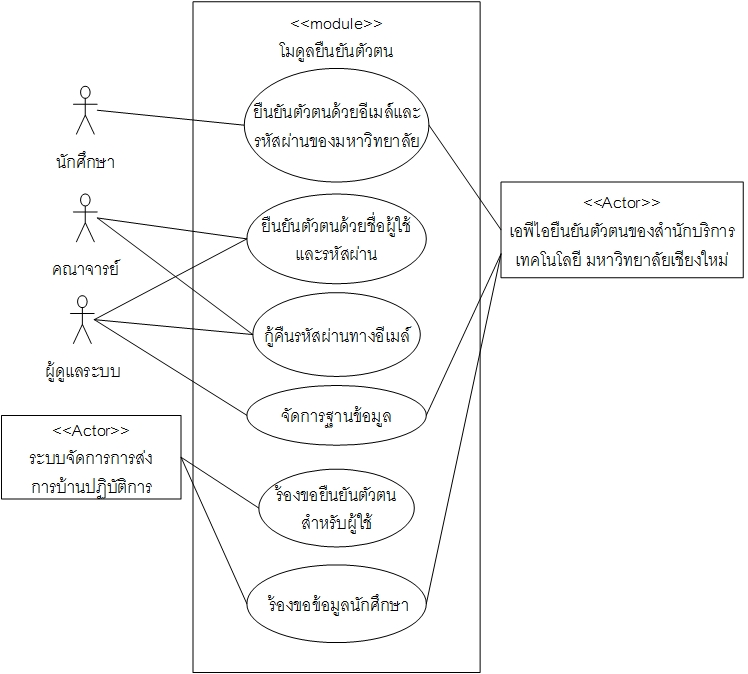
การวิเคราะห์โมดูลยืนยันตัวตนเพื่อการออกแบบนั้น ทางผู้ออกแบบได้ใช้แผนภาพแบบยูเอ็มแอลเพื่อแสดงการทำงานในภาพรวมระดับสูง เช่น แผนภาพยูสเคส (Use Case Diagram) ที่แสดงให้เห็นว่าผู้ใช้งานกับระบบภายนอกมีส่วนทำงานประสานกับโมดูล ทำงานอะไรบ้างเพื่อง่ายต่อการแสดงความต้องการของโมดูลแผนภาพกิจกรรม (Activity Diagram) แสดงการทำงานแบบกว้าง และแผนภาพขั้นลำดับ (Sequence Diagram) แสดงการทำงานและการส่งข้อมูลแบบละเอียด

### แผนภาพยูสเคส

แผนภาพที่แสดงการทำงานของผู้ใช้ระบบ (User) และความสัมพันธ์กับระบบย่อย (Sub Systems) ภายในระบบใหญ่ ในการเขียนแผนภาพการใช้งาน ผู้ใช้ระบบ (User) จะถูกกำหนดว่าให้เป็นผู้ใช้งาน (Actor) และ ระบบย่อย คือ แผนภาพยูสเคส ซึ่งใช้สัญญาลักษณ์ดังตาราง 3.3

ตารางที่ . ตารางสัญลักษณ์แผนภาพยูสเคส

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Actor | สัญลักษณ์ แทนสิ่งที่อยู่นอกระบบ เช่น คน สิ่งของ หน่วยงาน |
|  | Use Case | สัญลักษณ์ แทนกระบวนการ หรือการประมวลผล |
|  | association | สัญลักษณ์เชื่อมความสัมพันธ์ |
|  | System | สัญลักษณ์ กรอบการทำงานของระบบ |



รูปที่ . แผนภาพยูสเคสของโมดูลยืนยันตัวตน

**ชื่อการใช้งาน:** ยืนยันตัวตนด้วยอีเมลและรหัสผ่านของมหาวิทยาลัย

**คำอธิบาย:** นักศึกษาในฐานะนักแสดงทำการยืนยันตัวตนกับโมดูลโดยใช้ อีเมล และรหัสผ่าน เดียวกันกับที่ใช้ของมหาวิทยาลัยเชียงใหม่ โดยโมดูลนำอีเมลและรหัสผ่านที่ได้ตรวจสอบกับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี เพื่อนักศึกษาสามารถเข้าใช้ระบบที่ต้องการ เช่น ระบบจัดการการส่งการบ้านปฏิบัติการ

**จุดสำคัญของเหตุการณ์:** อีเมลและรหัสผ่านนักศึกษามีความถูกต้อง

**เงื่อนไขก่อน:** นักศึกษาเข้าสู่หน้าเว็บกรอกข้อมูลยืนยันตัวตนเพื่อเข้าใช้ระบบที่ต้องการ

**ผลลัพธ์เมื่อสำเร็จ:** นักศึกษายืนยันตัวตนสำเร็จ

**ชื่อการใช้งาน:** ยืนยันตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน

**คำอธิบาย:** ผู้ดูแลระบบ/คณาจารย์ ยืนยันตัวตนกับโมดูลโดยใช้ ชื่อผู้ใช้และรหัสผ่านที่ถูกกำหนดไว้ก่อนภายในฐานข้อมูลของโมดูลแล้ว เพื่อให้ได้สิทธิ์แบบผู้ดูแลระบบ/คณาจารย์ เข้าใช้ระบบที่ต้องการ เช่น สิทธิ์การจัดการข้อมูลภายในระบบนั้น

**จุดสำคัญของเหตุการณ์:** ชื่อผู้ใช้และรหัสผ่านมีความถูกต้อง

**เงื่อนไขก่อน:** ผู้ดูแลระบบ/คณาจารย์ เข้าสู่หน้าเว็บกรอก ชื่อผู้ใช้และรหัสผ่าน เพื่อยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบ/คณาจารย์สามารถยืนยันตัวตนกับโมดูลได้สำเร็จ

**ชื่อการใช้งาน:** กู้คืนรหัสผ่านทางอีเมล

**คำอธิบาย:** ผู้ดูแลระบบ/คณาจารย์ร้องขอรหัสผ่านจากฐานข้อมูลในระบบ โดยระบบจะส่งผ่านทางอีเมลของผู้ใช้ จากฐานข้อมูลในโมดูล โดยโมดูลรับเข้าชื่อผู้ใช้เพื่อกำหนดอีเมลเป้าหมายที่ต้องส่งข้อความ

**จุดสำคัญของเหตุการณ์:** ชื่อผู้ใช้ที่กรอกถูกต้อง

**เงื่อนไขก่อน:** ผู้ดูแลระบบ/คณาจารย์เข้าสู่เมนู กู้คืนรหัสผ่านทางอีเมลแล้วกรอกชื่อผู้ใช้ของตัวเอง

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบ/คณาจารย์ ได้รับข้อความอีเมลแสดงรหัสผ่าน ที่โมดูลยืนยันตัวตนส่งให้

**ชื่อการใช้งาน:** จัดการฐานข้อมูล

**คำอธิบาย:** ผู้ดูแลระบบ จัดการข้อมูลในฐานข้อมูลของโมดูลได้ ทั้งจากหน้าเว็บที่โมดูลมีให้ และจากคำสั่งเอสคิวแอลโดยตรง ผู้ดูแลระบบสามารถจัดการข้อมูลทุกอย่างภายในฐานข้อมูล เช่น การเปลี่ยนชื่อ และอีเมลของผู้ใช้

**จุดสำคัญของเหตุการณ์:** คำสั่งจัดการและข้อมูลมีความถูกต้อง

**เงื่อนไขก่อน:** ถ้าจัดการผ่านหน้าเว็บผู้ดูแลระบบเข้าสู่ยูอาร์แอลจากเบราเซอร์ สำหรับการจัดการเอสคิวแอลโดยตรงให้เข้าระบบปฏิบัติการโดยตรงหรือผ่านการควบคุมระยะไกล โดยใช้บัญชีผู้ใช้ของระบบปฏิบัติการ

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ดูแลระบบสามารถเพิ่ม แก้ไข หรือลบข้อมูลผู้ใช้ในฐานข้อมูลของโมดูลได้

**ชื่อการใช้งาน:** ร้องขอยืนยันตัวตนสำหรับผู้ใช้

**คำอธิบาย:** ระบบนอกในที่นี้คือ ระบบจัดการการส่งการบ้านปฏิบัติการ ทำการสร้างคำร้องยืนยันตัวตนแบบแซมแอล (SAML Request Assertion) เพื่อให้เบราเซอร์ส่งต่อมายังโมดูลยืนยันตัวตน เมื่อการยืนยันตัวตนสำเร็จระบบนอกจึงรับผลลัพธ์การยืนยันตัวตนแซมแอล (SAML Response Assertion) จากโมดูลยืนยันตัวตน เพื่อใช้ในการยืนยันว่าผู้ใช้งานสามารถเข้าใช้งานระบบได้

**จุดสำคัญของเหตุการณ์:** ผลลัพธ์การยืนยันตัวตนแซมแอลที่ได้รับแสดงถึงการยืนยันตัวตนของผู้ใช้สำเร็จ

**เงื่อนไขก่อน:** ระบบนอกสร้างคำร้องยืนยันตัวตนแบบแซมแอล เพื่อเบราเซอร์ใช้ยืนยันตัวตนกับโมดูลยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ผู้ใช้ยืนยันตัวตนสำเร็จเข้าใช้งานระบบได้

**ชื่อการใช้งาน:** ร้องขอข้อมูลนักศึกษา

**คำอธิบาย:** ระบบนอกส่งคำร้องเพื่อขอข้อมูลผู้ใช้ภายในฐานข้อมูลของโมดูลยืนยันตัวตน โดยส่งข้อมูลระหว่างกันผ่านทางโพรโทคอลเอชทีทีพี (HTTP Protocol)

**จุดสำคัญของเหตุการณ์:** คำร้องขอของระบบนอกมีความถูกต้อง

**เงื่อนไขก่อน:** ระบบนอกสร้างคำสั่งร้องขอข้อมูลนักศึกษาแบบ GET โดยกำหนดตัวแปรและข้อมูลที่ต้องการจากโมดูลยืนยันตัวตน

**ผลลัพธ์เมื่อสำเร็จ:** ระบบนอกได้รับข้อมูลผู้ใช้ตรงตามความต้องการ

### แผนภาพกิจกรรม

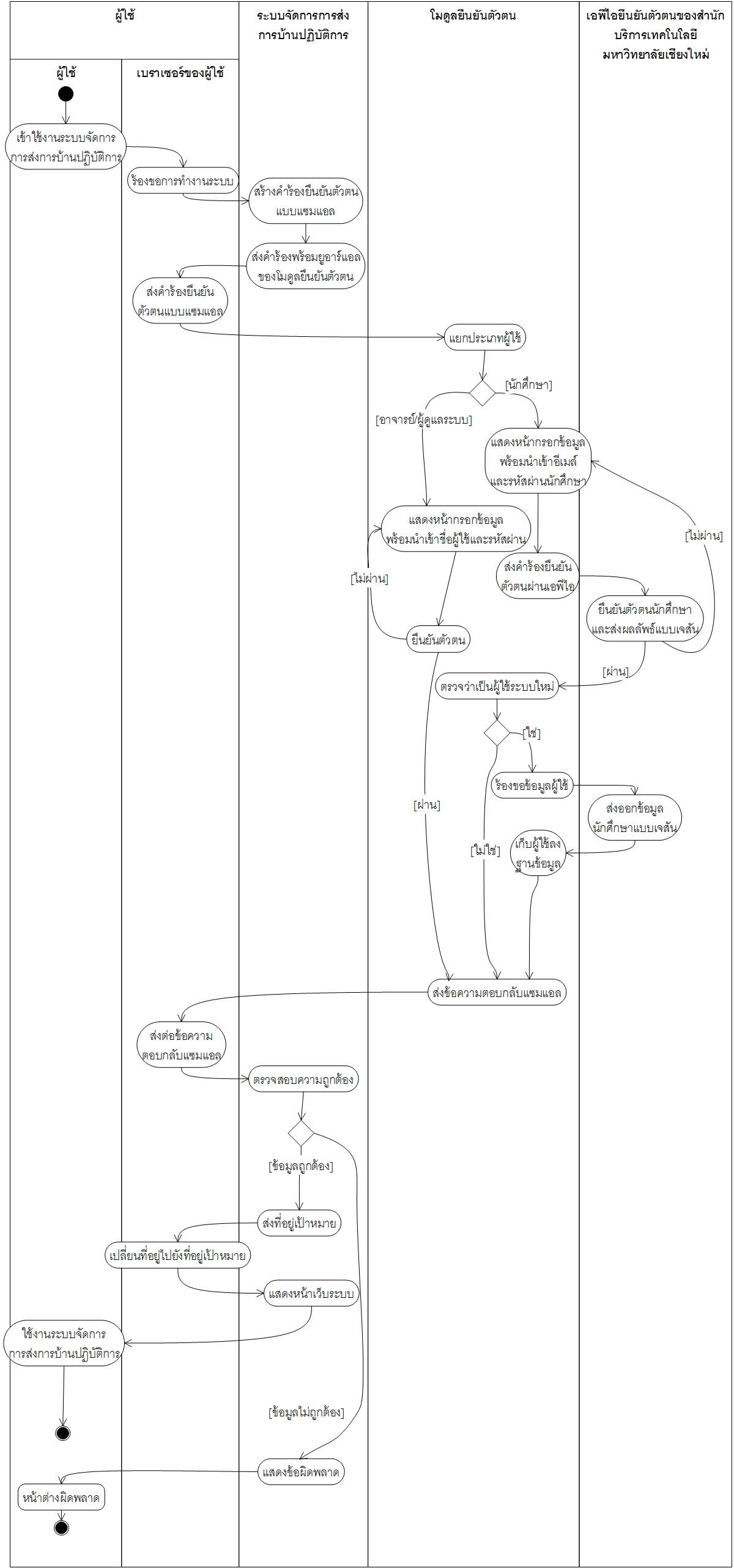
การใช้แผนภาพกิจกรรม เป็นไปเพื่อแสดงขั้นตอนการส่งข้อมูล การทำงานแสดงความสัมพันธ์ระหว่างผู้ใช้ระบบนอก เช่น ระบบจัดการการส่งการบ้านปฏิบัติการ และเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี ที่มีต่อโมดูลยืนยันตัวตน โดยมีการรวมการใช้งานในบางแผนภาพเพื่อให้เห็นการทำงานร่วมกันของผู้ใช้และระบบ ซึ่งแผนภาพนี้ใช้สัญญาลักษณ์ดังตาราง 3.4

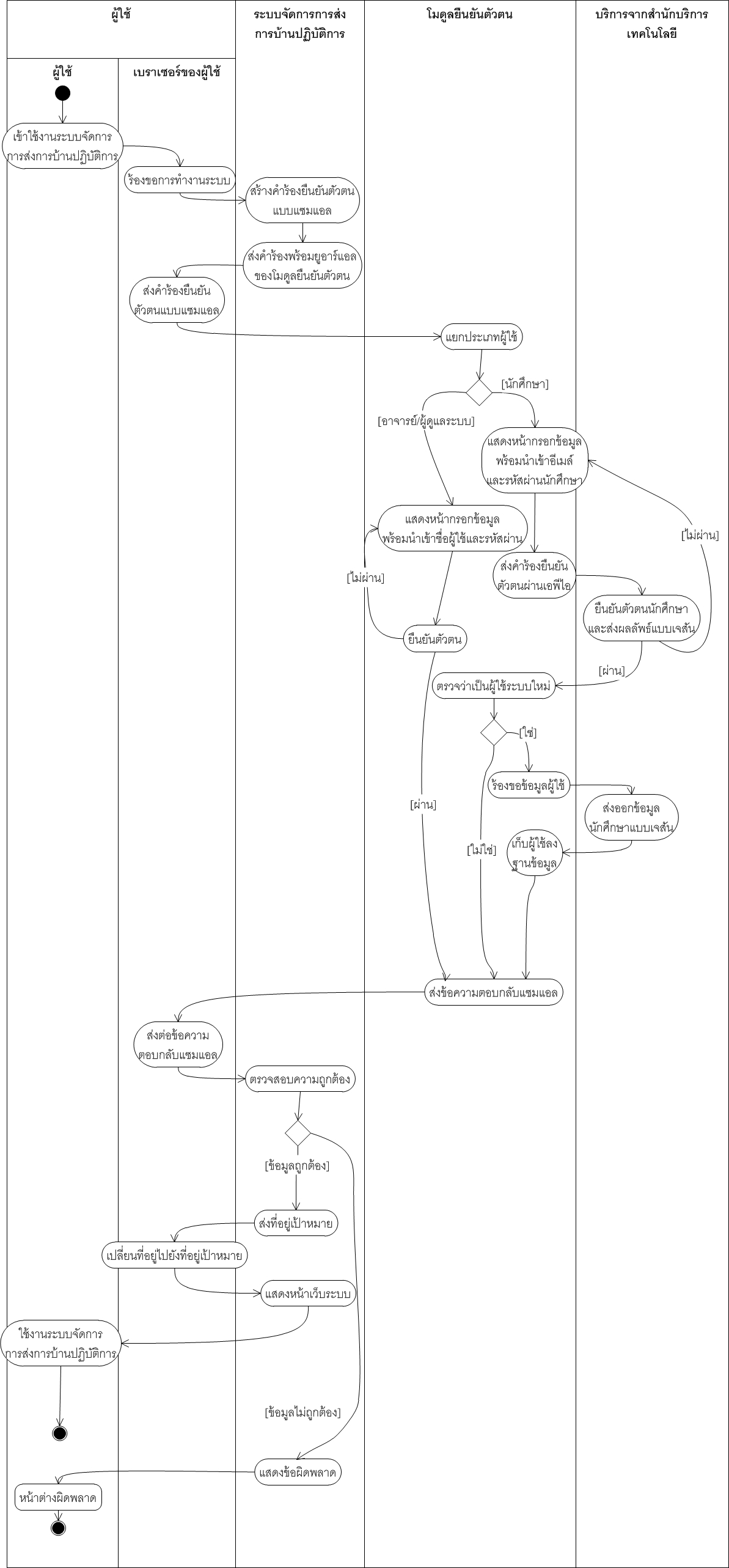
ตารางที่ . ตารางสัญลักษณ์แผนภาพกิจกรรม

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Start State | สัญญาลักษณ์สถานะเริ่มต้นในระบบ |
|  | Final State | สัญญาลักษณ์สถานะสุดท้ายในระบบ แสดงถึงการจบการทำงาน |
|  | State | สัญญาลักษณ์แสดงสถานะของระบบ |
|  | Decision | สัญญาลักษณ์การตัดสินใจเลือกสถานะของระบบ |
|  | Flow | สัญญาลักษณ์ให้เห็นลำดับถานะการทำงานในระบบ |
|  | System | สัญลักษณ์กรอบการทำงานของระบบ |

ตารางที่ . ตารางอธิบายคำศัพท์เฉพาะภายในแผนภาพยูเอ็มแอล

|  |  |
| --- | --- |
| **คำศัพท์** | **คำอธิบาย** |
| คำร้องยืนยันตัวตนแบบแซมแอล | เป็นข้อความคำร้องยืนยันตัวตนแบบแซมแอล ซึ่งถูกสร้างด้วยระบบนอก โดยโมดูลยืนยันตัวตนใช้เพื่อตรวจสอบก่อนให้บริการยืนยันตัวตนแก่ผู้ใช้ |
| ข้อความตอบกลับแบบแซมแอล | เป็นข้อความตอบกลับแสดงผลลัพธ์ยืนยันตัวตนแบบแซมแอล หลังจากผู้ใช้ยืนยันตัวตนกับโมดูลยืนยันตัวตนได้สำเร็จเพื่อให้เบราเซอร์ใช้ในการขอบริการกับระบบส่งการบ้าน โดยภายในข้อความประกอบไปด้วยค่าตัวแปรที่จำเป็นสำหรับการทำงานของระบบอื่น |
| ระบบจัดการการส่งการบ้านปฏิบัติการ | เปรียบเสมือนผู้ให้บริการ ให้บริการแก่นักศึกษาที่ลงทะเบียนกระบวนวิชาของภาควิชาวิทยาการคอมพิวเตอร์ คณาจารย์ประจำภาควิชา และผู้ดูแลระบบซึ่งมีการใช้บริการยืนยันตัวผู้ใช้งานผ่านโมดูลยืนยันตัวตน |
| เอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี มหาวิทยาลัยเชียงใหม่ | ส่วนให้บริการทำงานผ่าน เอชทีทีพี แบบ GET   1. ยืนยันตัวตนนักศึกษา 2. บริการส่งผ่านข้อมูลนักศึกษา |
| เงื่อนไข | เป็นแบบรูปแบบเงื่อนไขที่รวมทั้งข้อมูล ซึ่งถูกนำไปใช้เพื่อดึงข้อมูลบางส่วนจากฐานข้อมูลของโมดูลยืนยันตัวตน |
| ข้อมูลนักศึกษา | ข้อมูลนักศึกษา ประกอบไปด้วย ชื่อ นามสกุล เลขที่ประจำตัวนักศึกษาเป็นต้น |





รูปที่ . แผนภาพกิจกรรมแสดงการยืนยันตัวตนของผู้ใช้ และการส่งข้อมูลระหว่างระบบ

จากแผนภาพกิจกรรมจะเห็นว่า โมดูลแบ่งผู้ใช้เป็น 2 กลุ่ม คือ 1.นักศึกษา 2.คณาจารย์และผู้ดูแลระบบ

สำหรับข้อมูลที่ใช้ยืนยันตัวตนของนักศึกษาคือ อีเมลและรหัสผ่านของมหาวิทยาลัยเชียงใหม่ โดยโมดูลยืนยันตัวตนตรวจสอบตัวตนนักศึกษากับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีโดยค่าตอบกลับที่ได้เป็นแบบเจสัน เมื่อยืนยันตัวตนนักศึกษากับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีได้สำเร็จ จากนั้นจึงตรวจสอบว่ามีข้อมูลนักศึกษาที่ยืนยันตัวตนสำเร็จในระบบหรือไม่ ถ้าไม่มีให้ทำการเพิ่มข้อมูลนักศึกษาโดยร้องขอข้อมูลจากเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยีเพื่อจัดเก็บไว้ในฐานข้อมูลของโมดูลยืนยันตัวตน

สำหรับคณาจารย์และผู้ดูแลระบบยืนยันตัวตนกับโมดูลโดยใช้ชื่อผู้ใช้และรหัสผ่านที่มีอยู่ในฐานข้อมูลของโมดูลยืนยันตัวตน

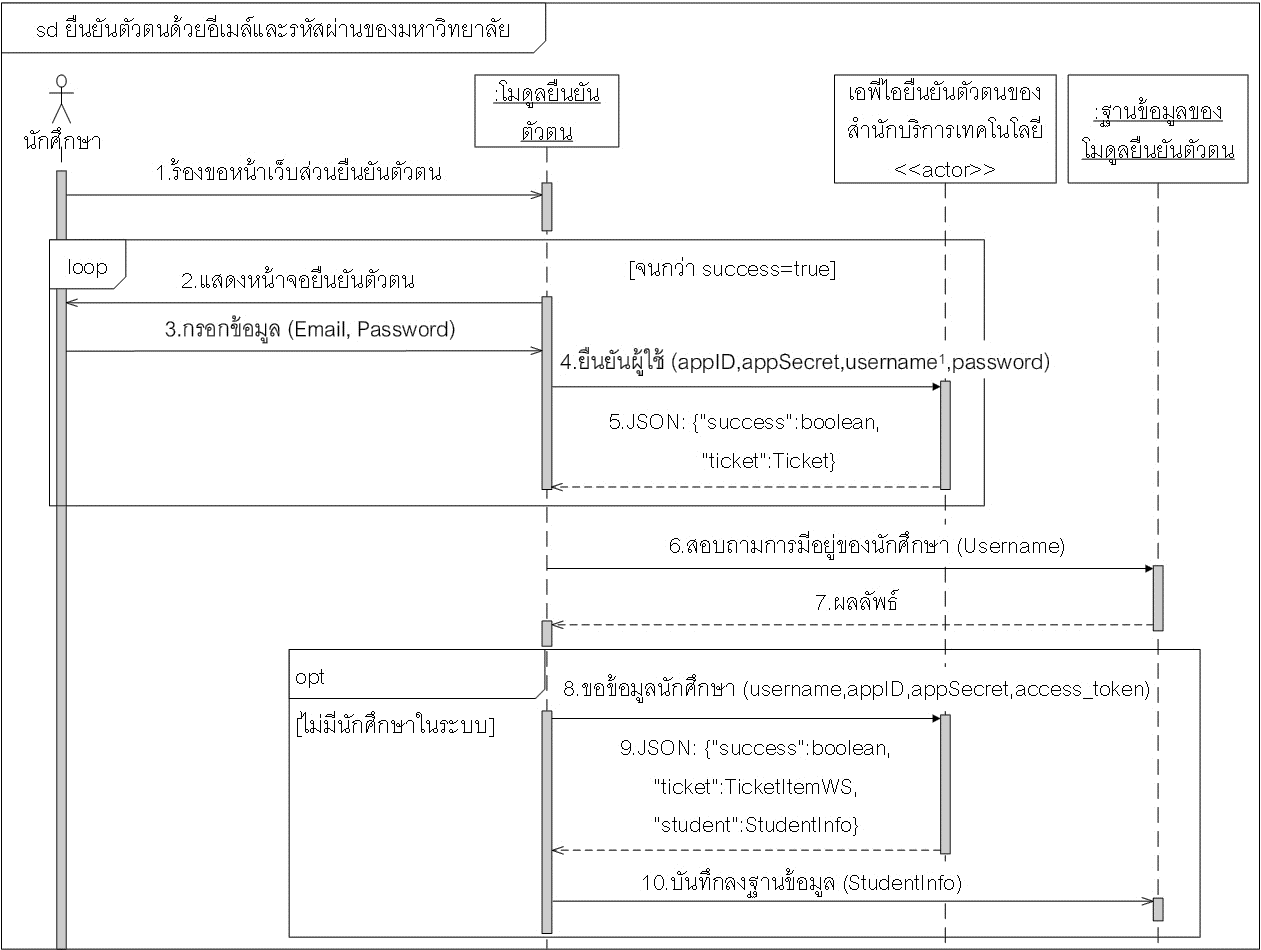
การติดต่อระหว่างโมดูลยืนยันตัวตนและระบบนอกที่ร้องขอการยืนยันตัวตน (ระบบจัดการการส่งการบ้านปฏิบัติการ) ใช้การส่งข้อความแซมแอลเป็นสื่อแลกเปลี่ยนข้อมูลระหว่างกันในการยืนยันตัวตนของผู้ใช้ โดยที่ระบบจัดการการส่งการบ้านปฏิบัติการทำการสร้างคำร้องยืนยันตัวตนแบบแซมแอลสำหรับแต่ละผู้ใช้ และส่งให้เบราเซอร์ของผู้ใช้เพื่อส่งต่อให้กับโมดูลยืนยันตัวตน เมื่อโมดูลยืนยันตัวตนได้รับคำร้องจึงจะให้บริการแก่ผู้ใช้ เมื่อการยืนยันตัวสำเร็จ โมดูลยืนยันตัวตนสร้างข้อความตอบกลับแบบแซมแอลโดยข้อความตอบกลับจะประกอบไปด้วยประเภทของผู้ใช้และข้อมูลผู้ใช้ที่จำเป็น จากนั้นจึงส่งให้เบราเซอร์เพื่อใช้ในการขอบริการกับระบบจัดการการส่งการบ้านปฏิบัติการ

### แผนภาพขั้นลำดับ

แผนภาพแสดงลำดับการทำงานของระบบ โดยมีวัตถุและเวลาเป็นตัวกำหนดลำดับของงาน และเน้นไปที่ การแสดงปฏิสัมพันธ์ ระหว่างวัตถุ ตามลำดับของเหตุการณ์ที่เกิดขึ้น ณ เวลาที่กำหนด ข้อความที่เกิดขึ้นระหว่างวัตถุ ซึ่งแผนภาพนี้ใช้สัญญาลักษณ์ดังตาราง 3.6

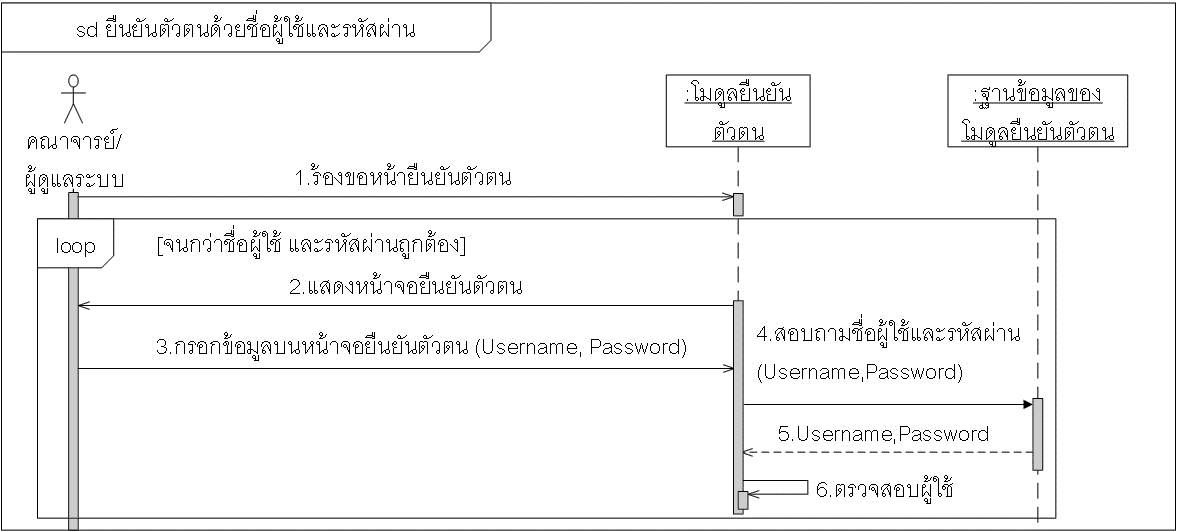
ตารางที่ . ตารางสัญลักษณ์แผนภาพ Sequence Diagram

|  |  |  |
| --- | --- | --- |
| **สัญลักษณ์** | **ชื่อสัญลักษณ์** | **คำอธิบาย** |
|  | Actor | สัญลักษณ์แสดงผู้ใช้งานที่เกี่ยวข้องกับระบบ |
|  | Instance | สัญลักษณ์แสดงสิ่งที่ระบบตอบสนองต่อผู้ใช้งาน |
|  | Lifeline | สัญลักษณ์เส้นแสดงถึงขอบเขตของแต่ละส่วนเกี่ยวข้อง |
|  | Message | สัญลักษณ์แสดงคำสั่งหรือการสั่งการ |
|  | Message Return | สัญลักษณ์แสดงถึงค่าส่งกลับจากระบบด้านขวาไปหาด้านซ้ายของแผนภาพ |
|  | Focus of Control/Activation | สัญลักษณ์จุดเริ่มต้นและจุดสิ้นสุดของแต่ละกิจกรรมในระหว่างการทำงาน |



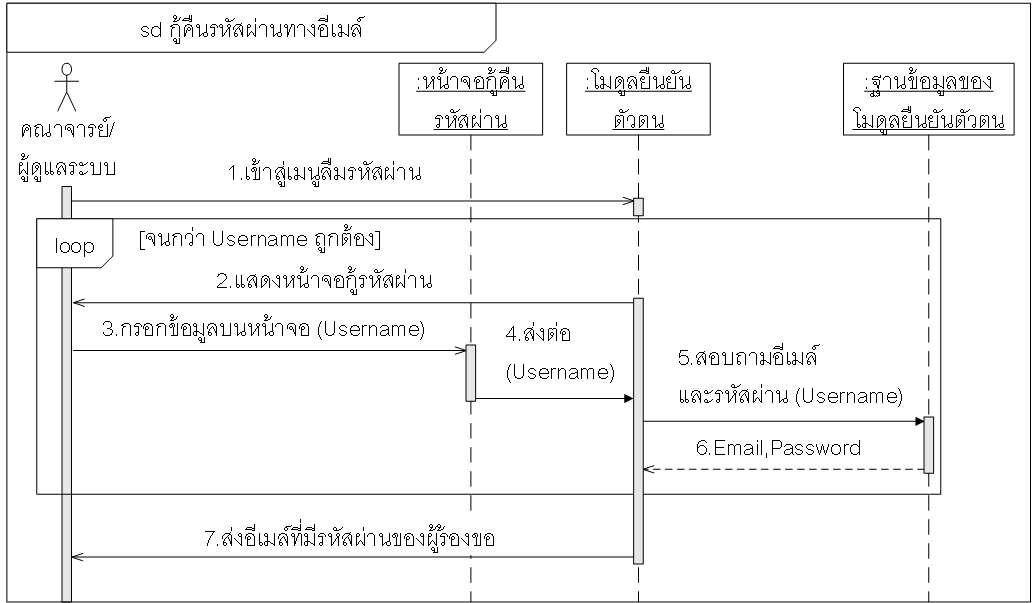
รูปที่ . แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของนักศึกษา

จากแผนภาพขั้นลำดับแสดงการยืนยันตัวตนกับระบบของนักศึกษา โดยโมดูลจะแสดงหน้าจอเพื่อรอรับข้อมูลเมื่อรับข้อมูลได้แล้วจึงจะส่งอีเมลและรหัสผ่านให้กับเอพีไอยืนยันตัวตนของสำนักบริการเทคโนโลยี โดยส่งข้อความในรูปแบบ การร้องขอเอชทีทีพีแบบ GET โดยที่ appID และ appSecret เป็นตัวแปรสำคัญในการร้องขอการบริการจากระบบที่ถูกต้อง ต่อด้วยชื่อผู้ใช้ (มาจากอีเมลโดยจะไม่ใส่ @cmu.ac.th )และรหัสผ่านของนักศึกษาเป็นรายบุคคล การตอบกลับสำหรับส่วนบริการยืนยันตัวตน จะเป็นข้อมูลแบบเจสัน ตัวแปรที่สำคัญ คือ success ที่จะบอกว่านักศึกษายืนยันตัวตนกับเอพีไอยืนยันตัวตนได้สำเร็จและ ticket ที่มีสมาชิกคือ access\_token ซึ่งจะถูกใช้ในการร้องขอข้อมูลนักศึกษาต่อไป เมื่อได้ผลลัพธ์ว่าเป็นนักศึกษาถูกต้องจึงตรวจสอบว่ามีข้อมูลนักศึกษาในฐานข้อมูลของโมดูล ถ้าไม่ให้ร้องขอแบบ GET โดยขอข้อมูลตามชื่อผู้ใช้ และได้ข้อมูลกลับมาแบบเจสันเช่นกัน โดยที่ในครั้งนี้ success จะบอกว่าขอข้อมูลนักศึกษาได้สำเร็จ ตัวแปร ticket จะเปลี่ยนแปลงค่าทุกครั้งเมื่อมีการร้องขอข้อมูลนักศึกษา และที่สำคัญคือ student ซึ่งเก็บข้อมูลกลุ่มของตัวแปรที่ระบุข้อมูลประจำตัวนักศึกษา เช่น ชื่อ นามสกุล ( ไทย-อังกฤษ )รหัสนักศึกษา เป็นต้น ซึ่งค่าในตัวแปร student จะถูกจัดเก็บต่อไป



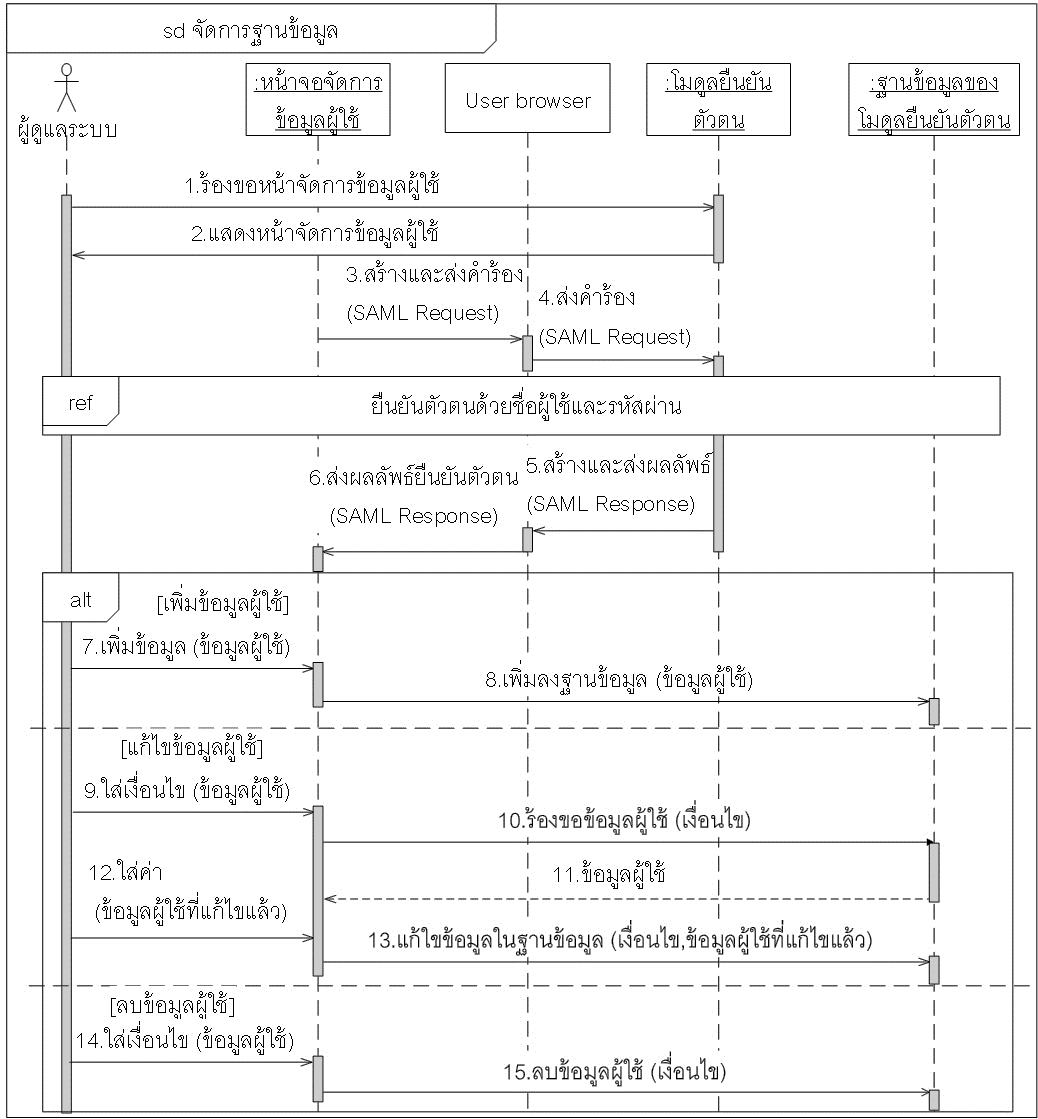
รูปที่ . แผนภาพขั้นลำดับสำหรับการยืนยันตัวตนของคณาจารย์และผู้ดูแล

เมื่อผู้ใช้เป็นคณาจารย์หรือผู้ดูแลระบบ สิ่งที่ใช้ยืนยันตัวตน คือ ชื่อผู้ใช้และรหัสผ่าน ที่จัดเก็บอยู่ภายในฐานข้อมูลของโมดูลยืนยันตัวตน การตรวจสอบยืนยันตัวตนจึงทำภายในโมดูลยืนยันตัวตน ไม่มีการร้องขอจากระบบภายนอก



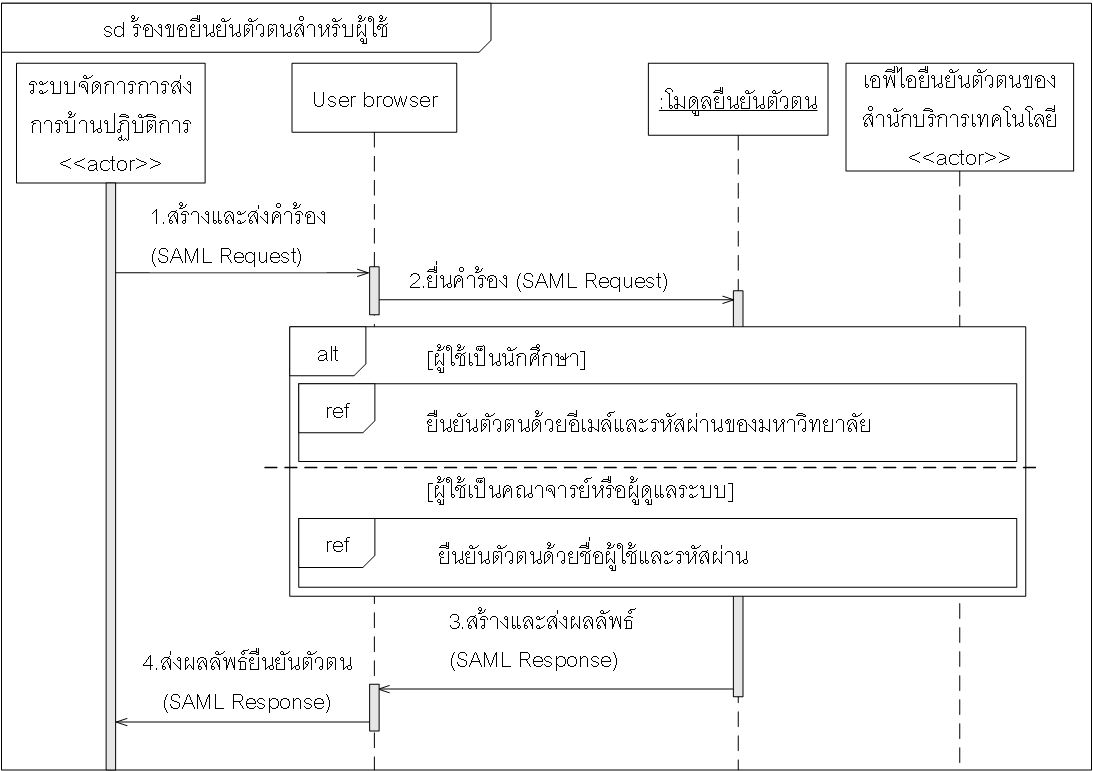
รูปที่ . แผนภาพขั้นลำดับการกู้คืนรหัสผ่านของคณาจารย์และผู้ดูแลระบบ

การกู้คืนรหัสผ่านเป็นส่วนสำหรับคณาจารย์หรือผู้ดูแลระบบ ที่จะสามารถสอบถามรหัสผ่านเมื่อทำรหัสผ่านหาย หรือลืมรหัสผ่าน โดยจะให้ผู้ใช้กรอกชื่อผู้ใช้บนหน้าจอ แล้วโมดูลจะตรวจสอบที่อยู่อีเมล โมดูลยืนยันตัวตนจะใช้สำหรับส่งรหัสผ่านในฐานข้อมูลให้กับผู้ใช้ต่อไป



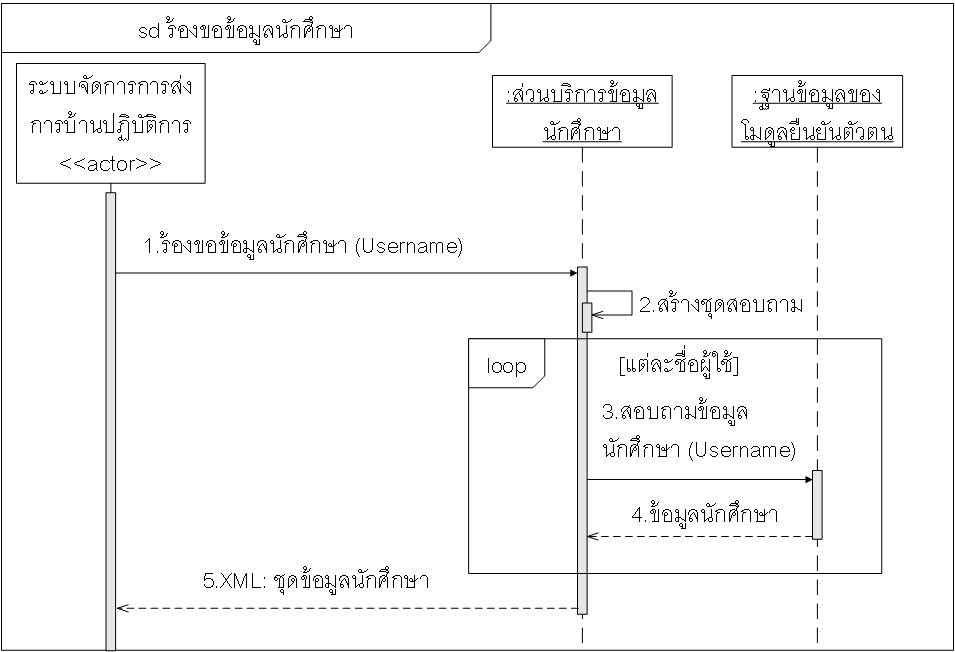
รูปที่ . แผนภาพขั้นลำดับแสดงการจัดการฐานข้อมูลของโมดูลยืนยันตัวตนของผู้ดูแล

จากแผนภาพเป็นการจัดการข้อมูลผู้ใช้ภายในฐานข้อมูลของโมดูลยืนยันตัวตน โดยผู้ใช้ที่มีสิทธ์มีเพียงผู้ดูแลระบบโดยการทำงานผ่านหน้าจอจัดการข้อมูลผู้ใช้ โดยหน้าจอจัดการข้อมูลผู้ใช้ทำงานเสมือนระบบนอกที่ต้องสร้างคำขอยืนยันตัวตนให้กับผู้ดูแลระบบและรับข้อความยืนยันจากโมดูลยืนยันตัวตน เมื่อการเข้าระบบสำเร็จผู้ใช้สามารถเพิ่ม แก้ไข และลบข้อมูลผู้ใช้ภายในฐานข้อมูล ทั้งของนักศึกษา อาจารย์ และผู้ดูแลระบบ



รูปที่ . แผนภาพขั้นลำดับแสดงระบบส่งการบ้านร้องขอการยืนยันตัวตนแก่ผู้ใช้

การร้องขอการยืนยันตัวให้กับผู้ใช้ของระบบจัดการการส่งการบ้านปฏิบัติการ ใช้ข้อความร้องขอแบบแซมแอลซึ่งทำงานบนโพรโทคอลที่อยู่บนพื้นฐานข้อมูลแบบเอ็กซ์เอ็มแอล ทำให้การง่ายต่อการใช้เป็นบัตรผ่านเพื่อให้เบราเซอร์ของผู้ใช้ร้องขอยืนยันตัวตนแก่ผู้ใช้ โดยโมดูลยืนยันตัวตนจะเป็นส่วนคัดแยกว่าผู้ใช้เป็นนักศึกษา คณาจารย์ หรือผู้ดูแลระบบ ข้อความตอบกลับแซมแอลจะประกอบด้วยข้อมูลของผู้ใช้ เช่น ชนิดของผู้ใช้ที่ยืนยันตัวตนสำเร็จ ชื่อ นามสกุล เป็นต้น ทำให้ระบบจัดการการส่งการบ้านปฏิบัติการสามารถนำไปใช้ได้ทันที โดยไม่ต้องร้องขอข้อมูลจากโมดูลยืนยันตัวตนหลายครั้ง เพิ่มประสิทธิภาพในการทำงาน



รูปที่ . แผนภาพขั้นลำดับแสดงระบบจัดการการส่งการบ้านปฏิบัติการร้องขอข้อมูลนักศึกษา

เมื่อระบบภายนอกต้องการปรับปรุงข้อมูลให้มีความเป็นปัจจุบัน จึงต้องมีการร้องขอข้อมูลกับโมดูลยืนยันตัวตน โดยที่สามารถร้องขอได้ทีละผู้ใช้ หรือร้องขอแบบเป็นกลุ่มผู้ใช้จำแนกตามชื่อผู้ใช้ ซึ่งการร้องขอแบบกลุ่มมีข้อดีในการลดการส่งข้อมูลจำนวนหลายรอบ ช่วยเพิ่มประสิทธิภาพของเครื่องแม่ข่าย โมดูลยืนยันตัวตนจึงมีส่วนบริการข้อมูลนักศึกษาที่จะคอยรับคำร้องจากระบบภายนอก และคืนค่าข้อมูลนักศึกษาตามจำนวนที่ถูกร้องขอ

# บทที่ 4 การออกแบบฐานข้อมูล

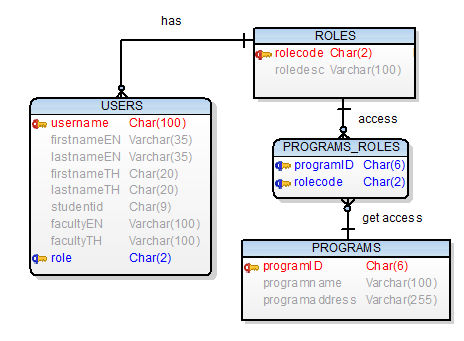
ในการพัฒนาการปรับปรุงโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ สำหรับการเตรียมข้อมูลเพื่อจัดทำฐานข้อมูล จำเป็นต้องศึกษาลักษณะเฉพาะของข้อมูล และรายละเอียดข้อมูลของผู้ใช้งานโมดูลยืนยันตัวตน เพื่อออกแบบความสัมพันธ์ของข้อมูลที่รองรับการทำงานของระบบด้วยความเหมาะสมสามารถแบ่งขั้นตอนการออกแบบฐานข้อมูลออกเป็น 3 ขั้นตอน คือ การออกแบบฐานข้อมูลในระดับความคิด (Conceptual Database Design) การออกแบบฐานข้อมูลในระดับตรรกะ (Logical Database Design) การออกแบบฐานข้อมูลระดับในกายภาพ (Data Dictionary) แต่ละขั้นตอนมีรายละเอียดดังนี้

## การออกแบบฐานข้อมูล

การออกแบบฐานข้อมูลของโมดูลยืนยันตัวตน อ้างอิงจากข้อมูลของผู้ใช้งานเป็นหลัก ประกอบด้วย นักศึกษา คณาจารย์ และผู้ดูแลระบบ จากการศึกษาข้อมูลสามารถสร้างความสัมพันธ์ของข้อมูล โดยใช้แผนภาพแสดงความสัมพันธ์ของเอนทิตี (Entity Relationship Diagram: ER - Diagram) แสดงความสัมพันธ์ระหว่างเอนทิตี โดยมีการแทนความสัมพันธ์ของข้อมูลโดยใช้สัญลักษณ์ดังตารางที่ 4.1 และรูปที่ 4.1 แสดงภาพความสัมพันธ์ของเอนทิตี้

ตารางที่ . แสดงสัญลักษณ์ที่ใช้ในการสร้างแผนภาพความสัมพันธ์ของเอนทิตี

|  |  |
| --- | --- |
| สัญลักษณ์ | คำอธิบาย |
|  | เอนทิตี (Entity) สิ่งที่สามารถระบุได้อย่างแจ้งชัด เป็นรูปธรรมหรือนามธรรม |
|  | คุณสมบัติ (Attribute) รายละเอียดที่เกี่ยวข้องกับลักษณะของเอนทิตี โดยคุณสมบัติมีอยู่ในทุกเอนทิตี |
|  | คุณสมบัติคีย์หลัก (Primary Key Attribute) ทำหน้าที่เป็นคีย์ที่มีคุณสมบัติของค่าข้อมูลไม่ซ้ำกัน |
|  | คุณสมบัติคีย์นอก (Foreign Key Attribute) ทำหน้าที่เป็นคีย์ที่มีคุณสมบัติ ได้มาจากคีย์หลักของเอนทิตีนอก |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ 1 : 1 (One to One Relationship) |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ 1 : N (One to Many Relationship) |
|  | อัตราส่วนความสัมพันธ์ของแถวข้อมูลระหว่างเอนทิตีแบบ M : N (Many to Many Relationship) |

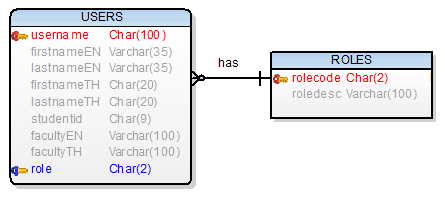


รูปที่ . แผนภาพความสัมพันธ์ระหว่างเอนทิตีต่างภายในโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่

### แผนภาพความสัมพันธ์ระหว่างเอนทิตี

จากแผนภาพแสดงความสัมพันธ์ดังรูปที่ 4.1 สามารถอธิบายความสัมพันธ์ระหว่างเอนทิตีได้ดังนี้

1. เอนทิตีผู้ใช้งานใช้อ้างถึงผู้ใช้งานทุกระดับการใช้งาน โดยผู้ใช้งานแต่ละคนมีบทบาทประจำตัวผู้ใช้งาน ซึ่งผู้ใช้งานมีได้แค่บทบาทเดียว แต่หนึ่งบทบาทมีได้หลายผู้ใช้ ดังนั้น ความสัมพันธ์ระหว่างสองเอนทิตีนี้มีความสัมพันธ์แบบกลุ่มต่อหนึ่ง ดังรูปที่ 4.2



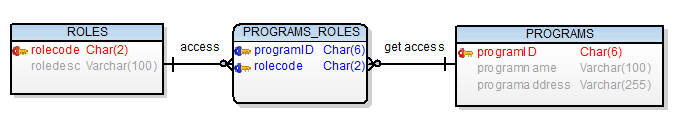
รูปที่ . แผนภาพความสัมพันธ์ระหว่างเอนทิตีผู้ใช้ และเอนทิตีบทบาท

จากผังความสัมพันธ์ของเอนทิตี สามารถแปลงแผนภาพเป็นความสัมพันธ์ ได้ดังนี้

USERS (username, firstnameEN, lastnameEN, firstnameTH, lastnameTH, studentid, facultyEN,   
 facultyTH, role)

ROLES (rolecode, roledesc)

1. เอนทิตีโปรแกรมใช้อ้างถึงโปรแกรมประยุกต์ที่ใช้งานโมดูลยืนยันตัวตน โดยผู้ใช้งานที่สามารถเข้าสู่การใช้งานโปรแกรมประยุกต์ขึ้นอยู่กับบทบาทของผู้ใช้งาน โดยหลายโปรแกรมสามารถถูกใช้งานโดยหลายบทบาทของผู้ใช้งาน ดังนั้น ความสัมพันธ์ระหว่างสองเอนทิตีนี้มีความสัมพันธ์แบบกลุ่มต่อกลุ่ม ดังรูปที่ 4.3 และจากลักษณะความสัมพันธ์ดังกล่าว ก่อให้เกิดเอนทิตีใหม่ คือ เอนทิตีแฝงความสัมพันธ์แบบกลุ่มต่อกลุ่ม ชื่อว่า โปรแกรม\_บทบาท (PROGRAMS\_ROLES)



รูปที่ . แผนภาพความสัมพันธ์ระหว่างเอนทิตีโปรแกรม และเอนทิตีบทบาท

จากผังความสัมพันธ์ของเอนทิตี สามารถแปลงแผนภาพเป็นความสัมพันธ์ ได้ดังนี้

ROLES (rolecode, roledesc)

PROGRAMS (programID, programname, programaddress)

PROGRAMS\_ROLES (programID, rolecode)

## การออกแบบฐานข้อมูลในระดับตรรกะและกายภาพ

การออกแบบฐานข้อมูลในระดับตรรกะและระดับกายภาพ เป็นขั้นตอนที่แปลงจากตัวแบบข้อมูลในระดับแนวคิด ซึ่งเป็นตัวแบบที่จะนำไปปฏิบัติใช้งานจริง โดยในขั้นตอนนี้จะได้ตารางที่ใช้สำหรับจัดเก็บข้อมูลของโมดูลยืนยันตัวตนเพื่อเข้าใช้ระบบจัดการการส่งการบ้านปฏิบัติการ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ จำนวน 4 ตาราง เพื่อให้ได้โครงสร้างของตารางที่ถูกต้องและลดความซ้ำซ้อนของข้อมูลภายในฐานข้อมูล ซึ่งแสดงรายละเอียดของตารางทั้งหมด ดังตาราง 4.2

ตารางที่ . ข้อมูลรายละเอียดของตารางทั้งหมดของโมดูล

|  |  |  |
| --- | --- | --- |
| **ลำดับที่** | **ชื่อตาราง** | **คำอธิบาย** |
| 1 | USERS | ตารางเก็บข้อมูลผู้ใช้งาน ประกอบด้วยลักษณะประจำดังนี้   * ชื่อผู้ใช้ (username) * ชื่อภาษาอังกฤษ (firstnameEN) * นามสกุลภาษาอังกฤษ (lastnameEN) * ชื่อภาษาไทย (firstnameTH) * นามสกุลภาษาไทย (lastnameTH) * รหัสนักศึกษา (studentid) * ชื่อคณะภาษาอังกฤษ (facultyEN) * ชื่อคณะภาษาไทย (facultyTH) * บทบาท (role) |
| 2 | PROGRAMS | ตารางเก็บข้อมูลโปรแกรมที่เชื่อมต่อกับโมดูล ประกอบด้วยลักษณะประจำดังนี้   * เลขโปรแกรม (programID) * ชื่อโปรแกรม (programname) * ที่อยู่โปรแกรม (programaddress) |
| 3 | ROLES | ตารางเก็บข้อมูลบทบาท ประกอบด้วยลักษณะประจำดังนี้   * รหัสบทบาท (rolecode) * คำอธิบายบทบาท (roledesc) |
| 4 | PROGRAMS\_ROLES | ตารางเก็บข้อมูลการใช้โปรแกรมของแต่ละบทบาท ประกอบด้วยลักษณะประจำดังนี้   * เลขโปรแกรม (programID) * รหัสบทบาท (rolecode) |