การพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ

โดย
นางสาวอัจฉริยา แซ่อึ้ง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ แผน ก แบบ ก 2 ระดับปริญญามหาบัณฑิต
ภาควิชาภาควิชาคอมพิวเตอร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2559

การพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ

โดย
นางสาวอัจฉริยา แซ่อึ้ง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ แผน ก แบบ ก 2 ระดับปริญญามหาบัณฑิต
ภาควิชาภาควิชาคอมพิวเตอร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2559

DEVELOPMENT OF CLOUD RESOURCES ACCESS MANAGEMENT SYSTEMS

By

MISS Ajchariya SAEUNG

A Thesis Submitted in partial Fulfillment of Requirements

for Master of Science (INFORMATION TECHNOLOGY)

Department of COMPUTER SCIENCE

Graduate School, Silpakorn University

Academic Year 2016

หัวข้อ	การพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ
โดย	อัจฉริยา แซ่อึ้ง
สาขาวิชา	เทคโนโลยีสารสนเทศ แผน ก แบบ ก 2 ระดับปริญญามหาบัณฑิต
อาจารย์ที่ปรึกษาหลัก	รองศาสตราจารย์ ดร. ปานใจ ธารทัศนวงศ์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ได้รับพิจารณาอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต

..... คณบดีบัณฑิตวิทยาลัย

(รองศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์)

พิจารณาเห็นชอบโดย

..... ประธานกรรมการ

(ดร. วัสรา รอดเหตุภัย)

..... อาจารย์ที่ปรึกษาหลัก

(รองศาสตราจารย์ ดร. ปานใจ ธารทัศนวงศ์)

..... ผู้ทรงคุณวุฒิภายใน

(ดร. ณัฐโชติ พรหมฤทธิ์)

..... ผู้ทรงคุณวุฒิภายนอก

(ดร. เฉลิมพล ชาญศรีภิญโญ)

57309304 : เทคโนโลยีสารสนเทศ แผน ก แบบ ก 2 ระดับปริญญามหาบัณฑิต
คำสำคัญ : การบริหารจัดการ, การเข้าใช้ทรัพยากร, ทรัพยากร, การประมวลผลแบบกลุ่มเมฆ

นางสาว อัจฉริยา แซ่อึ้ง: การพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ อาจารย์ที่ปรึกษาวิทยานิพนธ์ : รองศาสตราจารย์ ดร. ปานใจ ธารทัศนวงศ์

ในงานวิจัยนี้ได้พัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆโดยมีวัตถุประสงค์เพื่อศึกษาและพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆและเพื่อพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ โดยงานวิจัยนี้ได้ใช้เทคโนโลยี Shibboleth ในการพิสูจน์ตัวตนการเข้าใช้งานเพียงครั้งเดียวที่ทำงานเป็นตัวกลางในการส่งต่อเพื่อไปเข้าสู่ระบบโดยใช้เทคโนโลยี Active Directory บนระบบปฏิบัติการวินโดวส์และใช้เทคโนโลยี OpenLDAP บนระบบปฏิบัติงานลินุกซ์

โดยงานวิจัยนี้เป็นการพัฒนาบริหารจัดการทรัพยากรโดยเฉพาะทรัพยากรที่ต้องการความปลอดภัยสูง เช่น ระบบที่ใช้ในทางการแพทย์ ผู้วิจัยได้ใช้เทคโนโลยีการเข้าใช้ทรัพยากรโดยใช้โปรโตคอล SSL และ SFTP ในการแลกเปลี่ยนส่งไฟล์ระหว่างเครื่องเซิร์ฟเวอร์ที่อยู่บนระบบประมวลผลแบบกลุ่มเมฆทำให้ผู้ใช้สามารถเข้าไปบริหารจัดการทรัพยากรที่อยู่บนระบบปฏิบัติการลินุกซ์และระบบปฏิบัติการวินโดวส์ได้ โดยผู้ใช้สามารถจัดการได้ทั้งไฟล์และแอปพลิเคชันที่อยู่ในพื้นที่ของผู้ใช้เองไม่สามารถจัดการทรัพยากรของผู้อื่นได้ ทำให้ทรัพยากรที่อยู่บนระบบมีประสิทธิภาพทั้งด้านของการเข้าใช้และด้านของการจัดการ

57309304 : Major (INFORMATION TECHNOLOGY)
Keyword : Management, Access to resources, Resources, Cloud Computing

MISS Ajchariya SAEUNG: Development of cloud Resources Access Management Systems Thesis advisor : Associate Professor Panjai Tantatsanawong, Ph.D.

This research has developed a resource access management system on cloud computing. The objective of this research is this study and develop an authentication system for resource access management system on cloud computing and develop resource access management system. In this research used Shibboleth Single Sign On as a middleman to sign in both Active Directory on Windows OS and OpenLDAP on Linux OS.

This research is the development of resource management system, especially for high security resources like medical system. Researchers have access to resources using SSL and SFTP protocols to transfer files between servers running on cloud computing, users can manage resources on both the Linux OS and the Windows OS. The user can manage both files and applications that available in user's space, but the user can't manage the others resource. In this case, it makes the resources on the system are effective in term of acess and management.

กิตติกรรมประกาศ

ผู้วิจัยต้องขอขอบพระคุณ รองศาสตราจารย์ ดร. ปานใจ ธารทัศนวงศ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ที่ให้คำปรึกษาทั้งเรื่องทั่วไป ให้ความรู้ใหม่ๆ ตลอดเวลา ให้คำแนะนำรวมถึงคำชี้แนะแนวทางที่ควบคุมให้ไม่หลุดกรอบ ตลอดจนแนวทางในการทำวิจัย ให้สามารถสำเร็จลุล่วงไปได้ด้วยดี

ขอบขอบพระคุณอาจารย์ ดร. วัสรา รอดเหตุภัย ประธานกรรมการม อาจารย์ ดร. ณัฐโชติ พรหมฤทธิ์ กรรมการ และ ดร. เฉลิมพล ชาญศรีภิญโญ ผู้ทรงคุณวุฒิ ที่กรุณาให้คำแนะนำและตรวจสอบวิทยานิพนธ์

ขอบพระคุณครอบครัวที่คอยช่วยสนับสนุน ให้กำลังใจ ให้คำชี้แนะ ตลอดทุกวัน ทุกเวลา และขอบคุณเพื่อนสนิทที่คอยช่วยเหลือในการเสนอความคิดเห็นต่างๆ และให้กำลังใจตลอดเวลา

สุดท้ายนี้ขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ประสาทประสิทธิ์ความรู้ให้แก่ผู้วิจัย จนทำให้สามารถนำความรู้ที่มีมาใช้ในการดำเนินงานวิจัยจนสำเร็จลุล่วงเป็นวิทยานิพนธ์ฉบับนี้

อัจฉริยา แซ่อึ้ง

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1
บทนำ

ที่มาและความสำคัญของปัญหา

ระบบประมวลผลแบบกลุ่มเมฆเป็นระบบที่มีความหลากหลายในการให้บริการโดยประกอบไปด้วยเทคโนโลยีการให้บริการ 3 รูปแบบคือ 1) การให้บริการทางด้านซอฟต์แวร์ (Software as a service), 2) การให้บริการทางด้านแพลตฟอร์ม (Platform as a Service) และ 3) การให้บริการทางด้านโครงสร้าง (Infrastructure as a Service) และระบบประมวลผลแบบกลุ่มเมฆยังถูกแบ่งออกเป็น 3 ประเภทคือ ระบบประมวลผลแบบกลุ่มเมฆส่วนตัว, ระบบประมวลผลแบบกลุ่มเมฆสาธารณะและระบบประมวลผลแบบกลุ่มเมฆแบบผสม โดยในแต่ละการให้บริการของระบบประมวลผลแบบกลุ่มเมฆนี้มีจุดประสงค์เพื่อแบ่งปันทรัพยากรให้กับผู้ใช้ที่เข้ามาในระบบจึงทำให้ระบบบนทรัพยากรแบบกลุ่มเมฆจึงต้องมีความปลอดภัยในการเข้าถึงข้อมูล โดยการรักษาความปลอดภัยของข้อมูลนั้นจะถูกแบ่งระดับออกตามความสำคัญของข้อมูลที่จะทำการแบ่งปันหรือแบ่งออกตามประเภทของข้อมูลและในการจัดการบริหารทรัพยากรผู้ใช้จะต้องมีบัญชีการเข้าสู่ระบบทุกระบบที่ทำการลงทะเบียนไว้ ทำให้ผู้ใช้มีหลายบัญชีการเข้าใช้งานเมื่อจะเข้าสู่ระบบการจัดการใดจำเป็นจะต้องทำการเข้าสู่ระบบทุกครั้ง

จากปัญหาข้างต้น ผู้วิจัยจึงได้เสนอแนวทางการพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆและการจัดการการควบคุมการใช้งานระบบ โดยจะเน้นไปที่ระบบที่ต้องการความปลอดภัยสูง ๆ เช่น ระบบที่ใช้ในทางการแพทย์ เป็นต้น โดยวิธีการดำเนินงานผู้วิจัยได้แบ่งการทำงานออกเป็นสองส่วนคือการตรวจสอบตัวตนการเข้าใช้งานบนระบบประมวลผลแบบกลุ่มเมฆและการบริหารจัดการการใช้งานทรัพยากรที่อยู่บนระบบประมวลผลแบบกลุ่มเมฆ โดยผู้วิจัยได้นำเทคโนโลยีการตรวจสอบตัวตนและกำหนดสิทธิ์โดยใช้ Active Directory และ OpenLDAP ที่ได้รับมาตรฐานนำมาใช้กับระบบ เพื่อให้ผู้ใช้สามารถจัดการทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆได้อย่างมีความประสิทธิภาพและความปลอดภัย

ในงานวิจัยนี้ได้ใช้เทคโนโลยี Shibboleth ในตรวจสอบตัวตนและการทำระบบเข้าใช้งานเพียงครั้งเดียวทำงานเป็นเซิร์ฟเวอร์หลัก เทคโนโลยี Active Directory และ OpenLDAP ทำงานบน

เซิร์ฟเวอร์ที่ให้บริการแอปพลิเคชันโดย Active Directory จะถูกติดตั้งบนผู้ให้บริการระบบประมวลผลแบบกลุ่มเมฆคือ Amazon Web Services (AWS) และการบริหารจัดการทรัพยากรจะเทคโนโลยีของ SSH ในการจัดการทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ

วัตถุประสงค์ของงานวิจัย

1. เพื่อศึกษาและพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ
2. เพื่อพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ

ขอบเขตของงานวิจัย

1. ศึกษากลไกพิสูจน์ตัวตนผู้ใช้สำหรับระบบปฏิบัติการลินุกซ์และระบบปฏิบัติการวินโดวส์เพื่อที่จะระบุกลไกการพิสูจน์ตัวตนผู้ใช้ที่เหมาะสมและสามารถทำงานร่วมกันระหว่างแพลตฟอร์ม
2. ออกแบบและพัฒนาระบบพิสูจน์ตัวตนที่มีความสามารถในการทำการเข้าใช้งานครั้งเดียวสำหรับเข้าใช้งานระบบได้ทั้งสองระบบปฏิบัติการ
3. ออกแบบและพัฒนาส่วนเชื่อมต่อกับแอปพลิเคชันระหว่างระบบที่พัฒนาและ Active Directory, Shibboleth และ OpenLDAP ที่สามารถใช้งานได้ทั้งสองระบบปฏิบัติการ
4. ออกแบบและพัฒนาระบบตัวอย่างแอปพลิเคชันสารสนเทศทางการแพทย์คือ ระบบคัดกรองผู้ป่วยโรคหัวใจและระบบคัดกรองผู้ป่วยโรคเบาหวาน

ประโยชน์ที่คาดว่าจะได้รับ

1. ได้กลไกการพิสูจน์ตัวตนที่สามารถทำงานร่วมกันระหว่างระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์บนระบบประมวลผลแบบกลุ่มเมฆ
2. ได้ระบบจัดการผู้ใช้งานบนระบบประมวลผลแบบกลุ่มเมฆ
3. ได้ระบบบริหารจัดการทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ

เครื่องมือและอุปกรณ์

ฮาร์ดแวร์

1. CPU Intel Celeron 2.40 GHz
2. RAM 4 GB
3. Hard disk 500 GB

ซอฟต์แวร์

1. VMWare Workstation 11
2. CentOS 6.0
3. Windows Server 2008 R2
4. Active directory (Windows)
5. OpenLDAP
6. Shibboleth
7. PHP

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในงานวิจัยการพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆได้มีการศึกษาทฤษฎีและผลงานวิจัยที่เกี่ยวข้องกับงานวิจัยนี้โดยจะประกอบไปด้วยทฤษฎีระบบประมวลผลแบบกลุ่มเมฆ, ทฤษฎีเทคโนโลยีการยืนยันตัวตน, ทฤษฎีเทคโนโลยีการจัดการทรัพยากรและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีของระบบประมวลผลแบบกลุ่มเมฆ

Cloud Computing [1]

คลาวด์คอมพิวติ้ง (Cloud Computing) หรือ กระบวนการประมวลผลแบบกลุ่มเมฆ คือรูปแบบการให้บริการประมวลผลคอมพิวเตอร์ที่ผู้ใช้ไม่ต้องดูแลระบบเซิฟเวอร์ เพียงแต่เช่าใช้บริการโดยผู้ใช้บริการสามารถเพิ่มหรือลดขนาดของฮาร์ดแวร์ เช่น ซีพียู เมมโมรี่ โดยไม่ต้องปรับเปลี่ยนแอปพลิเคชันหรือซอฟต์แวร์ใหม่

รูปที่ 2-1 แสดงอุปกรณ์ที่สามารถเข้าถึงระบบประมวลผลแบบกลุ่มเมฆ
ที่มา : Tom Dheere, Cloud-Based Tools [ออนไลน์], เข้าถึงเมื่อ 25 ธันวาคม 2558

เข้าถึงได้จาก: https://www.linkedin.com/pulse/my-3-favorite-cloud-based-tools-gkn-weekly-update-4715-tom-dheere

จากรูปที่ 2-1 แสดงอุปกรณ์ที่สามารถเข้าถึงระบบประมวลผลแบบกลุ่มเมฆโดยการประมวลผลแบบกลุ่มเมฆนี้จะสามารถจัดเก็บทรัพยากรได้หลายรูปแบบเช่น เอกสาร, รูปภาพ, อีเมล หรือแอปพลิเคชันที่มีการป้องกันการเข้าถึงอยู่ ในการจัดการเรื่องประสิทธิภาพของการประมวลผลของระบบประมวลผลแบบกลุ่มเมฆเกิดจากการที่ระบบประกอบไปด้วยคอมพิวเตอร์หลาย ๆ เครื่องทำงานร่วมกัน จะประกอบไปด้วยกลุ่มของเซิร์ฟเวอร์ ซึ่งมีเป็นจำนวนมาก

ประเภทของระบบประมวลผลแบบกลุ่มเมฆ

การประมวลผลแบบประมวลผลแบบกลุ่มเมฆสามารถแบ่งออกเป็น 3 กลุ่มใหญ่ๆ คือ

1. Private Cloud หรือระบบประมวลผลบนกลุ่มเมฆส่วนตัวเป็นการใช้งานภายในองค์กร โดยใช้ศักยภาพของศูนย์ข้อมูลภายในองค์กร
2. Public Cloud หรือระบบประมวลผลบนกลุ่มเมฆสาธารณะเป็นรูปแบบที่มีผู้ให้บริการสาธารณะ การเข้าถึงข้อมูลจะผ่านทางอินเทอร์เน็ต
3. Hybrid Cloud หรือระบบประมวลผลบนกลุ่มเมฆแบบผสม เป็นรูปแบบการรวมกันระหว่างระบบประมวลผลบนกลุ่มเมฆส่วนตัวและระบบประมวลผลบนกลุ่มเมฆแบบสาธารณะซึ่งเพิ่มความยืดหยุ่นในการจัดการได้มากขึ้น

ทฤษฎีเทคโนโลยีการยืนยันตัวตน

ในงานวิจัยนี้ได้นำเทคโนโลยีการยืนยันตัวตนที่มีความปลอดภัยสูงและเทคโนโลยีที่เกี่ยวข้องมาพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆโดยเทคโนโลยีที่ใช้มีดังต่อไปนี้

Directory [2]

ไดเรกทอรี คือ ฐานข้อมูลที่จัดเก็บข้อมูลเกี่ยวกับสิ่งใดสิ่งหนึ่งโดยจะแบ่งออกเป็นไดเรกทอรีของระบบไฟล์ จะจัดเก็บข้อมูลเกี่ยวกับไฟล์ต่าง ๆ และไดเรกทอรีเครือข่ายเก็บทรัพยากรเกี่ยวกับเครือข่ายและให้บริการข้อมูลเกี่ยวกับทรัพยากรที่มีอยู่รวมถึงข้อมูลการเข้าใช้

ประโยชน์ของบริการไดเรกทอรี

1. การค้นหาข้อมูล : ผู้ใช้ที่ต้องการที่ค้นหาข้อมูลที่มีอยู่ในเครือข่าย ไดเรกทอรีจะจัดเก็บข้อมูลเหล่านี้ เช่น อีเมล, เบอร์โทรศัพท์, ตำแหน่ง
2. ระบบรักษาความปลอดภัย : ไดเรกทอรีทำหน้าที่เป็นระบบรักษาความปลอดภัยในการตรวจสอบการเข้าใช้ทรัพยากรต่าง ๆ ผู้ใช้อาจต้องล็อกอินเพื่อตรวจสอบสิทธิ
3. การรวบรวมระบบ : ในองค์กรจะมีระบบเฉพาะหลายๆ ระบบ ไดเรกทอรีบางประเภทสามารถแลกเปลี่ยนข้อมูลระหว่างระบบได้
4. การบริหารและจัดการเครือข่ายแบบศูนย์รวม : ไดเรกทอรีเป็นเครื่องมือหนึ่งที่ใช้จัดการทรัพยากรต่าง ๆ

มาตรฐานของ X.500 [3]

ระบบจะประกอบด้วยออบเจ็กต์ประเภทต่าง ๆ เช่น ผู้ใช้หรือคอมพิวเตอร์ โดยโครงสร้างของมาตรฐานนี้ประกอบด้วย DUA (Directory User Agent) และ DSA (Directory System Agent) และมีโปรโตคอลที่ใช้เข้าถึงอยู่สองโปรโตคอล คือ

- DAP (Directory Access Protocol) : เป็นโปรโตคอลที่ DUA ใช้เรียกข้อมูลจากไดเรกทอรีเซิร์ฟเวอร์

- DSP (Directory System Protocol) : เป็นโปรโตคอลที่ใช้สื่อสารกันระหว่างผู้ใช้

โครงสร้างของฐานข้อมูลแบบทรี

โครงสร้างฐานข้อมูลแบบต้นไม้และรูปแบบของข้อมูลที่เก็บไว้ดังนั้น โครงสร้างของฐานข้อมูลแบบทรีของไดเรกทอรีเป็นตัวกำหนดคุณสมบัติของออบเจ็กต์ประเภทต่าง ๆ ในการสร้างออบเจ็กต์ใหม่ต้องกำหนดค่าออบเจ็กต์นั้นอยู่ในคลาสใด ๆ ของโครงสร้างของฐานข้อมูลแบบทรี

การเรียกชื่อออบเจ็กต์ใน X.500

การเรียกชื่อแบ่งออกเป็น 2 ประเภทคือ

- DN (Distinguished Name): เป็นชื่อเฉพาะที่แต่ละออบเจ็กต์ไม่ซ้ำกัน

- RDN (Relative Distinguished Name): ชื่อสัมพันธ์ เป็นส่วนหนึ่งของ DN

Directory Access Protocol (DAP)

เป็นโปรโตคอลที่ออกแบบมาให้ผู้ใช้หรือ DUA ร้องขอข้อมูลจาก DSA ประกอบด้วย 5 ฟังก์ชัน คือ

- Read: ผู้ใช้ร้องขอข้อมูลของออบเจ็กต์ในไดเรกทอรีซึ่งอาจเป็นแอตทริบิวต์ทั้งหมดหรือค่าบางค่า
- Compare: การร้องขอข้อมูลของแอตทริบิวต์ของออบเจ็กต์ เช่น การตรวจสอบรหัสลับ ผู้ใช้จะไม่มีสิทธิ์อ่านแต่สามารถเปรียบเทียบค่าในไดเรกทอรีได้
- List: การร้องขอรายการที่อยู่ภายใต้ต้นไม้ย่อยใน DIT
- Abandon: ยกเลิกการร้องขอจากผู้ใช้

นอกจากนี้ DAP สามารถปรับเปลี่ยนหรือเพิ่มออบเจ็กต์ใหม่ในไดเรกทอรีได้ ซึ่งมี 4 ฟังก์ชัน คือ

- Add: การเพิ่มออบเจ็กต์ใหม่ในไดเรกทอรี
- Remove: การลบออบเจ็กต์ที่มีอยู่
- Modified: ปรับเปลี่ยนค่าแอตทริบิวต์
- Modified Distinguished Name: การร้องขอเพื่อเปลี่ยนค่าของ RDN ของออบเจ็กต์ซึ่งอาจเป็นการย้ายเอนทรีไปไว้ในต้นไม้ย่อยใหม่

LDAP (Lightweight Directory Access Protocol) [4]

LDAP ถูกยอมรับให้เป็นโปรโตคอลมาตรฐานสำหรับเข้าใช้ไดเรกทอรีโดยผู้ใช้ของ LDAP จะติดต่อกับ DSA โดยผ่าน LDAP Provider หรือ LDAP Server ใช้โปรโตคอล TCP แทนการใช้ OSI โดย LDAP ประกอบด้วย 3 ฟังก์ชันคือ

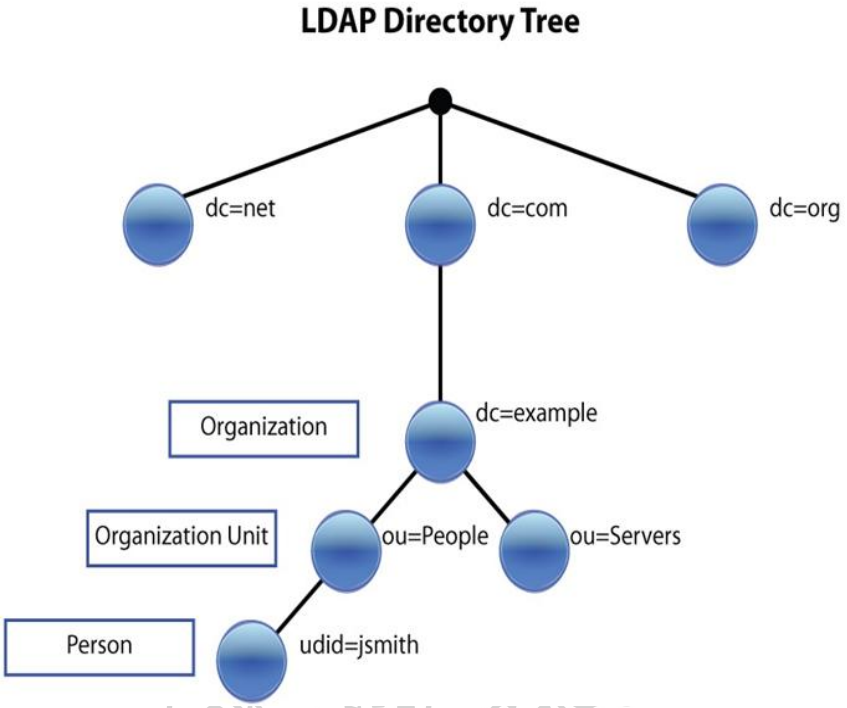
1. Compare : ใช้เปรียบเทียบค่าแอตทริบิวต์
2. Search : ใช้ค้นหาเอนทรีในไดเรกทอรี
3. Abandon : ยกเลิกการขอข้อมูล

OpenLDAP

โครงสร้างและรูปแบบข้อมูลที่จัดเก็บใน LDAP อยู่บนพื้นฐานเอนทรีโดยเอนทรีเป็นชุดข้อมูลซึ่งประกอบด้วยแอตทริบิวต์ที่มีชื่อเฉพาะ (DN) ซึ่งจะชี้ไปยังแต่ละเอนทรีในไดเรกทอรีแต่ละแอตทริบิวต์ของเอนทรีจะจัดเป็น Type และมีค่า Value ที่กำหนดให้กับแอตทริบิวต์นั้น ๆ

การเรียกชื่อและค้นหา แต่ละเอนทรีจะถูกอ้างถึงโดยใช้ชื่อเฉพาะ (DN) และตามด้วยชื่อของเอ็นทรีที่อยู่ระดับเหนือกว่า สามารถค้นหาและอ่านค่าข้อมูลได้เฉพาะบางส่วนของฐานข้อมูลโดยเปรียบเทียบเงื่อนไขที่กำหนดตอนค้นหา

รูปแบบโครงสร้างต้นไม้โดย LDAP จะอนุญาตให้สามารถควบคุมแอตทริบิวต์ว่าอะไรที่จำเป็นต้องมีหรือไม่มี โดยกำหนดผ่านแอตทริบิวต์พิเศษชื่อ objectClass ค่าที่กำหนดให้กับ objectClass จะกำหนดกฎสกีมาที่เอ็นทรีนั้นจะต้องมีในการเรียกชื่อและการค้นหา แต่ละเอ็นทรีจะถูกอ้างถึงได้โดยใช้ชื่อเฉพาะหรือ DN ซึ่งชื่อเฉพาะนี้จะประกอบด้วยชื่อของเอ็นทรีนั้นหรือ RDN และตามด้วยชื่อที่อยู่ระดับเหนือกว่าดังรูปที่ 2-2 แสดงโครงสร้างไดเรกทอรีLDAP จะมีชื่อ RDN เป็น udid=jsmith ส่วนชื่อเฉพาะ DN ก็จะเป็น udid=jsmith, ou=People, dc=example, dc=com รูปแบบข้อมูลของชื่อเฉพาะ DN ได้กำหนดไว้ใน RFC2253



รูปที่ 2-2 แสดงโครงสร้างไดเรกทอรีLDAP

ที่มา : Craig Ellrod, LDAP Authentication [ออนไลน์], เข้าถึงเมื่อ 29 มกราคม 2559

เข้าถึงได้จาก : https://www.citrix.com/blogs/2010/11/05/load-balancing-ldap-authentication

Active Directory (AD) [5]

เป็นบริการในการจัดการทรัพยากรของเครือข่ายพร้อมทั้งมีระบบรักษาความปลอดภัยในการเข้าใช้ทรัพยากรโดยจะจัดเก็บข้อมูลเกี่ยวกับออบเจ็กต์ต่างๆ เช่น ผู้ใช้, กลุ่มผู้ใช้, คอมพิวเตอร์, โดเมน , หน่วยย่อยองค์กร และ นโยบายการรักษาความปลอดภัย ไดเรกทอรีนั้นจะถูกเก็บไว้ที่ Domain Controller หรือ DC ซึ่งผู้ดูแลระบบ, ผู้ใช้ หรือ แอปพลิเคชันสามารถเข้าใช้ข้อมูลที่จัดเก็บได้

โครงสร้างของ Active Directory (AD)

เซิร์ฟเวอร์ที่ติดตั้ง AD จะถูกเรียกว่า Domain Controller ซึ่งในหนึ่งโดเมนอาจมี DC หลายเครื่อง โดยแต่ละเครื่องสามารถเปลี่ยนแปลงฐานข้อมูลได้ และถ้ามีการเปลี่ยนแปลงเครื่องนั้นจะส่งการเปลี่ยนแปลงไปยัง DC อื่น ๆ ในโดเมนอัตโนมัติ

โครงสร้างของฐานข้อมูลแบบทรี AD

- Object: ออบเจ็กต์เก็บข้อมูลของสิ่งต่างๆ ที่อยู่ในเครือข่าย

- Attributes: เป็นคุณสมบัติของออบเจ็กต์

- Schema: เป็นตัวกำหนดว่าออบเจ็กต์แต่ละประเภทมีคุณลักษณะใดบ้าง

- Containers: จะมีลักษณะคล้ายกับโฟลเดอร์ในระบบไฟล์ คอนเทนเนอร์ใน AD จะแบ่งออกเป็น 3 ประเภทดังนี้

1. Domains : เป็นขอบเขตของการรักษาความปลอดภัย
2. Sites : จะแทนเครือข่ายที่เชื่อมต่อกันด้วยแบนด์วิดธ์สูงๆ เช่น แลน
3. Organizational Units : เป็นคอนเทนเนอร์ที่สามารถใส่คอมพิวเตอร์ ผู้ใช้ เครื่องพิมพ์ แต่ไม่สามารถใส่ออบเจ็กต์จากโดเมนอื่นได้

Context and Naming

ใน Window NT ชื่อคอมพิวเตอร์จะเป็นชื่อแบบ NetBIOS ซึ่งมีความยาวไม่เกิน 15 ตัวอักษร ส่วนใน Windows 2000/2003 เรียกชื่อจะใช้ตามมาตรฐาน LDAP โดยแบ่งออกเป็นสองประเภทคือ ชื่อเฉพาะ DN และชื่อทั่วไป CN ซึ่งชื่อนี้จะชี้ไปยังออบเจ็กต์ที่อยู่ในไดเรกทอรี ประกอบด้วยส่วนต่าง ๆ ดังนี้

- DC – Domain Component: ชื่อโดเมน

- OU – Organizational Unit: ชื่อองค์กรย่อย

- CN – Common Name: แอตทริบิวต์ที่บอกชื่อออบเจ็กต์

Global Catalog (GC)

GC เป็นเซอร์วิสที่ช่วยในการค้นหาออบเจ็กต์ในไดเรกทอรีเป็นโดเมนคอนโทรลเลอร์ที่จัดเก็บข้อมูลของออบเจ็กต์ เมื่อออบเจ็กต์ใหม่ถูกสร้างและเพิ่มเข้าไปในไดเรกทอรี AD จะกำหนดหมายเลขเฉพาะสำหรับออบเจ็กต์นั้น ซึ่งเรียกหมายเลขนั้นว่า GUID (Globally Unique Identifier)

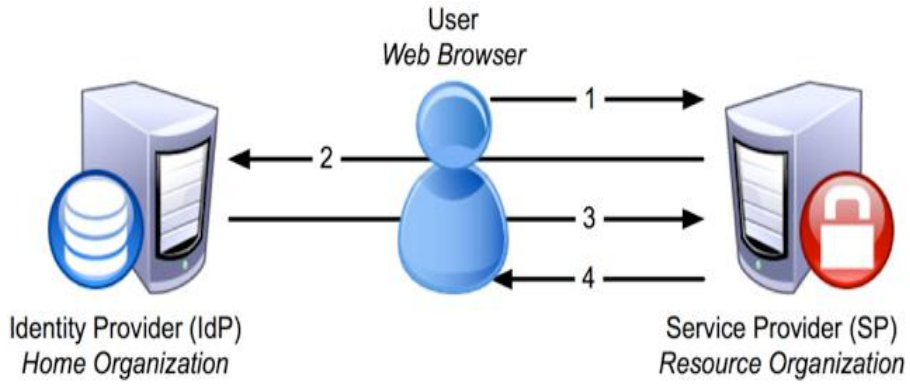
Replication and Security

เป็นการถ่ายโอนฐานข้อมูลระหว่างเซิร์ฟเวอร์โดยต้องมั่นใจว่า ทุก ๆ เซิร์ฟเวอร์มีฐานข้อมูลที่เหมือนกันทั้งหมด ระบบการรักษาความปลอดภัยนั้นได้ถูกรวมเข้ากับ AD ตั้งแต่การล็อกอินและควบคุมการเข้าใช้ รองรับการเข้าใช้งานแบบครั้งเดียว

ใน Active Directory จะมีส่วนที่เพิ่มขึ้นมาตั้งแต่วินโดวส์ 2008 คือ Active Directory Domain Services (ADDS) จะเป็นบทบาทที่ทำงานเกี่ยวกับการตรวจสอบตัวตนและสิทธิการเข้าใช้งานทรัพยากรเบนเครื่อง (Authentication & Authorization) โดยเป็นศูนย์กลางในการจัดการการเข้าถึงทรัพยากรในระบบ

Shibboleth [6]

เป็นงานหนึ่งของ Internet2 นำมาใช้สำหรับการจัดการการระบุตัวตนและเป็นระบบแบบรวมได้ (Federated System) โดยมี OASIS SAML (Organization for the Advancement of Structured Information System, Security Assertion Markup Language) เป็นมาตรฐานที่กำหนดรูปแบบในการร้องขอ, การสร้าง, การสื่อสาร และการยืนยัน คือ โครงสร้างในการยืนยันตัวตนและกำหนดสิทธิบนพื้นฐาน SAML ใช้แนวคิดของ Federated Identity โดยระบบนี้ แบ่งออกเป็นสองส่วนคือผู้ให้บริการข้อมูล หรือ Identity Provider (IdP) และผู้ให้บริการเครือข่ายหรือ Service Provider (SP)



รูปที่ 2-3 กระบวนการ Shibboleth

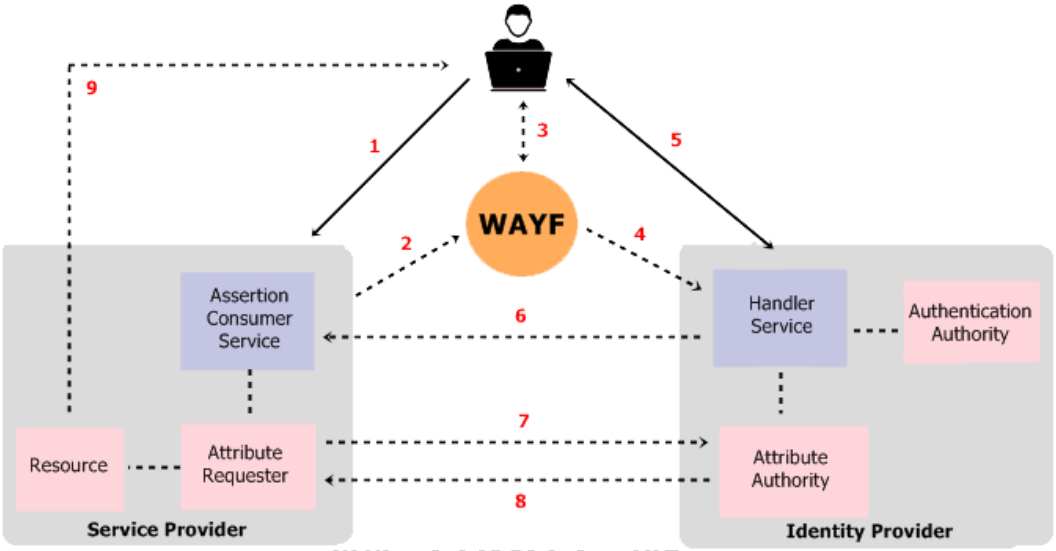
ที่มา : Scott Cantor, Basic Interaction [ออนไลน์], เข้าถึงเมื่อ 29 กรกฎาคม 2559

เข้าถึงได้จาก : https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

จากรูปที่ 2-3 กระบวนการ Shibboleth แสดงให้เห็นถึงการเชื่อมต่อระหว่างผู้ใช้งานที่กำลังใช้งานผ่านเว็บเบราว์เซอร์โดยการตรวจสอบตัวตนผ่านผู้ให้บริการข้อมูลกับผู้ให้บริการเครือข่ายที่เก็บทรัพยากรตั้งอยู่ที่อื่นขั้นตอนการส่งข้อมูลของ Shibboleth มีดังต่อไปนี้

1. ผู้ใช้พยายามจะเข้าถึงทรัพยากรโดยผู้ให้บริการเครือข่ายตรวจพบเจอผู้ใช้งาน
2. SP สร้างการร้องขอการยืนยันตัวตนโดยการส่งคำร้องขอไปที่ผู้ให้บริการข้อมูล
3. เมื่อผู้ให้บริการข้อมูลตรวจสอบสิทธิ์ของผู้ใช้แล้ว จะส่งการยืนยันตัวตนและสิทธิ์กลับมาที่ผู้ให้บริการเครือข่าย
4. เมื่อผู้ให้บริการเครือข่ายตรวจสอบสิ่งที่ผู้ให้บริการข้อมูลส่งกลับมาแล้วจะทำการส่งทรัพยากรกลับไปยังผู้ใช้ต่อไป

WAYF (“Where Are You Form”) หรือ Discovery Service คือส่วนหนึ่งของ Shibboleth ที่จะทำการค้นหาคีย์หรือกุญแจที่อยู่ในไฟล์เมตาดาต้า SAML2 เพื่อเลือกผู้ให้บริการข้อมูล ที่ต้องการและทำการตรวจสอบความถูกต้องของข้อมูลที่ทำการร้องขอ กระบวนการของ Shibboleth จะแสดงอยู่ในรูปที่ 2-4 กระบวนการการทำงานภายใน Shibboleth



รูปที่ 2-4 กระบวนการการทำงานภายใน Shibboleth

ที่มา : SWITCHaai, WAYF Service [ออนไลน์], เข้าถึงเมื่อ 29 กรกฎาคม 2559

เข้าถึงได้จาก : https://www.switch.ch/aai/support/tools/wayf/

จากรูปที่ 2-4 กระบวนการการทำงานภายใน Shibboleth แสดงถึงขั้นตอนการดำเนินงานในกรณีที่ผู้ใช้จะต้องลงทะเบียนไว้ที่ผู้ให้บริการข้อมูลไว้แล้วโดยกระบวนการการทำงานมีขั้นตอนดังต่อไปนี้

1. ผู้ใช้พยายามเข้าถึงทรัพยากรที่อยู่บนผู้ให้บริการเครือข่ายของ Shibboleth
2. Shibboleth จะทำการส่งคำร้องขอไปยัง WAYF
3. ผู้ใช้ทำการเลือกผู้ให้บริการข้อมูลที่ต้องการเข้าถึง
4. WAYF จะส่งต่อข้อมูลมาตรวจสอบที่การจัดการบริการ (Handle Service) ที่อยู่ในผู้ให้บริการข้อมูล
5. ระบบจะส่งกลับมาที่ผู้ใช้เพื่อให้ผู้ใช้ป้อนข้อมูลรับรองความถูกต้อง (ชื่อผู้ใช้ และรหัสผ่าน) และจะถูกส่งกลับมาที่การจัดการบริการ เพื่อทำการค้นหาทรัพยากรที่ผู้ใช้สามารถเข้าถึงได้โดยผ่านกระบวนการการส่งข้อมูลการยืนยันตัวตนไปยังขั้นตอนรับรองคุณสมบัติ (Attribute Authority) และขั้นตอนการรับรองตัวตน (Authentication Authority)
6. ขั้นตอนการตรวจสอบการยืนยันจากฝั่งผู้ให้บริการข้อมูลจะถูกส่งมาที่ฝั่งผู้ให้บริการเครือข่าย ในการยืนยันการให้บริการ (Assertion Consumer Service) โดยการสร้างเซสชัน

7. เมื่อตรวจสอบแล้วจะทำการร้องขอคุณลักษณะสำหรับผู้ใช้ไปยังผู้ให้บริการข้อมูล
8. ผู้ให้บริการข้อมูลจะส่งคุณลักษณะของผู้ใช้กลับมายังผู้ให้บริการเครือข่าย
9. ผู้ให้บริการเครือข่ายจะส่งคุณลักษณะและข้อมูลทรัพยากร (Resource) ที่ร้องขอกลับไปให้ผู้ใช้

เปรียบเทียบเทคโนโลยีตรวจสอบสิทธิ์

จะเห็นว่าการทำงานของ Shibboleth, OpenLDAP และ Active Directory จะมีความคล้ายคลึงกันตรงที่ทั้งสามเทคโนโลยีนี้มีระบบการทำการเข้าใช้งานเพียงครั้งเดียว แต่จะมีความต่างตรงระบบจัดการเฉพาะตัว ประสิทธิภาพในการทำงาน และ การรองรับระบบปฏิบัติการต่าง ๆ ดังตารางที่ 2-1 เปรียบเทียบข้อแตกต่างของเทคโนโลยีการยืนยันตัวตน

ตารางที่ 2-1 เปรียบเทียบข้อแตกต่างของเทคโนโลยีการยืนยันตัวตน

	Shibboleth	LDAP	Active Directory
บทบาท	แก้ปัญหาในการยืนยันตัวตนแบบศูนย์รวม เชื่อมโยงไปยังผู้ใช้ภายในและภายนอกองค์กร	- เป็นโปรโตคอลเพื่อเข้าถึงบริการไดเรกทอรี	เป็นระบบฐานข้อมูลที่มีจัดให้มีการตรวจสอบตัวตน, ไดเรกทอรี, นโยบายและการให้บริการอื่นๆ
วัตถุประสงค์	ขยายการให้บริการการเข้าใช้งานแบบครั้งเดียวไปยังภายนอกองค์กร	ตรวจสอบความถูกต้องตามชั้นความปลอดภัย	อนุญาตให้ผู้ใช้จัดระบบไฟล์ในการเข้าถึงแบบไดเรกทอรีได้
ระบบปฏิบัติการ	ลินุกซ์ หรือ วินโดวส์	ลินุกซ์	วินโดวส์
รองรับการเข้าใช้งานแบบครั้งเดียว	เว็บเซอร์วิสเพียงอย่างเดียว	รองรับ	รองรับ
ระดับ	องค์กรขนาดใหญ่	องค์กร	ส่วนบุคคล

ทฤษฎีเทคโนโลยีการจัดการทรัพยากร

SSH (Secure Shell) [7]

เป็นโปรโตคอลเครือข่ายที่ให้ผู้ดูแลระบบสามารถเข้าถึงคอมพิวเตอร์ระยะไกลและแลกเปลี่ยนข้อมูลได้อย่างปลอดภัย โดยมีการตรวจสอบความถูกต้องและการแลกเปลี่ยนสื่อสารข้อมูลที่ถูกเข้ารหัสลับไว้ ระหว่างคอมพิวเตอร์สองเครื่องที่เชื่อมต่อผ่านเครือข่ายที่ไม่ปลอดภัยเช่น อินเทอร์เน็ต SSH ได้มี SSH-1 [8] ซึ่งเป็นโปรโตคอลที่ได้รับการพัฒนาขึ้นในปี 1995 โดย Tatu Ylönen เป็นนักวิจัยจาก Helsinki University of Technology ประเทศฟินแลนด์ SSH มีสถาปัตยกรรมแบบไคลเอ็นต์ / เซิร์ฟเวอร์ และการเข้ารหัสลับที่มีความปลอดภัยสูงเพื่อป้องกันดักฟังและการโจมตีจากที่อื่น โดยปกติแล้ว SSH จะทำงานบนระบบปฏิบัติการที่เป็น LINUX หรือ UNIX โดย SSH นี้ได้ถูกใช้กันอย่างแพร่หลายในการจัดการระบบและแอปพลิเคชันในระยะไกล

คุณลักษณะของ SSH [9]

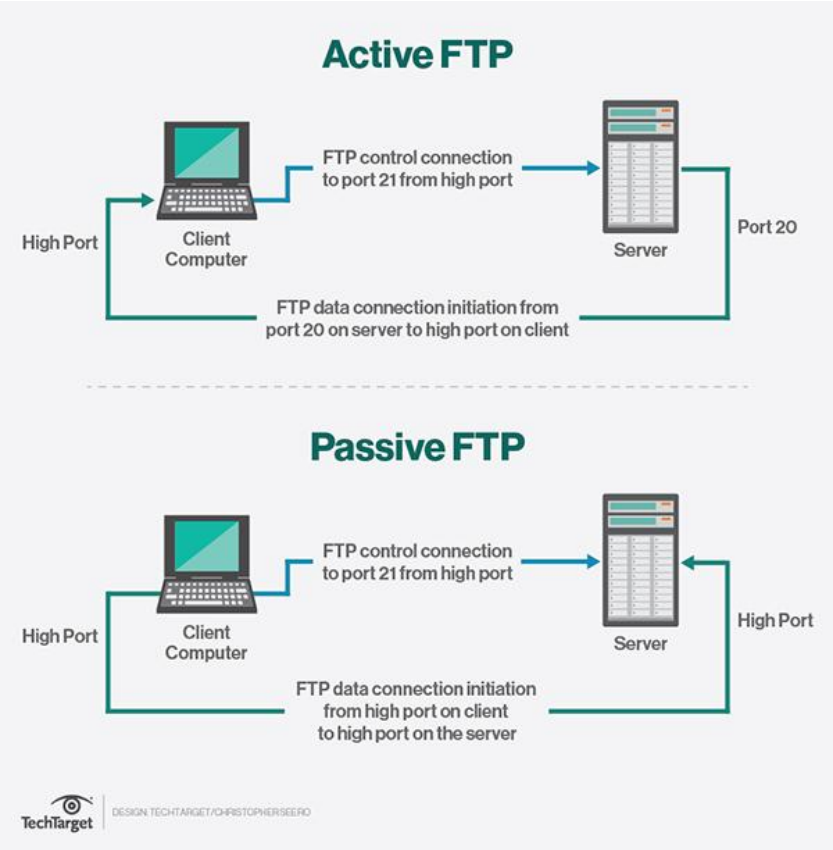
1. Privacy: ความเป็นส่วนตัวของข้อมูลที่ถูกเข้ารหัสที่แข็งแกร่ง
2. Integrity: ความสมบูรณ์ของการสื่อสารระหว่างข้อมูล
3. Authentication: การตรวจสอบตัวตนเช่นหลักฐานการระบุตัวตนของผู้ส่งและผู้รับ
4. Authorization: การกำหนดสิทธิ์หรือการอนุญาตให้เข้าถึงบัญชีได้
5. Forwarding: เส้นทางที่เข้ารหัสบนพื้นฐานเซสชันของ TCP/IP

FTP (File Transfer Protocol) [10]

FTP เป็นโปรโตคอลมาตรฐานสำหรับการส่งไฟล์ระหว่างคอมพิวเตอร์บนอินเทอร์เน็ตผ่านทาง TCP/IP มีสถาปัตยกรรมแบบไคลเอ็นต์/เซิร์ฟเวอร์ มีความปลอดภัยในการแลกเปลี่ยนไฟล์ผ่านอินเทอร์เน็ตโดยผู้ใช้สามารถอัพโหลด, ดาวน์โหลด, เปลี่ยนชื่อ, ย้ายไฟล์, หรือคัดลอกได้

FTP จะแบ่งการทำงานออกเป็นสองโหมดคือ โหมดการไม่ทำงาน (Passive Mode) และโหมดการทำงาน (Active Mode) โดยโหมดการทำงานนี้จะเริ่มขึ้นตั้งแต่ที่ผู้ใช้เริ่มต้นใช้คำสั่งในการเชื่อมต่อข้อมูลกับเครื่องเซิร์ฟเวอร์เพื่อการถ่ายโอนข้อมูล ส่วนโหมดการไม่ทำงานนี้จะใช้ช่องคำสั่งเพื่อส่งข้อมูลไปให้ผู้ใช้โดยผู้ใช้ต้องทำการเปิดช่องรับข้อมูลไว้ด้วย จะทำงานได้ดีในการข้ามไฟร์วอลล์และการใช้เกตเวย์แบบ NAT (Network Address Translation) ดังรูปที่ 2-5 แสดงโมเดลการทำงานและ

ไม่ทำงานของ FTP โดย FTP นี้จะมีโปรโตคอลที่เรียกว่า SFTP (Secured File Transfer Protocol) เป็นโปรโตคอลที่นำมาใช้แทน FTP โดยเป็นส่วนหนึ่งของ SSH



รูปที่ 2-5 แสดงโมเดลการทำงานและไม่ทำงานของ FTP
ที่มา : Margaret Rouse, File Transfer Protocol [ออนไลน์], เข้าถึงเมื่อ 26 กรกฎาคม 2560

เข้าถึงได้จาก: http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol

งานวิจัยที่เกี่ยวข้อง

Courtney Powell, Takashi Aizawa, Masaharu Munetomo (2012) [11] ได้ออกแบบโครงสร้างการยืนยันตัวบุคคลสำหรับการจัดการระบบการกระจายไปยังระบบประมวลผลแบบกลุ่มเมฆที่ต่างชนิดกันโดยจัดการระบบประมวลผลแบบกลุ่มเมฆส่วนมิดเดิลแวร์ไปยังการสื่อสารแลกเปลี่ยนข้อมูลหรือการใช้โปรแกรมระหว่างระบบรวมเข้ากับระบบการประมวลผลแบบกลุ่มเมฆแบบอินเตอร์ ในโครงสร้างในการยืนยันตัวตนนี้จะทำได้โดย Single sign-on (SSO) ที่ผู้ใช้สามารถเข้าใช้งานได้ครั้งเดียวแต่สามารถไปได้หลายๆ ระบบประมวลผลแบบกลุ่มเมฆโดยปราศจากการถาม

คำถามอีกครั้งในระบบประมวลผลแบบกลุ่มเมฆนี้มีการใช้นโยบายการรับรองการยืนยันตัวตนโดยใช้เทคโนโลยี Shibboleth มาประยุกต์ใช้กับต้นแบบที่ออกแบบนำไปใช้เพื่อยืนยันประสิทธิภาพการทำงานของระบบในที่นี่มีการใช้ Shibboleth ในการทำระบบยืนยันตัวตนโดยการทำ SSO นี้ได้ทดลองทำระหว่างมหาวิทยาลัยฮอกไกโดและสถาบันคิตามิที่ประเทศญี่ปุ่น

Singapore Advanced Research and Education Network (2003) [12] เป็นองค์กรเครือข่ายการวิจัยและการศึกษาแห่งชาติของประเทศสิงคโปร์ โดยมีงานวิจัยหลากหลายที่ได้ก่อตั้งขึ้น หนึ่งในงานวิจัยของ SingAREN คือ Singapore Access Federation หรือ ตัวกลางการให้บริการข้อมูลที่มีบริการระบบจัดการการระบุตัวตนสำหรับงานการศึกษาและงานวิจัยโดยงานนี้ได้ใช้ Shibboleth เป็นตัวที่ใช้ตรวจสอบการยืนยันตัวตนและการตรวจสอบสิทธิ์ที่สามารถเข้าใช้งานในระบบได้แบบไม่จำกัดขนาด โดย SingAREN ได้มีเซอร์วิสย่อยที่เรียกว่า การให้บริการทรัพยากรบนการประมวลผลแบบกลุ่มเมฆ หรือ Cloud Computational Services โดยมีจุดประสงค์เพื่อให้ผู้ใช้ที่ร้องขอการเข้าถึงทรัพยากรบนระบบเสมือนสำหรับงานวิจัยตามสถาบันที่เข้าร่วมด้วย เมื่อผู้ใช้ทำการลงทะเบียนแล้วจะสามารถเข้าใช้งานทรัพยากรได้แยกตามสิทธิของผู้ใช้งานที่เป็นนักเรียน, เจ้าหน้าที่และอาจารย์ โดยทรัพยากรที่ให้เข้าถึงจะมีลักษณะที่ต่างกันโดยจะถูกสร้างและกำหนดโดยผู้ที่เป็นเจ้าหน้าที่ดูแลระบบของสถาบันนั้น ๆ

Saley Mato Idrissa, Karimou Djibo, Saley Bisso and Hamadou Saliah-Hassane (2016) [13] ได้ทำวิจัยเรื่อง การจัดการการเข้าถึงทรัพยากรที่มีความปลอดภัยในสภาพแวดล้อมระบบประมวลผลแบบกลุ่มเมฆของการศึกษา โดยได้นำเสนอวิธีการที่ทำงานอยู่บนเทคโนโลยีเครือข่ายและอัลกอริธึม แนวคิดหลักที่ผู้วิจัยทำคือการสร้างความไว้วางใจระหว่างผู้ให้บริการเครือข่ายและผู้ใช้บริการที่ต้องการเข้ามาควบคุมการจัดการข้อมูลทรัพยากรและในงานนี้ได้ใช้ openvz เป็นเซิร์ฟเวอร์ที่ทำงานอยู่บนระบบประมวลผลแบบกลุ่มเมฆ โดยการสร้างเซิร์ฟเวอร์ที่ใช้ในการควบคุมการเข้าถึงและคำสั่ง iptables เพื่อบล็อกเซิร์ฟเวอร์อื่นที่ไม่ได้อนุญาตเข้ามาและงานวิจัยนี้ได้กำหนดตัวการที่รองรับความถูกต้องในการตรวจสอบสิทธิ์และการจัดการความถูกต้อง โดยงานวิจัยนี้ได้ใช้ SSH เพื่อใช้ในการเข้าถึงตัวเซิร์ฟเวอร์และใช้วิธีการของแฮชฟังก์ชันเพื่อตรวจสอบตัวตนของผู้ใช้และความสมบูรณ์ของข้อมูล

บทที่ 3
วิธีการดำเนินงานวิจัย

งานวิจัยนี้ได้ใช้เทคโนโลยีการเข้าใช้งานระบบแบบครั้งเดียวเข้ามาใช้ในงานเพื่อพัฒนาระบบจากวัตถุประสงค์โดยอ้างอิงจากงานวิจัยและทฤษฎีที่เกี่ยวข้อง ในการวิจัยครั้งนี้มีการดำเนินงานตามวัตถุประสงค์ประกอบด้วย 5 ขั้นตอนซึ่งมีขั้นตอนการดำเนินงานที่ประกอบไปด้วยขั้นตอนที่ 1 ศึกษาและออกแบบระบบงานวิจัย, ขั้นตอนที่ 2 ศึกษากลไกและออกแบบกระบวนการรักษาความปลอดภัย, ขั้นตอนที่ 3 พัฒนาระบบบริหารจัดการการใช้งานทรัพยากร, ขั้นตอนที่ 4 พัฒนาระบบแอปพลิเคชันบนระบบประมวลผลแบบกลุ่มเมฆและขั้นตอนที่ 5 ทดสอบระบบ

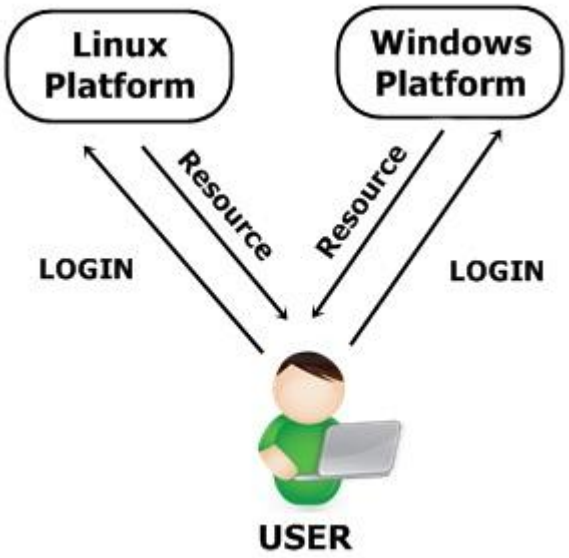
เตรียมทรัพยากรสำหรับตั้งค่าระบบ

ในขั้นตอนการเตรียมทรัพยากรที่ใช้ในการทำระบบนี้จะต้องเตรียมเครื่องเสมือนสำหรับงานวิจัยจำนวน 3 เครื่องและระบบประมวลผลแบบกลุ่มเมฆอีก 1 เครื่องซึ่งมีรายละเอียดดังต่อไปนี้

1. เครื่องเสมือนสำหรับทำระบบตรวจสอบตัวบุคคลด้วยเทคโนโลยี Shibboleth ส่วนของผู้ให้ทรัพยากรเครือข่ายติดตั้ง Ubuntu Server 16.04.2 LTS และผู้ให้ทรัพยากรข้อมูลติดตั้ง Centos6
2. เครื่องเสมือนสำหรับทำระบบตรวจสอบตัวบุคคลด้วยเทคโนโลยี OpenLDAP ติดตั้ง Ubuntu Server 16.04.2 LTS
3. ระบบประมวลผลแบบกลุ่มเมฆใช้บริการของ Amazon Web Services ทำเครื่องเสมือนระบบตรวจสอบตัวบุคคลด้วยเทคโนโลยี Active Directory ติดตั้ง Windows Server 2008 R2 Base

ศึกษาและออกแบบระบบงานวิจัย

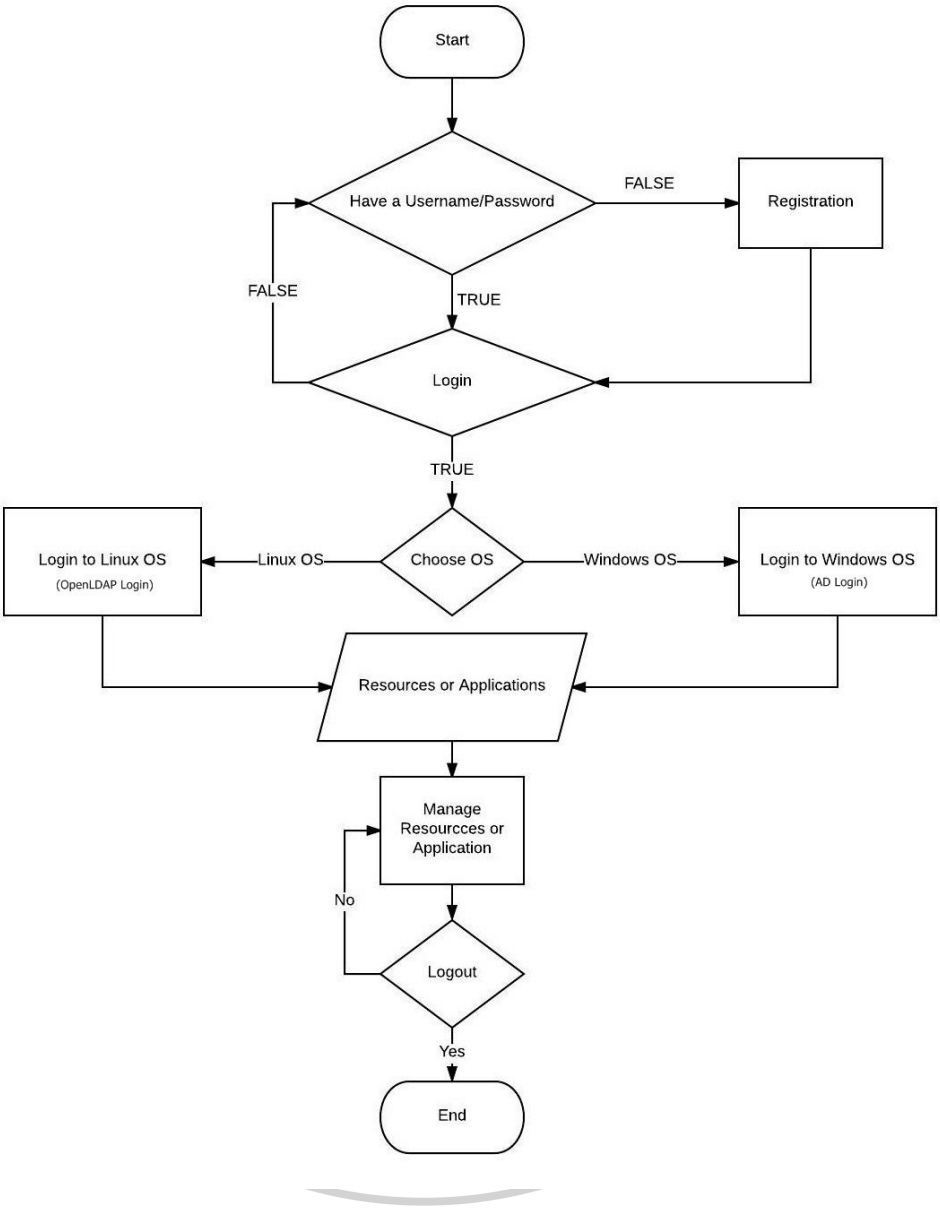
จากระบบเดิมในกระบวนการทำงานตรวจสอบตัวตนการเข้าใช้งานนี้ผู้ใช้จะเข้าใช้งานผ่านการเข้าสู่ระบบโดยตรงเพียงระบบเดียวเท่านั้นและการใช้งานทรัพยากรหรือแอปพลิเคชันที่อยู่บนระบบจะสามารถเข้าใช้งานหรือจัดการบริหารได้หนึ่งครั้งต่อการเข้าสู่ระบบหนึ่งครั้งโดยไม่มีตัวกลางมาจัดการผู้ใช้ ดังรูปที่ 3-1 แสดงระบบการเข้าใช้งานเดิม



รูปที่ 3-1 แสดงระบบการเข้าใช้งานเดิม

จากรูปที่ 3-1 แสดงระบบการเข้าใช้งานเดิมเป็นระบบดั้งเดิมที่ผู้ใช้จะสามารถเข้าใช้งานระบบในแพลตฟอร์มต่าง ๆ ได้โดยตรงและผู้ใช้ต้องเข้าสู่ระบบก่อนทุกครั้งในการใช้งานโดยไม่มีตัวกลางมาควบคุมและในกรณีนี้ผู้ใช้จะต้องมีระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์

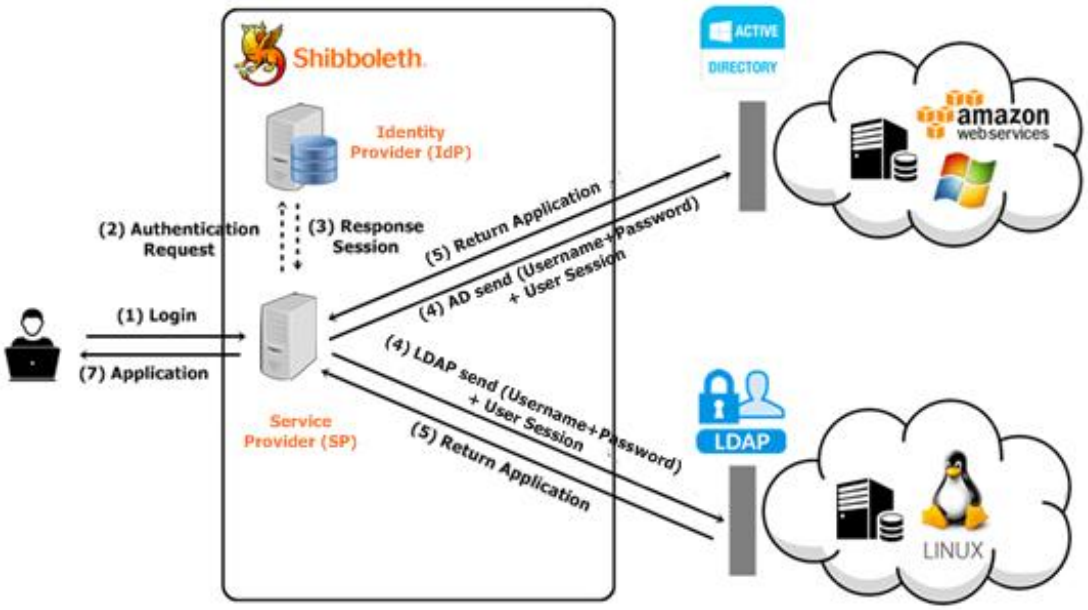
จากระบบเดิมที่ไม่มีตัวกลางในการส่งต่อข้อมูลการเข้าสู่ระบบ ในงานวิจัยนี้ได้นำเสนอกลไกการรักษาความปลอดภัย โดยการจำลองระบบประมวลผลแบบกลุ่มเมฆที่สามารถใช้บริการและทรัพยากรบนเครื่องที่ให้บริการได้ การเข้าใช้งานระบบทำเป็นรูปแบบการเข้าใช้งานครั้งเดียว โดยเครื่องเซิร์ฟเวอร์ที่เป็นตัวกลางได้ใช้เทคโนโลยีของ Shibboleth เป็นตัวจัดการการเข้าใช้งานระบบที่มีระบบตัวกลางในการส่งต่อข้อมูลของผู้ใช้ไปยังระบบประมวลผลบนกลุ่มเมฆที่เป็นระบบปฏิบัติการที่เหมือนหรือต่างกันและในระบบนั้นได้มีการรักษาความปลอดภัยภายในระบบคือใช้ AD ในการรักษาความปลอดภัยทางฝั่งระบบประมวลผลบนกลุ่มเมฆที่เป็นระบบปฏิบัติการวินโดวส์และใช้ OpenLDAP บนระบบประมวลผลบนกลุ่มเมฆที่เป็นระบบปฏิบัติการลินุกซ์ดังรูปที่ 3-2 ผังงานการเข้าใช้ระบบที่มีตัวกลาง



รูปที่ 3-2 ผังงานการเข้าใช้ระบบที่มีตัวกลาง

จากรูปที่ 3-2 ผังงานการเข้าใช้ระบบที่มีตัวกลาง ผู้ใช้จะต้องทำการตรวจสอบชื่อผู้ใช้และรหัสผ่าน ในกรณีที่ไม่มี ต้องเข้าสู่ระบบการลงทะเบียนก่อน เมื่อผู้ใช้งานมีชื่อผู้ใช้และรหัสผ่านแล้วจะทำการเข้าสู่ระบบเมื่อถูกต้องจะไปยังการเลือกเข้าถึงระบบปฏิบัติการและให้ผู้ใช้เลือกระบบปฏิบัติการเพื่อเข้าไปจัดการยังทรัพยากรหรือแอปพลิเคชันได้จนกว่าจะออกจากระบบ

จากการดำเนินงานผู้วิจัยได้ดำเนินการโดยใช้ระบบประมวลผลบนกลุ่มเมฆของ Amazon Web Services (AWS) ในการตั้งค่าทรัพยากรที่เป็นระบบปฏิบัติการวินโดวส์ สำหรับแนวคิดของระบบในงานวิจัยมีรายละเอียดดังรูปที่ 3-3 โครงสร้างรูปแบบระบบการเข้าใช้งาน



รูปที่ 3-3 โครงสร้างรูปแบบระบบการเข้าใช้งาน

ในโครงสร้างระบบนี้จะแบ่งออกเป็นส่วนใหญ่ ๆ สองส่วนด้วยกันคือ

1. **ระบบการตรวจสอบตัวตนเครื่องหลัก**

ในส่วนนี้ผู้ใช้จะทำการร้องขอการใช้งานและทำการตรวจสอบตัวบุคคลที่เซิร์ฟเวอร์ตัวนี้ผ่านเทคโนโลยี Shibboleth โดยระบบปฏิบัติการของเครื่องเซิร์ฟเวอร์คือระบบปฏิบัติการลินุกซ์ เครื่องนี้มีหน้าที่ในการรับชื่อผู้ใช้และรหัสผ่านมาทำการตรวจสอบค้นหาตัวบุคคล เมื่อได้ผลการตรวจสอบแล้วจะทำการส่งเซสชันของผู้ใช้และทำการยืนยันตัวตนโดยระบบที่อยู่บนเครื่องให้บริการ

กรณีที่ผู้ใช้ยังไม่มีชื่อผู้ใช้อยู่ในระบบจะต้องทำการลงทะเบียนกับระบบก่อนในขั้นต้นหลังจากนั้นจึงจะสามารถเข้าสู่ระบบเพื่อไปใช้งานได้

2. ระบบตรวจสอบตัวตนเครื่องให้บริการทรัพยากร

ในส่วนนี้จะมีเครื่องเซิร์ฟเวอร์อยู่สองตัวคือเครื่องที่เป็นระบบปฏิบัติการวินโดวส์และเครื่องที่เป็นระบบปฏิบัติการลินุกซ์

เครื่องระบบปฏิบัติการวินโดวส์จะทำการติดตั้งไว้ที่ผู้ให้บริการระบบประมวลผลบนกลุ่มเมฆ คือ Amazon Web Services (AWS) ทำการสร้างเครื่องเสมือนสำหรับ Windows Server 2008 R2 และติดตั้งและตั้งค่าระบบตรวจสอบตัวบุคคลคือ AD โดยเมื่อรับข้อมูลที่ใช้ในการตรวจสอบตัวตนจากเครื่องหลักแล้วจะทำการค้นหาใน Directory และส่งค่ากลับไปยังเครื่องหลักเพื่อให้สามารถเข้าถึงแอปพลิเคชันที่อยู่ในระบบปฏิบัติการวินโดวส์ได้

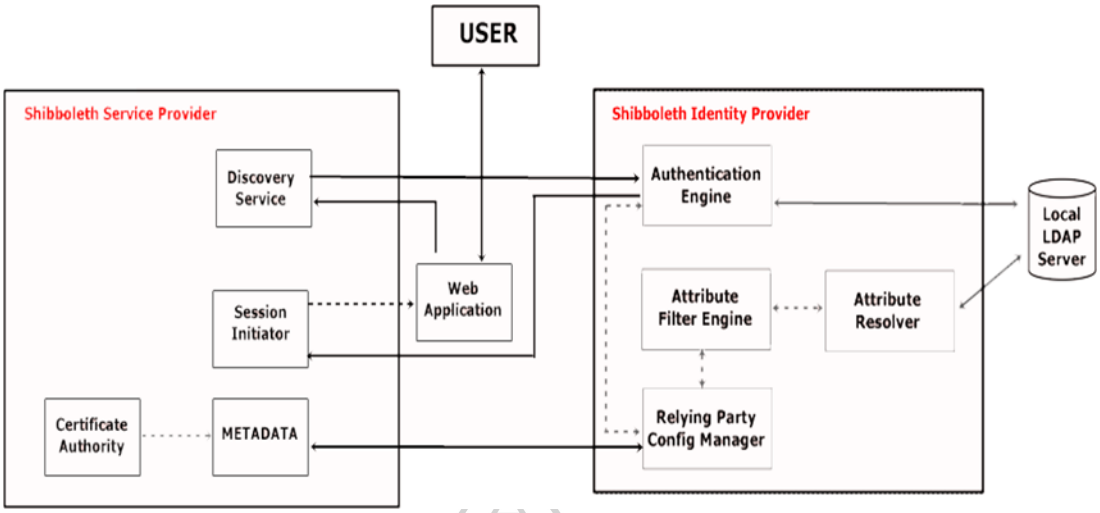
เครื่องระบบปฏิบัติการลินุกซ์ทำการติดตั้ง Ubuntu 16.04.2 LTS ไว้บนเครื่องเสมือน เพื่อติดตั้งและตั้งค่าระบบตรวจสอบตัวบุคคลคือ OpenLDAP โดยเมื่อรับข้อมูลที่ใช้ในการตรวจสอบตัวตนจากเครื่องหลักแล้วจะทำการค้นหาใน Directory และส่งค่ากลับไปยังเครื่องหลักเพื่อให้สามารถเข้าถึงแอปพลิเคชันที่อยู่ในระบบปฏิบัติการลินุกซ์ได้

ศึกษากลไกและออกแบบกระบวนการรักษาความปลอดภัย

ในการศึกษากลไกของกระบวนการรักษาความปลอดภัยนี้ ได้แบ่งการศึกษาตามวัตถุประสงค์ออกเป็นสองส่วนคือ

1. กลไกการพิสูจน์ตัวตนการเข้าใช้งานระบบ

จากวัตถุประสงค์ในการศึกษาและพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรบนระบบประมวลผลบนกลุ่มเมฆผู้วิจัยจึงได้นำเสนอกลไกการเข้าใช้งานระบบโดยใช้เทคโนโลยีของ Shibboleth มาเป็นตัวพัฒนาระบบกลไกการเข้าใช้งานในระบบ ในกลไกนี้จะมีฝั่งการให้บริการอยู่สองฝั่งคือผู้ให้บริการทางข้อมูลและผู้ให้บริการทางเครือข่าย โดยการจัดเก็บข้อมูลจะใช้ LDAP เป็นเพียงฐานข้อมูลเท่านั้น ดังรูปที่ 3-4 กลไกการเข้าใช้งานระบบ



รูปที่ 3-4 กลไกการเข้าใช้งานระบบ

ฝั่งทางผู้ให้บริการเครือข่ายจะประกอบไปด้วย ส่วนของการสร้างใบรับรองความปลอดภัย นำไปจัดเก็บที่เมตาดาต้า ส่วนของการส่งข้อมูลผู้ใช้ที่บริการการส่งข้อมูลแบบเข้ารหัสและการสร้างเซสชันของผู้ใช้

ฝั่งทางผู้ให้บริการข้อมูลจะประกอบไปด้วย ส่วนหลักที่ไว้ตรวจสอบข้อมูลของผู้ใช้ (Authentication Engine) และค้นหาความสัมพันธ์ของข้อมูลที่ทำการแลกเปลี่ยนกับฝั่งผู้ให้บริการเครือข่าย ในการจัดการคุณลักษณะจะทำการคัดกรองรูปแบบและตรวจสอบความถูกต้อง

ในกระบวนการทำงานของกลไกนี้เมื่อผู้ใช้เข้าสู่ระบบโดยผ่านเว็บแอปพลิเคชันแล้วชื่อผู้ใช้และรหัสผ่านจะถูกส่งไปที่ Discovery Service และเข้ารหัสนำส่งตรวจสอบที่ Authentication Engine ในระบบนี้จะเริ่มตรวจสอบโดยการเข้าไปตรวจสอบที่ Relying party ในส่วนนี้จะทำการตรวจสอบว่าข้อมูลที่รับมาถูกส่งมาจากที่ใด ข้อมูลนี้ถูกส่งมาทาง URL นั่นคือชื่อโดเมนและรหัสข้อมูล SAML ถ้าเป็นเครื่องที่ลงทะเบียนไว้แล้ว จะทำการเก็บไว้บันทึกไว้ที่ส่วนนี้ดังรูปที่ 3-5 การตั้งค่าตรวจสอบข้อมูลผู้ให้บริการเครือข่าย

```
<!-- Load the SP2's metadata -->
<metadata:MetadataProvider xsi:type="FilesystemMetadataProvider"
        xmlns="urn:mace:shibboleth:2.0:metadata" id="SP2METADATA"
        metadataFile="/opt/shibboleth-idp/metadata/sp2-metadata.xml" />
```

รูปที่ 3-5 การตั้งค่าตรวจสอบข้อมูลผู้ให้บริการเครือข่าย

เมื่อตรวจสอบข้อมูลโดยการเช็คคีย์ที่ส่งมาแล้ว ต่อไปจะทำการตรวจสอบแอตทริบิวต์ ที่ Attribute Filter Engine และ Attribute Resolver ในงานวิจัยได้ใช้ข้อมูลที่ตรวจสอบ 2 ตัวคือ แอตทริบิวต์ของชื่อและแอตทริบิวต์ของรหัสผ่านเพื่อทำการเข้าไปค้นหาในไดเรกทอรีของ LDAP เมื่อตรวจสอบเสร็จสิ้นจะส่งกลับมาเพื่อสร้างเซสชันและส่งกลับไปให้ผู้ใช้

2. กลไกตัวกลางการเข้าใช้งานครั้งเดียว

จากวัตถุประสงค์ในการพัฒนาระบบตัวกลางการเข้าใช้งานครั้งเดียว สำหรับระบบยืนยันตัวตนที่แตกต่างกันเพื่อเข้าใช้ทรัพยากรจากลินุกซ์แพลตฟอร์มและวินโดวส์แพลตฟอร์ม ระบบตัวกลางที่ต้องการให้สามารถเข้าใช้งานข้ามแพลตฟอร์มได้โดยการเข้าสู่ระบบเพียงครั้งเดียวจากการเข้าใช้งานระบบที่ใช้เทคโนโลยี Shibboleth ในกระบวนการนี้ผู้วิจัยได้นำเสนอกลไกของระบบตัวกลางที่สามารถส่งต่อข้อมูลไปยังลินุกซ์แพลตฟอร์มและวินโดวส์แพลตฟอร์ม ดังรูปที่ 3-6 กลไกของระบบตัวกลาง (Exchange System) โดยมีขั้นตอนกระบวนการดังต่อไปนี้

1. ติดต่อระบบปฏิบัติการวินโดวส์

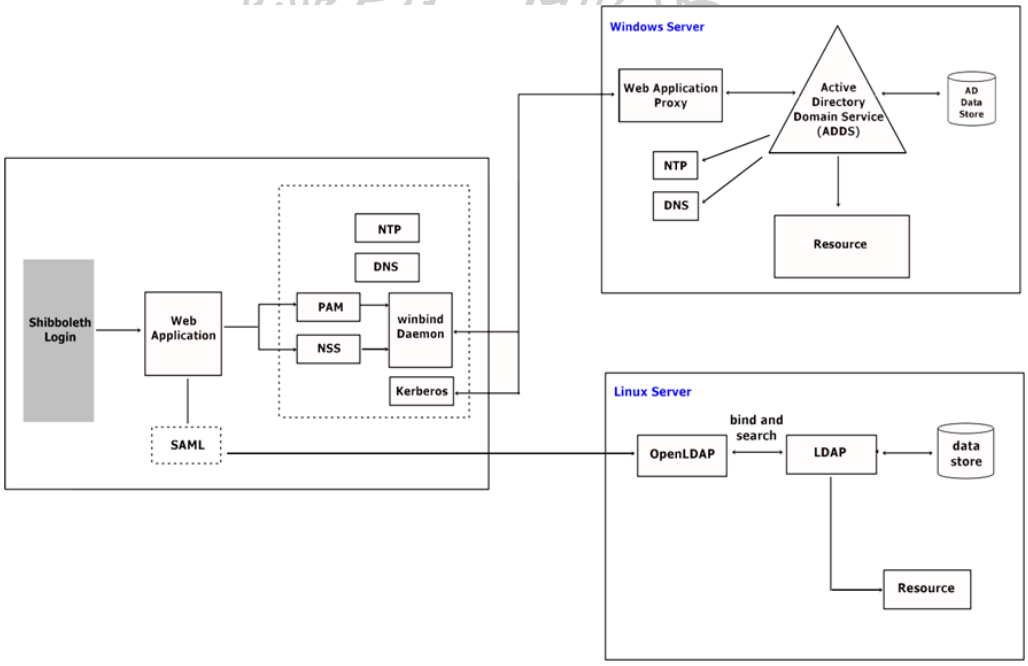
กรณีเลือกเส้นทางไปยังระบบปฏิบัติการวินโดวส์ในกลไกการส่งข้อมูลข้ามแพลตฟอร์มในงานวิจัยนี้ได้ทำการใช้เซอร์วิสของ Winbind และ Kerbeos ทำการร้องขอเข้าถึงข้อมูลเพื่อตรวจสอบที่ AD แบบผ่านพร็อกซีแอปพลิเคชันโดยเซอร์วิสที่ใช้ในการติดต่อมีองค์ประกอบดังนี้

- DNS (Domain Name System) คือการกำหนดชื่อที่ใช้ติดต่อกับ AD
- NTP (Network Time Protocol) คือเป็นโปรโตคอลที่ใช้เทียบเวลากับเครื่องระบบปฏิบัติการวินโดวส์
- PAM (Pluggable Authentication Modules) และ NSS (Name Service Switch) สองตัวนี้เป็นตัวอนุญาตให้สามารถใช้งานแอปพลิเคชันได้โดยใช้ข้อมูล

รับรองจาก Kerberos เพื่อช่วยให้สามารถเข้าใช้งานได้แบบครั้งเดียวโดยมีแคชแบบออฟไลน์ที่สามารถดึงมาใช้ได้เลย

- Winbind เป็น เซอร์วิสที่ใช้ในการเข้าสู่ระบบสำหรับ Microsoft Remote Procedure Call ทำงานร่วมกับ PAM และ NSS เพื่อให้สามารถเข้าใช้งานในวินโดวส์โดเมนได้
- Kerberos เป็นเซอร์วิสการพิสูจน์ตัวตนบนระบบเครือข่ายในการขอเข้าใช้ใน AD จะต้องส่งคำร้องขอไปที่ KDC (Key Distribution Center) ที่อยู่ภายใน AD และกำหนดขอบเขตของ Kerberos ที่สามารถให้ Winbind จัดการได้

จากเซอร์วิสและเครื่องมือที่มีเมื่อผู้ใช้ต้องการเข้าใช้งานแอปพลิเคชันจะสามารถเข้าถึงได้หลังจากตรวจสอบแล้วว่า DNS มีอยู่ในระบบ NTP ตรงกัน จากนั้นค้นหาชื่อผู้ใช้งานและรหัสผ่านจากไดเรกทอรีเมื่อตรวจสอบครบทุกกรณีแล้วผู้ใช้งานสามารถเข้าใช้งานแอปพลิเคชันที่อยู่บนระบบปฏิบัติการวินโดวส์ได้โดยไม่จำเป็นต้องทำการเข้าสู่ระบบ AD จากผู้ใช้อีกครั้ง

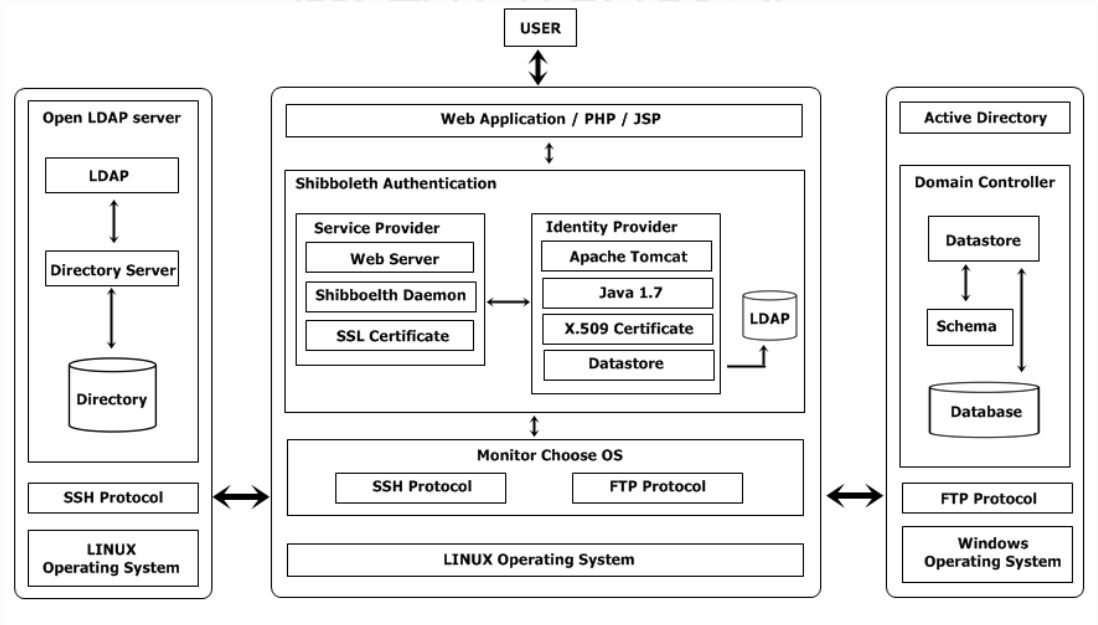


รูปที่ 3-6 กลไกการติดต่อกับระบบปฏิบัติการ

2. ติดต่อกับระบบปฏิบัติการลินุกซ์

เนื่องจากลินุกส์เป็นระบบปฏิบัติการเดียวกันกับระบบตัวกลางทำให้เมื่อได้เซสชันมาสามารถส่งต่อเซสชันนี้โดยใช้ SAML เพื่อไปพิสูจน์ตัวตนโดยการร้องขอการเชื่อมต่อและค้นหาข้อมูลของผู้ใช้ผ่าน OpenLDAP จากการเก็บไดเรกทอรีที่ LDAP เมื่อค้นเจอจะอนุญาตให้ผู้ใช้เข้าใช้งานทรัพยากรต่อได้

จากวัตถุประสงค์การพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆนี้ ได้พัฒนาโดยใช้เทคโนโลยี Shibboleth, Active Directory และ OpenLDAP และได้ใช้ภาษา PHP ในการพัฒนาระบบแอปพลิเคชันทางฝั่งระบบปฏิบัติการวินโดวส์และทางฝั่งระบบปฏิบัติการลินุกซ์ ดังรูป 3-7 สถาปัตยกรรมระบบบริหารจัดการ



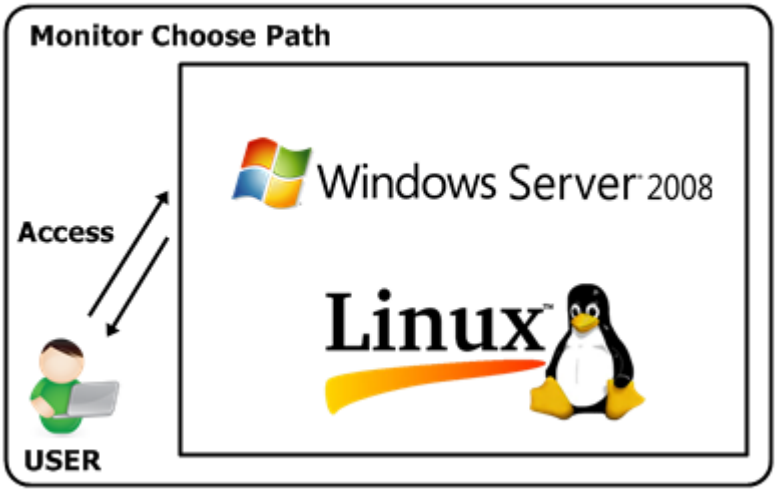
รูปที่ 3-7 สถาปัตยกรรมระบบบริหารจัดการ

โดยระบบหลักจะทำงานบนระบบปฏิบัติการลินุกซ์ โดยใช้เทคโนโลยีการตรวจสอบตัวตนของ Shibboleth มีการตั้งค่าที่ผู้ให้บริการเครือข่ายและผู้ให้บริการข้อมูล โดยผู้ใช้จะสามารถเข้าถึงระบบได้จากเว็บแอพพลิเคชั่น ในระบบมีการรักษาความปลอดภัยโดยใช้ใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์ SSL Certificate และ X.509 Certificate และในระบบปฏิบัติการลินุกซ์จะใช้

OpenLDAP ในการจัดการรายชื่อผู้ใช้งานและสิทธิ์ต่างๆ ส่วนในระบบปฏิบัติการวินโดวส์จะใช้ Active Directory ในการจัดการรายชื่อผู้ใช้และสิทธิ์ต่าง ๆ ในระบบหลักนี้จะทำการติดตั้งโปรโตคอลสองตัวคือ SFTP และ SSH โดย SSH จะถูกติดตั้งที่ระบบให้บริการทรัพยากรที่ทำงานบนระบบปฏิบัติการลินุกซ์ด้วยโดย SSH จะใช้ในการเข้าสู่ระบบและจัดการทรัพยากรต่าง ๆ ที่อยู่บนระบบปฏิบัติการลินุกซ์และ SFTP จะถูกติดตั้งที่ระบบให้บริการที่ทำงานบนระบบปฏิบัติการวินโดวส์ โดย SFTP ใช้ในการเข้าสู่ระบบและจัดการทรัพยากรต่าง ๆ ที่อยู่บนระบบปฏิบัติการวินโดวส์

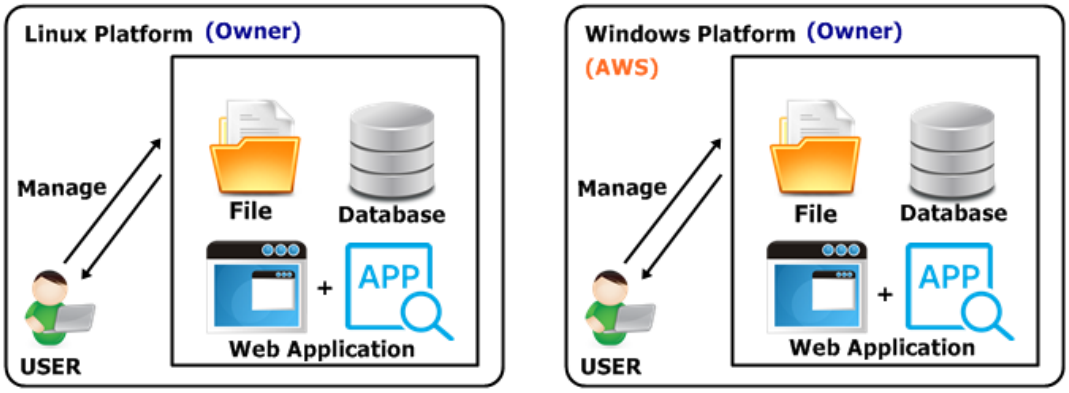
พัฒนาระบบบริหารจัดการการใช้งานทรัพยากร

ในส่วนของการใช้งานทรัพยากรนี้เมื่อผ่านกระบวนการเข้าสู่ระบบแล้วผู้ใช้จะสามารถจัดการทรัพยากรที่มีอยู่ในระบบได้ในงานนี้ได้นำเสนอการจัดการพื้นที่จัดเก็บคือ ผู้ใช้หนึ่งคนจะสามารถจัดการทรัพยากรที่อยู่บนระบบปฏิบัติการลินุกซ์และระบบปฏิบัติการวินโดวส์ได้ในพื้นที่ของผู้ใช้เองจะไม่สามารถเข้าถึงทรัพยากรของผู้ใช้อื่นได้



รูปที่ 3-8 แสดงส่วนของระบบปฏิบัติการที่เข้าจัดการทรัพยากร

จากรูปที่ 3-8 แสดงส่วนของระบบปฏิบัติการที่เข้าจัดการทรัพยากรเมื่อผู้ใช้เข้าสู่ระบบเรียบร้อยแล้วผู้ใช้จะสามารถเลือกระบบปฏิบัติการที่จะเข้าไปจัดการทรัพยากรได้สองระบบปฏิบัติการคือ ระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์



รูปที่ 3-9 แสดงการเข้าจัดการทรัพยากรทั้งสองระบบปฏิบัติการ

จากรูปที่ 3-9 แสดงการเข้าจัดการทรัพยากรทั้งสองระบบปฏิบัติการเมื่อผู้ใช้ได้เลือกเข้าสู่ระบบปฏิบัติการแล้วผู้ใช้จะสามารถจัดการต่าง ๆ ได้บนระบบเช่น การจัดการไฟล์, การจัดการฐานข้อมูล, การจัดการแอปพลิเคชัน โดยผู้ใช้รายอื่นจะไม่สามารถเห็นข้อมูลของผู้ใช้คนนั้นๆ ได้และเมื่อผู้ใช้สร้างแอปพลิเคชันที่อยู่บนระบบแล้วผู้ใช้จะสามารถให้ผู้อื่นเข้าถึงแอปพลิเคชันที่สร้างได้โดยการส่งลิงก์หรือส่งตัวติดตั้งให้กับผู้ใช้รายอื่น ๆ ต่อได้ โดยการเข้าไปจัดการทรัพยากรที่อยู่บนระบบปฏิบัติการจะแบ่งออกตามระบบปฏิบัติการดังนี้

1. ระบบปฏิบัติการลินุกซ์

ในการจัดการระบบปฏิบัติการลินุกซ์นี้จะเข้าถึงได้โดยใช้โปรโตคอล SSH ในการติดต่อและส่งข้อมูลที่มีการเข้ารหัสไว้กับเครื่องตัวกลางที่ผู้ใช้ได้ทำการเข้าสู่ระบบมาเมื่อ SSH เข้าสู่ระบบปฏิบัติการได้แล้วผู้ใช้จะสามารถจัดการทรัพยากรต่าง ๆ บนระบบในส่วนของผู้ใช้ที่ทำการเข้าสู่ระบบมาเท่านั้น

2. ระบบปฏิบัติการวินโดวส์

ในการจัดการระบบปฏิบัติการวินโดวส์นี้จะเข้าถึงได้โดยใช้โปรโตคอล SFTP การในการติดต่อและส่งข้อมูลที่มีการเข้ารหัสไว้กับเครื่องตัวกลางที่ผู้ใช้ได้ทำการเข้าสู่ระบบมาเมื่อ SFTP เข้าสู่

ระบบปฏิบัติการได้แล้วผู้ใช้จะสามารถจัดการทรัพยากรต่าง ๆ บนระบบในส่วนของผู้ใช้ที่ทำการเข้าสู่ระบบมาเท่านั้น

พัฒนาระบบแอปพลิเคชันบนระบบประมวลผลแบบกลุ่มเมฆ

ในการพัฒนาระบบนี้จะใช้ตัวอย่างแอปพลิเคชันที่ต้องการความปลอดภัยสูง ๆ ประเภทระบบทางการแพทย์ คือ ระบบคัดกรองผู้ป่วย

ระบบคัดกรองผู้ป่วยนี้จะถูกสร้างไว้ที่ระบบปฏิบัติการลินุกซ์และระบบปฏิบัติการวินโดวส์โดยเป็นระบบที่ใช้คัดกรองต่างโรคกัน ระบบคัดกรองผู้ป่วยกลุ่มเสี่ยงโรคเบาหวานทำงานบนวินโดวส์แพลตฟอร์มและระบบคัดกรองผู้ป่วยกลุ่มเสี่ยงโรคหัวใจทำงานบนระบบปฏิบัติการลินุกซ์ โดยการสร้างแอปพลิเคชันด้วยภาษา PHP และฐานข้อมูล MySQL

1. ระบบคัดกรองผู้ป่วยกลุ่มเสี่ยงโรคเบาหวาน

ในระบบคัดกรองผู้ป่วยกลุ่มเสี่ยงโรคเบาหวานนี้จะอ้างอิงจากมูลนิธิเพื่อการวิจัยและพัฒนาระบบยาโดยชอบธรรม [14] โดยอิงจากปัจจัยที่อาจก่อให้เกิดโรคเบาหวานเช่น เพศ, อายุ, ดัชนีมวลกาย เป็นต้น จะแบ่งการประเมินออกเป็นสองส่วนคือ เกณฑ์ที่ใช้ในการประเมินความเสี่ยงต่อโรคเบาหวานและการแปลผลจากการทำแบบประเมินความเสี่ยง โดยการนำข้อมูลทั้งหมดมาแปรผลโดยใช้ฐานข้อมูลจัดเก็บเงื่อนไขคือตรวจสอบทุกคำถามประกอบไปด้วยตารางดังต่อไปนี้

ตาราง Diabetes

ตาราง Age

ตาราง Gender

ตาราง BMI

ตาราง Waist

ตารางที่ 3-1 Diabetes

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
age	อายุ	1	char	FK
gender	เพศ	1	char	FK
bmi	ดัชนีมวลกาย	4	varchar	FK
waist	รอบเอว	4	varchar	FK
bp	ความดันโลหิต	“N”,”Y”	enum	
family	ประวัติครอบครัวเป็นเบาหวาน	“N”,”Y”	enum	
result	ผลลัพธ์		text	

คำอธิบาย

ตารางที่ 3-1 Diabete ที่จัดทำขึ้นนี้อ้างอิงผลลัพธ์โดยใช้คะแนนที่ได้ในแต่ละข้อตามเกณฑ์ของการประเมินมาแปรผลเป็นผลลัพธ์ที่ใช้ในการวิเคราะห์

ตารางที่ 3-2 Age

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
ageID	รหัสช่วงอายุ	1	char	PK
ageName	ช่วงอายุ	100	varchar	

คำอธิบาย

ตารางที่ 3-2 Age เป็นเกณฑ์ของอายุจัดเป็นกลุ่ม

กลุ่มที่ 1 ตั้งแต่ 34 – 39 ปี

กลุ่มที่ 2 ตั้งแต่ 40 – 44 ปี

กลุ่มที่ 3 ตั้งแต่ 45 – 49 ปี

กลุ่มที่ 4 มากกว่า 50 ปี

โดยผู้ที่มีอายุมากกว่า 50 ปีจะมีความเสี่ยงสูงกว่าผู้ที่อายุน้อย

ตารางที่ 3-3 Gender

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
genderID	รหัสเพศ	1	char	PK
genderName	ชื่อเพศ	20	varchar	

คำอธิบาย

ตารางที่ 3-3 Gender เป็นเกณฑ์ของเพศจัดเป็นกลุ่ม

กลุ่มที่ 1 ชาย

กลุ่มที่ 2 หญิง

โดยเพศชายจะมีความเสี่ยงสูงกว่าเพศหญิง

ตารางที่ 3-4 BMI

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
bmiID	รหัสดัชนีมวลกาย	1	char	PK
bmiName	ช่วงดัชนีมวลกาย	100	varchar	

คำอธิบาย

ตารางที่ 3-4 BMI เป็นเกณฑ์ของดัชนีมวลกายจัดเป็นกลุ่ม

กลุ่มที่ 1 ต่ำกว่า 23 kg/m^2

กลุ่มที่ 2 ตั้งแต่ 23 kg/m^2 แต่ต่ำกว่า 27.5 kg/m^2

กลุ่มที่ 3 ตั้งแต่ 27.5 kg/m^2 ขึ้นไป

โดยผู้ที่มีดัชนีมวลกายมากกว่าหรือเท่ากับ 23 kg/m^2 (สำหรับคนเอเชีย) ถ้าน้ำหนักตัวมากจะมีโอกาสเป็นโรคเบาหวานมากกว่าคนปกติถึง 2 เท่า

ตารางที่ 3-5 Waist

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
waistID	รหัสช่วงรอบเอว	1	char	PK
waistName	ช่วงรอบเอว	100	varchar	

คำอธิบาย

ตารางที่ 3-5 Waist เป็นเกณฑ์ของเส้นรอบเอวจัดเป็นกลุ่ม

กลุ่มที่ 1 ผู้ชายต่ำกว่า 90 ซม. ผู้หญิงต่ำกว่า 80 ซม.

กลุ่มที่ 2 ผู้ชายสูงกว่า 90 ซม. ผู้หญิงสูงกว่า 80 ซม.

การแปรผลระดับโอกาสเสี่ยง

- น้อยกว่าร้อยละ 5 โอกาสเกิดโรค 1/20
- ร้อยละ 5-10 โอกาสเกิดโรค 1/12
- ร้อยละ 11-20 โอกาสเกิดโรค 1/7
- มากกว่า ร้อยละ 20 โอกาสเกิดโรค 1/3 – 1/4

2. ระบบคัดกรองผู้ป่วยกลุ่มเสี่ยงโรคหัวใจ

ในระบบการคัดกรองโรคหัวใจนี้จะอ้างอิงจากกรมควบคุมโรคกระทรวงสาธารณะสุข กลุ่มโรคไม่ติดต่อเรื้อรัง สำนักโรคไม่ติดต่อ [15] เป้าหมายของการคัดกรองโรคนี้เพื่อลดปัจจัยเสี่ยงและปรับพฤติกรรมสุขภาพให้ถูกต้องเหมาะสม โดยขั้นตอนการวินิจฉัยจะใช้เกณฑ์สำหรับผู้ที่ไม่ได้ตรวจหาคลอเรสเตอรอลในเลือดโดยการนำข้อมูลทั้งหมดมาแปรผลโดยใช้ฐานข้อมูลจัดเก็บเงื่อนไขคือตรวจสอบทุกคำถามประกอบไปด้วยตารางดังต่อไปนี้

ตาราง Cardiovascular

ตาราง Age

ตาราง Gender

ตาราง BP

ตารางที่ 3-6 Cardiovascular

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
age	อายุ	1	char	FK
gender	เพศ	1	char	FK
diabetes	เป็นโรคเบาหวาน	"N","Y"	enum	
smoking	สูบบุหรี่	"N","Y"	enum	
bp	ความดันโลหิต	1	char	FK
result	ผลลัพธ์		text	

คำอธิบาย

จากตางรางที่ 3-6 Cardiovascular เป็นการวิเคราะห์เบื้องต้นในการหาภาวะเสี่ยงต่อการเป็นโรคหัวใจสำหรับผู้ที่ไม่ได้รับการตรวจคลอเรสเตอรอลในเลือดเท่านั้น

ตารางที่ 3-7 Age

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
ageID	รหัสช่วงอายุ	1	char	PK
ageName	ช่วงอายุ	100	varchar	

คำอธิบาย

จากตางรางที่ 3-7 Age เป็นเกณฑ์ของอายุจัดเป็นกลุ่ม

กลุ่มที่ 1 น้อยกว่า 40 – 49 ปี

กลุ่มที่ 2 ตั้งแต่ 50 – 59 ปี

กลุ่มที่ 3 ตั้งแต่ 60 – 69 ปี

กลุ่มที่ 4 มากกว่า 70 ปี

ตารางที่ 3-8 Gender

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
genderID	รหัสเพศ	1	char	PK
genderName	ชื่อเพศ	4	varchar	

คำอธิบาย

ตารางที่ 3-8 Gender เป็นเกณฑ์ของเพศจัดเป็นกลุ่ม

กลุ่มที่ 1 ชาย

กลุ่มที่ 2 หญิง

ตารางที่ 3-9 BP

แอตทริบิวต์	คำอธิบาย	ขนาด	ประเภท	คีย์
bpID	รหัสช่วงความดันโลหิต	1	char	PK
bpName	ช่วงความดันโลหิต	100	varchar	

คำอธิบาย

ตารางที่ 3-9 BP เป็นเกณฑ์ของการวัดความดันจัดเป็นกลุ่ม

กลุ่มที่ 1 น้อยกว่า 120-139 มม.ปรอท

กลุ่มที่ 2 140-159 มม.ปรอท

กลุ่มที่ 3 160-179 มม.ปรอท

กลุ่มที่ 4 180 มม.ปรอท ขึ้นไป

การแปรผลระดับโอกาสเสี่ยง

- น้อยกว่า ร้อยละ 10 โอกาสเกิดโรค ต่ำ
- ร้อยละ 10 - 20 โอกาสเกิดโรค ปานกลาง
- ร้อยละ 20 - 29 โอกาสเกิดโรค สูง
- ร้อยละ 30 - 39 โอกาสเกิดโรค สูงมาก
- มากกว่า ร้อยละ 40 โอกาสเกิดโรค สูงอันตราย

ทดสอบระบบ

ในการพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆนี้จะทดสอบการลงทะเบียนและการเข้าสู่ระบบ โดยการใช้งานระบบจะใช้งานระบบผ่านเว็บแอปพลิเคชัน ผู้ใช้จะต้องทำการลงทะเบียนการเข้าใช้งานในเบื้องต้นก่อนการเข้าสู่ระบบการใช้งานจัดการทรัพยากร เมื่อผู้ใช้งานเข้าสู่ระบบแล้ว ระบบจะทำการส่งค่าไปเข้าใช้สู่ระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์ โดยใช้ SFTP และ SSH ในการส่งไฟล์ข้ามแพลตฟอร์มตามลำดับ โดยผู้ใช้จะ

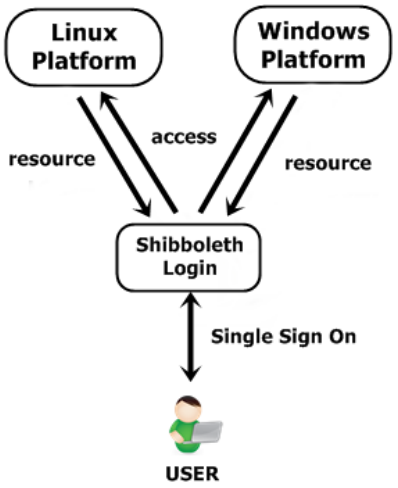
สามารถเข้าใช้งานระบบการจัดการบริหารทรัพยากรที่เป็นลักษณะของไฟล์และแอปพลิเคชันหรือเว็ปแอปพลิเคชันข้ามแพลตฟอร์มโดยมีตัวอย่างการทดสอบที่ต้องการความปลอดภัยคือระบบคัดกรองผู้ป่วยบนระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์

บทที่ 4
ผลการดำเนินงาน

หลังจากที่ได้ศึกษาและพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรและการพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆแล้ว โดยในบทนี้จะอธิบายถึงผลการดำเนินงานวิจัยของระบบอันประกอบไปด้วยเรื่อง การพัฒนาระบบพิสูจน์ตัวตนการเข้าใช้งานทรัพยากร การพัฒนาระบบการเข้าใช้งานทรัพยากรและการพัฒนาระบบบริหารจัดการการใช้งานทรัพยากร

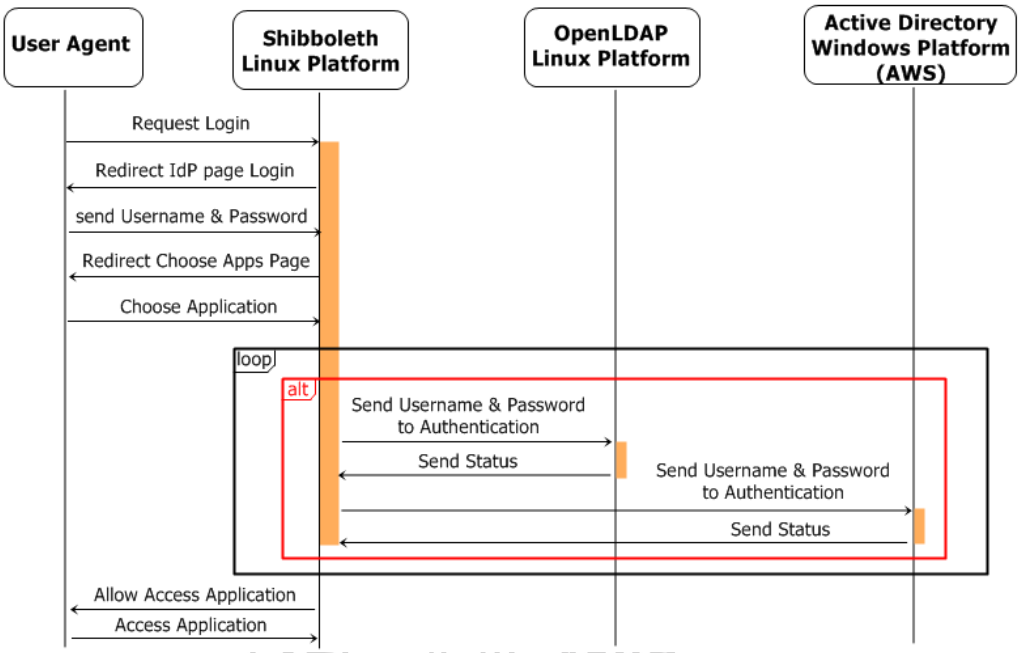
1. การพัฒนาระบบพิสูจน์ตัวตนการเข้าใช้งานทรัพยากร

ในการพัฒนาระบบพิสูจน์ตัวตนการเข้าใช้งานนี้ได้ศึกษาออกแบบและพัฒนาระบบจากทฤษฎีการตรวจสอบตัวตน การเข้าใช้งาน โปรโตคอลและงานวิจัยที่เกี่ยวข้องต่าง ๆ จากระบบเดิมที่ต้องเข้าใช้งานทีละระบบปฏิบัติการผลการดำเนินงานที่ได้คือผู้ใช้จะสามารถเข้าใช้งานระบบโดยผ่านตัวกลางในการส่งต่อข้อมูลของผู้ใช้ไปยังระบบรักษาความปลอดภัยที่อยู่บนระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์ดังรูปที่ 4-1 แสดงระบบการเข้าใช้งานผ่านตัวกลาง



รูปที่ 4-1 แสดงระบบการเข้าใช้งานผ่านตัวกลาง

จากการทำงานวิจัยเพื่อพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ จะได้ระบบที่มีการเข้าใช้งานผ่านตัวกลางในการเข้าใช้งานครั้งเดียว ในขั้นตอนของการรับส่งข้อมูลของผู้ใช้ดังรูป 4-2 แผนภาพแสดงการเข้าใช้งานระบบ



รูปที่ 4-2 แผนภาพแสดงการเข้าใช้งานระบบ

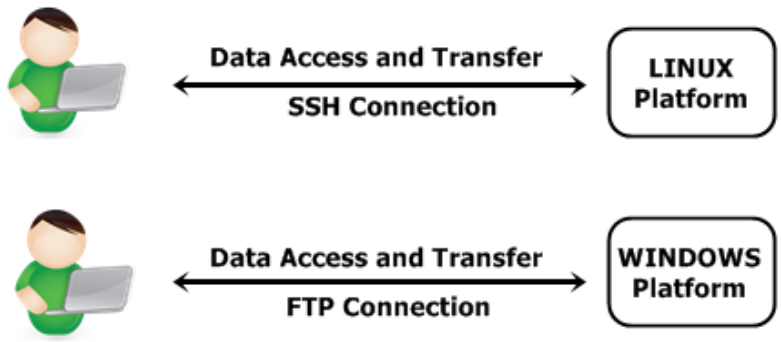
แผนภาพนี้เป็นการแสดงการเข้าร้องขอการเข้าใช้งานระบบของผู้ใช้โดยผ่านเทคโนโลยีรักษาความปลอดภัยของ Shibboleth บนระบบปฏิบัติการลินุกซ์ ผู้ใช้จะทำการร้องขอการเข้าระบบเพื่อที่จะขอเข้าไปใช้ทรัพยากรที่ Ubuntu และ AWS เมื่อถูกตรวจสอบตัวบุคคลแล้วผู้ใช้จะสามารถเข้าใช้ได้ทั้งสองระบบปฏิบัติการ

ขั้นตอนกระบวนการของโครงสร้างรูปแบบระบบเป็นดังต่อไปนี้

1. ผู้ใช้ทำการเข้าสู่ระบบ (Login) โดยการใส่ชื่อและรหัสผ่าน
2. เข้าสู่กระบวนการตรวจสอบตัวตนของ Shibboleth โดยการทำการร้องขอตรวจสอบตัวตน (Authentication Request) เพื่อส่งชื่อผู้ใช้และรหัสผ่านไปตรวจสอบ
3. เมื่อตรวจสอบผ่านแล้วผู้ให้บริการข้อมูลจะทำการส่งเซสชันของผู้ใช้ (Response Session) กลับมาที่ผู้ให้บริการเครือข่าย
4. เมื่อเข้าสู่ระบบสำเร็จแล้วผู้ให้บริการเครือข่ายจะส่งหน้าจอที่แสดงข้อมูลของผู้ใช้และรายชื่อแอปพลิเคชันที่ผู้ใช้สามารถเข้าใช้งานได้

5. เมื่อผู้ใช้เลือกระบบแอปพลิเคชันแล้วโดยส่วนนี้แอปพลิเคชันจะอยู่บนคนละระบบปฏิบัติการ ระบบจะทำการยืนยันตัวตน (Authentication) ในการร้องขอเข้าระบบปฏิบัติการ
   - ระบบปฏิบัติการวินโดวส์ จะส่งไปตรวจสอบที่ Active Directory
   - ระบบปฏิบัติการลินุกซ์ จะส่งไปตรวจสอบที่ LDAP
6. เมื่อข้อมูลถูกต้องระบบความปลอดภัยของแต่ละระบบปฏิบัติการจะยอมให้ผ่านไปยังข้อมูลทรัพยากรที่ผู้ใช้มีสิทธิเข้าถึงได้เท่านั้น
7. ผู้ใช้สามารถใช้งานทรัพยากรหรือแอปพลิเคชันจากระบบปฏิบัติการลินุกซ์หรือระบบปฏิบัติการวินโดวส์ได้

จากการดำเนินงานการเข้าถึงทรัพยากรระบบได้ใช้โปรโตคอล SSH และ SFTP ในการเข้าถึงพื้นที่ที่ใช้จัดเก็บทรัพยากรเพื่อให้ผู้ใช้สามารถเข้าไปจัดการทรัพยากรดังรูปที่ 4-3 แสดงการติดต่อเข้าไปจัดการทรัพยากร



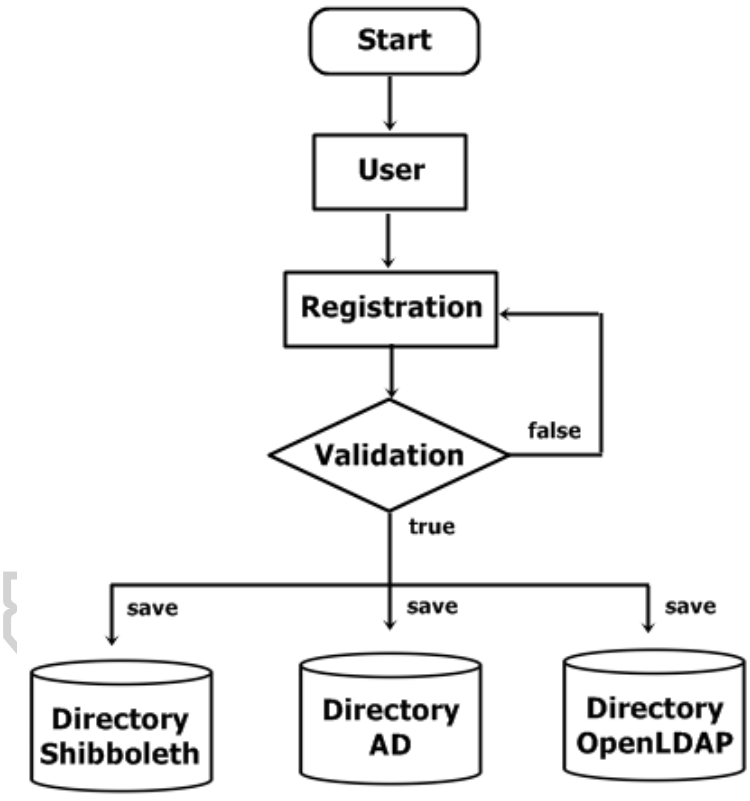
รูปที่ 4-3 แสดงการติดต่อเข้าไปจัดการทรัพยากร

2. การพัฒนาระบบการเข้าใช้งานทรัพยากร

เมื่อผู้ใช้สามารถลงทะเบียนและเข้าใช้งานระบบได้แล้วตามวัตถุประสงค์การศึกษาและพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆโดยการเข้าถึงทรัพยากรได้แบ่งออกเป็นสามส่วนดังนี้

1. ระบบการลงทะเบียน

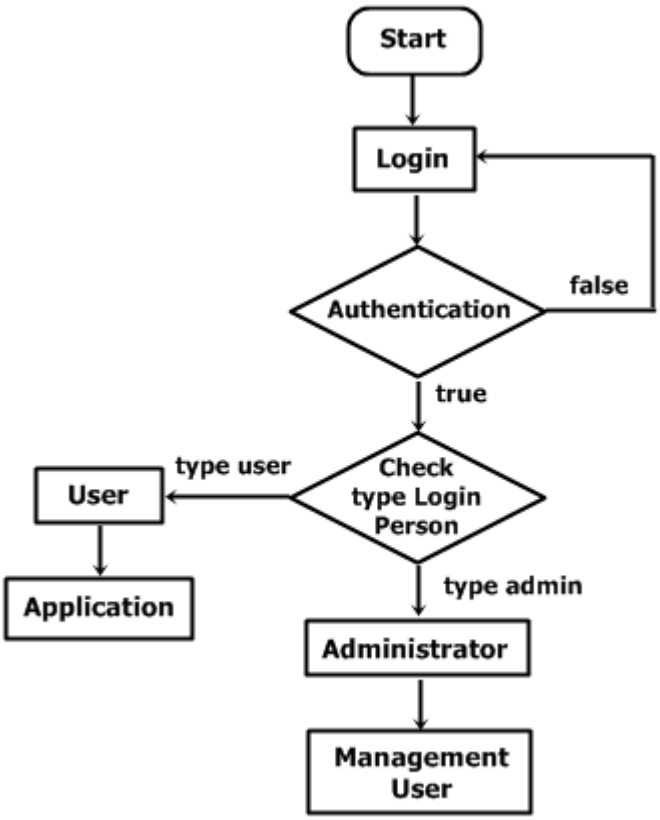
ในระบบการลงทะเบียนนี้ได้ใช้ภาษา PHP ในการพัฒนาระบบ โดยผู้ใช้ต้องกรอกข้อมูล ชื่อ, นามสกุล, ชื่อผู้ใช้ และ รหัสผ่าน ระบบจะทำการร้องขอการส่งค่าไปยัง IdP ที่อยู่บนเทคโนโลยี Shibboleth เพื่อขอสร้างชื่อผู้ใช้ลงไปยังไดเรกทอรีในที่นี้ใช้ LDAP หลังจากที่สามารถสร้างชื่อผู้ใช้ได้แล้ว จะส่งต่อไปยัง Active Directory และ OpenLDAP โดยใช้วิธีการสร้างชื่อผู้ใช้เช่นเดียวกับการสร้างชื่อผู้ใช้บน Shibboleth ดังรูปที่ 4-4 กระบวนการทำงานระบบลงทะเบียน



รูปที่ 4-4 กระบวนการทำงานระบบลงทะเบียน

2. ระบบการเข้าใช้งาน

ในส่วนของระบบการเข้าใช้งานนี้จะสามารถเข้าใช้งานได้หลังจากลงทะเบียนเรียบร้อยแล้ว ในการเข้าใช้งานระบบจะเข้าใช้งานผ่านเทคโนโลยี Shibboleth โดยกระบวนการการเข้าสู่ระบบจะเป็นไปดังรูปที่ 4-5 กระบวนการการเข้าสู่ระบบ



รูปที่ 4-5 กระบวนการการเข้าสู่ระบบ

จากรูปที่ 4-5 กระบวนการการเข้าสู่ระบบเริ่มต้นด้วยการที่ผู้ใช้ทำการเข้าสู่ระบบและระบบจะตรวจสอบตัวบุคคลของผู้ใช้ที่ลงทะเบียนไว้ที่ Shibboleth เมื่อตรวจสอบตัวตนแล้วระบบจะทำการตรวจสอบประเภทของผู้ใช้งาน ในกรณีที่ผู้ใช้เป็นประเภทผู้ใช้ทั่วไป เมื่อเข้าสู่ระบบได้แล้วจะสามารถเข้าสู่หน้าแอปพลิเคชันได้และในกรณีที่ผู้ใช้เป็นผู้ดูแลระบบเมื่อเข้าสู่ระบบได้แล้วเจอหน้าจัดการผู้ใช้และสามารถเข้าใช้งานได้

ในส่วนของระบบการเข้าใช้งานนี้จะใช้ภาษา JSP ในการพัฒนาระบบ ในการพัฒนาจะมีตัวอย่าง source code ดังรูปที่ 4-6 ตัวอย่าง source code การเข้าสู่ระบบ

```
<div class="content">
  <p>The web site described to the right has asked you to log in and you have chosen IDP.EXAMPLE.COM as your home :
  <% if ("true".equals(request.getAttribute("loginFailed"))) { %>
     <p><font color="red"> Credentials not recognized. </font> </p>
  <% } %>
  <% if(request.getAttribute("actionUrl") != null){ %>
    <form action="<%=request.getAttribute("actionUrl")%>" method="post">
  <% }else{ %>
    <form action="j_security_check" method="post">
  <% } %>
  <table>
    <tr>
       <td width="40%"><label for="username">Username:</label></td>
       <td><input name="j_username" type="text" id="username" autocapitalize="off" /></td>
    </tr>
    <tr>
       <td><label for="password">Password:</label></td>
       <td><input name="j_password" type="password" id="password" /></td>
    </tr>
    <tr><td></td><td><button value="Login" >Continue</button></td></tr>
  </table>
 </form>
```

รูปที่ 4-6 ตัวอย่าง source code การเข้าสู่ระบบ

ในการพัฒนาระบบการเข้าใช้งานโดยการส่งชื่อผู้ใช้และรหัสผ่านไปทาง URL ผ่านทาง HTTPS ผู้ให้บริการเครือข่ายจะส่งข้อมูลเครื่องไปยืนยันโดยใช้ URL

https://[Service Provider DNS NAME]/Shibboleth.sso/Login

เมื่อยืนยันตัวเครื่องเรียบร้อยผู้ใช้จะเข้าใช้งานระบบได้โดยผ่าน URL

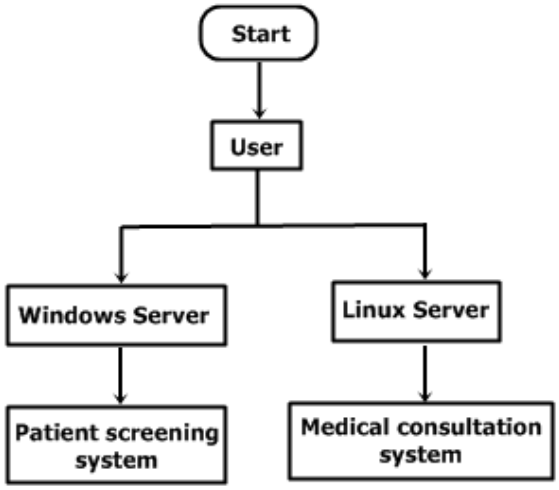
https://[Identity Provider DNS NAME]/idp/Authn/UserPassword

จากรูปที่ 4-7 หน้าจอการเข้าใช้งานระบบ แสดงหน้าจอที่ผู้ใช้ต้องใส่ชื่อผู้ใช้และรหัสผ่านโดยผ่าน URL ของ Identity Provider

รูปที่ 4-7 หน้าจอการเข้าใช้งานระบบ

3. ระบบการเข้าถึงแอปพลิเคชัน

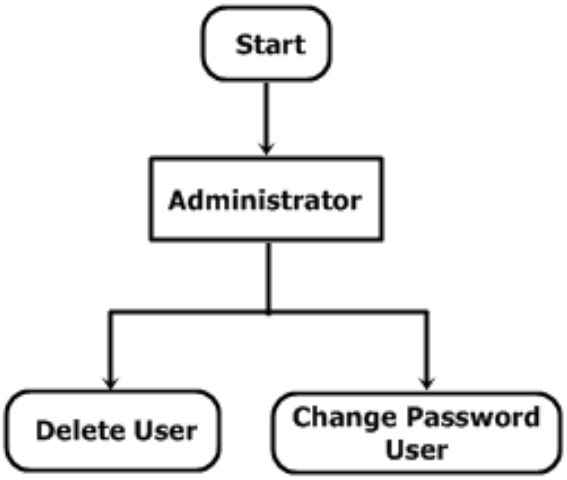
เมื่อผู้ใช้เข้าสู่ระบบเรียบร้อยแล้วจะเจอหน้าจอแสดงแอปพลิเคชันที่ผู้ใช้สามารถใช้งานได้โดย แอปพลิเคชันแต่ละตัวจะอยู่บนระบบปฏิบัติการที่แตกต่างกัน ผู้ใช้จะสามารถใช้งานแอปพลิเคชันได้จากส่วนนี้โดยกระบวนการเข้าใช้ทรัพยากรดังรูปที่ 4-8 กระบวนการเข้าใช้งานของผู้ใช้ทั่วไป



รูปที่ 4-8 กระบวนการเข้าใช้งานของผู้ใช้ทั่วไป

จากรูปที่ 4-8 กระบวนการเข้าใช้งานของผู้ใช้ทั่วไป เมื่อผู้ใช้งานเข้าสู่ระบบเรียบร้อยแล้ว ผู้ใช้จะเจอส่วนของให้เลือกเข้าใช้งานทรัพยากรสองส่วนคือ ในส่วนของแอปพลิเคชันการคัดกรองผู้ป่วยที่ทำงานบนระบบปฏิบัติการวินโดวส์และในส่วนของแอปพลิเคชันปรึกษาแพทย์ที่ทำงานบนระบบปฏิบัติการลินุกซ์

ในกรณีผู้ใช้เป็นผู้ดูแลระบบจะเจอหน้าจอในการจัดการผู้ใช้โดยสามารถลบและเปลี่ยนรหัสผ่านของผู้ใช้ได้ดังรูปที่ 4-9 กระบวนการเข้าใช้งานของผู้ดูแลระบบ



รูปที่ 4-9 กระบวนการเข้าใช้งานของผู้ดูแลระบบ

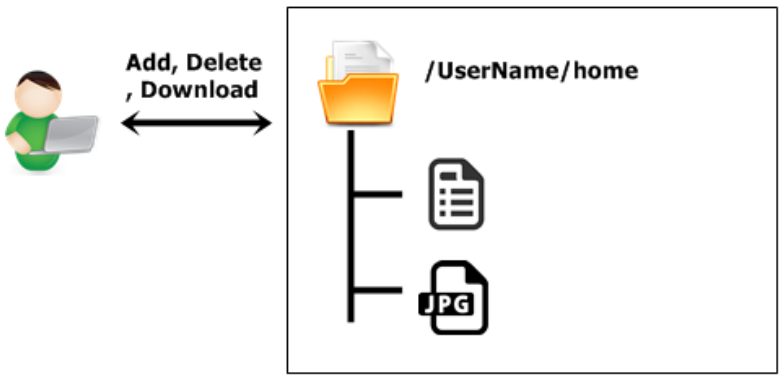
จากรูปที่ 4-9 กระบวนการเข้าใช้งานของผู้ดูแลระบบ เมื่อผู้ใช้เข้าสู่ระบบเรียบร้อยแล้วในกรณีที่ผู้ใช้เป็นผู้ดูแลระบบ ในส่วนนี้จะสามารถเข้าถึงหน้าจอแสดงการจัดการผู้ใช้โดยสามารถลบชื่อผู้ใช้งานระบบได้และสามารถแก้ไขรหัสผ่านผู้ใช้งานระบบได้ในทุกระบบปฏิบัติการ

3. การพัฒนาระบบบริหารจัดการการใช้งานทรัพยากร

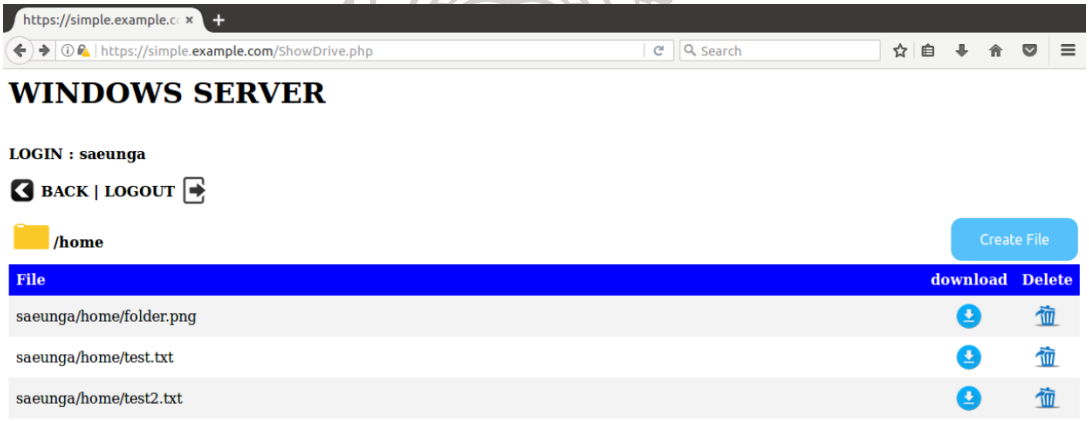
ในงานวิจัยนี้ได้พัฒนาระบบบริหารจัดการทรัพยากรตามวัตถุประสงค์เพื่อพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ โดยใช้ภาษา PHP และ MySQL ในการพัฒนาระบบบริหารจัดการทรัพยากรนี้ โดยได้แบ่งการใช้งานออกเป็นสองส่วนคือ การบริหารจัดการเอกสารและการบริหารจัดการแอปพลิเคชัน

1. การบริหารจัดการเอกสาร

ในการบริหารจัดการเอกสารนี้เป็นส่วนที่ผู้ใช้จะสามารถจัดการเอกสารได้จากเครื่องเซิร์ฟเวอร์ที่ทำงานบนระบบปฏิบัติการลินุกซ์และระบบปฏิบัติการวินโดวส์ ผู้ใช้จะสามารถใช้บริหารจัดการเอกสารได้จากเครื่องมือที่ผู้ใช้สามารถใช้งานได้คือ อัพโหลดไฟล์, ดาวน์โหลดไฟล์และลบไฟล์ ดังรูปที่ 4-10 แสดงการจัดการไฟล์บนระบบประมวลผลแบบกลุ่มเมฆ บนระบบปฏิบัติการวินโดวส์จะใช้ SFTP ในการติดต่อและระบบปฏิบัติการลินุกซ์จะใช้ SSH ในการติดต่อ



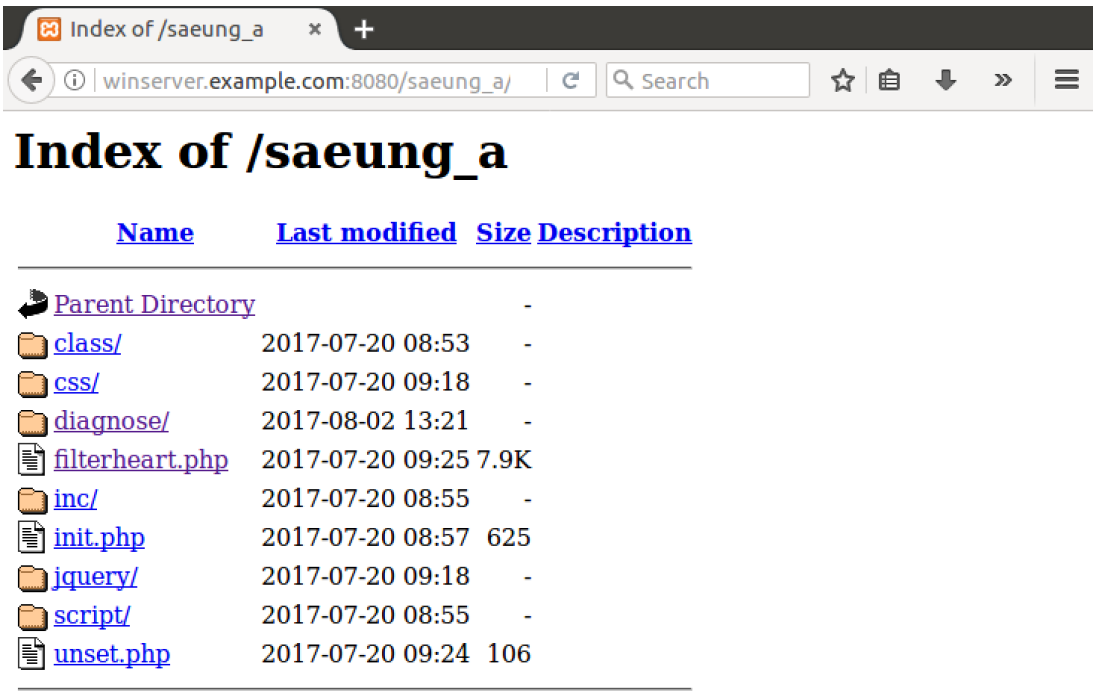
รูปที่ 4-10 แสดงการจัดการไฟล์บนระบบประมวลผลแบบกลุ่มเมฆ



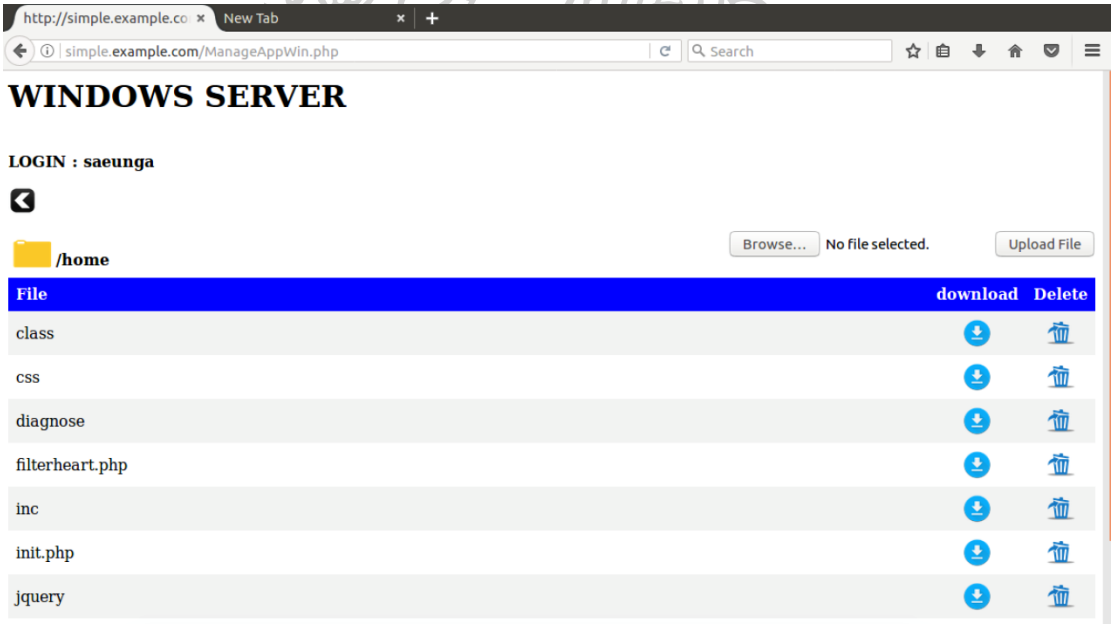
รูปที่ 4-11 แสดงหน้าจอการจัดการไฟล์บนระบบปฏิบัติการวินโดวส์

2. การบริหารจัดการแอปพลิเคชัน

ในการบริหารจัดการแอปพลิเคชันนี้จะทำงานบนระบบประมวลผลแบบกลุ่มเมฆโดยผู้ใช้จะสามารถสร้างแอปพลิเคชันบนพื้นที่ของผู้ใช้เองบนระบบปฏิบัติการวินโดวส์หรือระบบปฏิบัติการลินุกซ์ได้ โดยงานวิจัยนี้ได้เสนอการสร้างแอปพลิเคชันที่อยู่ในรูปแบบของเว็บแอปพลิเคชัน ดังรูปที่ 4-11 แสดงไดเรกทอรีทำงานเว็บแปพลิเคชันบนระบบปฏิบัติการวินโดวส์



รูปที่ 4-12 แสดงไดเรกทอรีทำงานเว็บแอปพลิเคชันบนระบบปฏิบัติการวินโดวส์



รูปที่ 4-13 แสดงหน้าจอการจัดการบริหารทรัพยากรแอปพลิเคชัน

ในส่วนของฐานข้อมูลผู้ใช้จะถูกสร้างชื่อลงบน My SQL และกำหนดสิทธิ์ในการเข้าใช้งานระบบจัดการทรัพยากรโดยการสร้างชื่อผู้ใช้จาก MySQL Shell ดังตัวอย่างการสร้างชื่อผู้ใช้ต่อไปนี้

```
CREATE USER 'newuser'@'localhost' IDENTIFIED BY 'password';
```

การสร้างชื่อผู้ใช้และกำหนดรหัสผ่านก่อนเบื้องต้นซึ่งรหัสผ่านระบบจะใช้รหัสผ่านของผู้ใช้ที่มีการเข้ารหัสอยู่แล้ว

```
GRANT privileges [ column ] ON item TO 'newuser'@'localhost';
```

การ GRANT เป็นการกำหนดสิทธิ์ของผู้ใช้

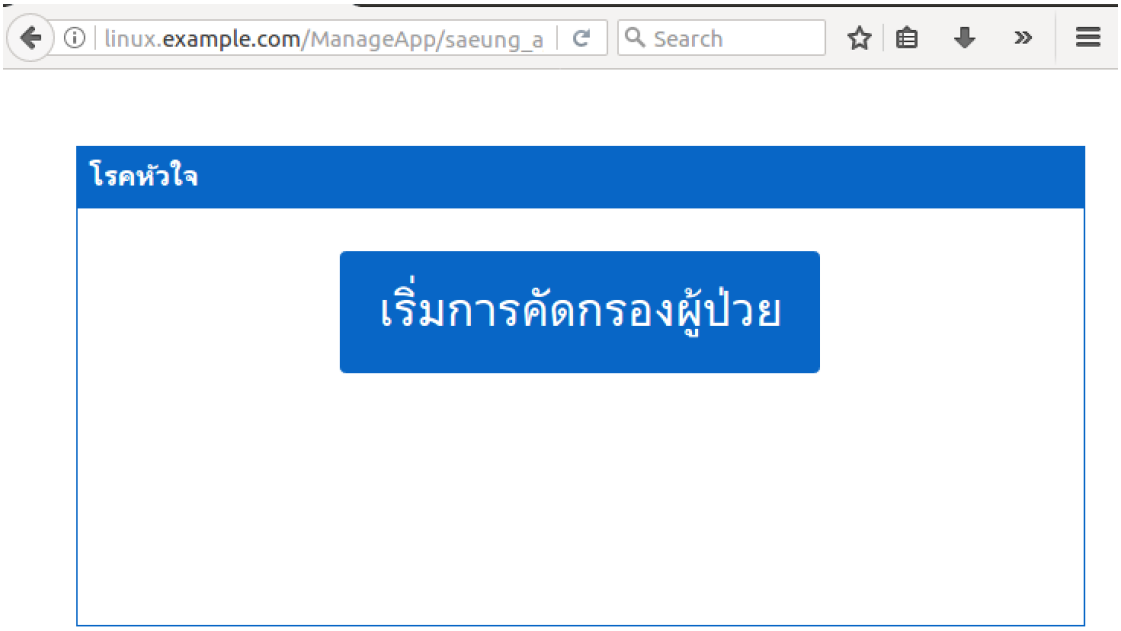
Column เป็นการระบุสิทธิ์กับคอลัมน์และสามารถใช้ชื่อคอลัมน์เดียวได้

Item คือ ฐานข้อมูล หรือ ตารางข้อมูลในการประยุกต์สิทธิใหม่

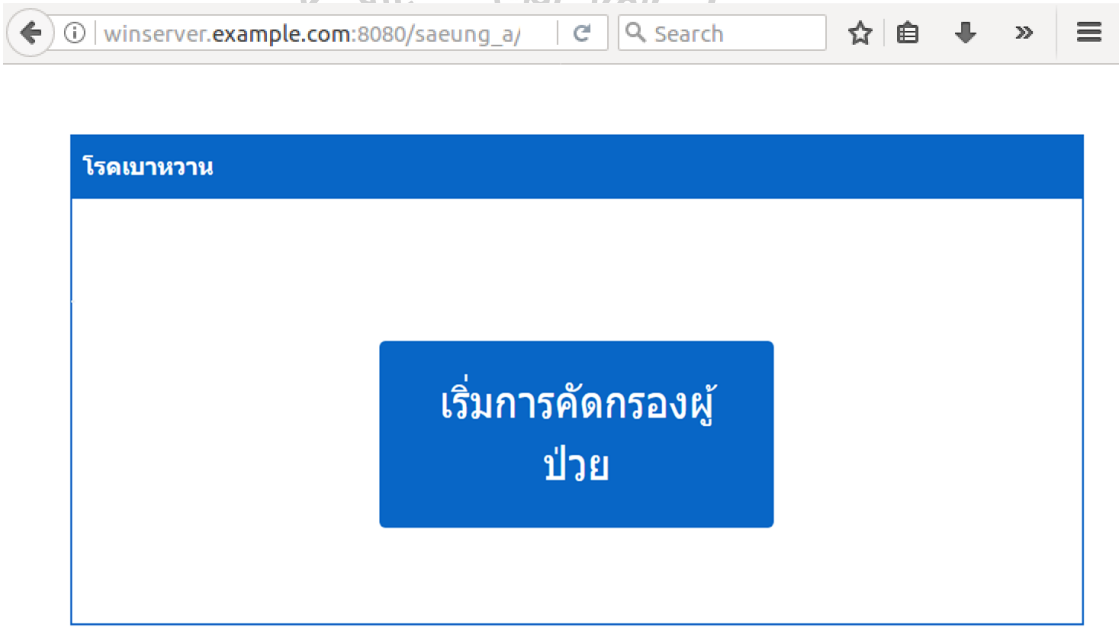
```
FLUSH PRIVILEGES;
```

FLUSH PRIVILEGES เป็นคำสั่งของการบันทึกค่าทั้งหมดที่ทำการกำหนดสิทธิ์ให้ผู้ใช้ถ้าไม่ใช้คำสั่งนี้คำสั่งที่เคยกำหนดมาจะไม่ถูกบันทึก

เมื่อผู้ใช้ทำการสั่งให้แอปพลิเคชันทำงานผู้ใช้ก็จะสามารถใช้งานได้ ดังรูปที่ 4-14 แสดงหน้าจอระบบคัดกรองผู้ป่วยโรคหัวใจและรูปที่ 4-15 แสดงหน้าจอระบบคัดกรองผู้ป่วยโรคเบาหวาน โดยผู้ใช้งานสามารถให้ผู้อื่นที่ไม่ได้ทำการลงทะเบียนหรือมีรายชื่อในระบบตัวกลางสามารถเข้าใช้งานระบบแอปพลิเคชันได้โดยการส่งลิงก์สำหรับเข้างานระบบ



รูปที่ 4-14 แสดงหน้าจอระบบคัดกรองผู้ป่วยโรคหัวใจ



รูปที่ 4-15 แสดงหน้าจอระบบคัดกรองผู้ป่วยโรคเบาหวาน

บทที่ 5
สรุปผลการวิจัย

งานวิจัยนี้ได้ศึกษาและพัฒนากลไกการพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรและพัฒนาระบบบริหารจัดการการเข้าใช้ทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆ โดยได้มีการศึกษาทฤษฎีของการตรวจสอบตัวตน Shibboleth, OpenLDAP และ Active Directory นำมาพัฒนาระบบพิสูจน์ตัวตนการเข้าใช้งานทรัพยากรและศึกษาทฤษฎีการจัดการทรัพยากร SSH และ SFTP ได้นำมาพัฒนาระบบการเข้าใช้งานทรัพยากรและพัฒนาระบบบริหารจัดการการใช้งานทรัพยากรที่ทำงานบนระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์ สรุปผลการวิจัยได้ดังนี้

1. ผู้ใช้สามารถใช้งานระบบบริหารจัดการทรัพยากรบนระบบปฏิบัติการวินโดวส์และระบบปฏิบัติการลินุกซ์ได้โดยการเข้าใช้งานครั้งเดียวทำให้ผู้ใช้ไม่จำเป็นต้องเข้าระบบซ้ำซ้อนเป็นการลดขั้นตอนการเข้าใช้งานระบบ
2. สามารถใช้งานระบบบริหารจัดการทรัพยากรที่สามารถจัดการทรัพยากรข้ามแพลตฟอร์มได้

ผลการดำเนินงานวิจัยนี้ทำให้ผู้ใช้สามารถเข้าใช้งานบริหารจัดการทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆได้โดยการเข้าใช้งานเพียงครั้งเดียวและสามารถบริหารจัดการทรัพยากรบนระบบประมวลผลแบบกลุ่มเมฆได้ทั้งระบบปฏิบัติการลินุกซ์และระบบปฏิบัติการวินโดวส์ได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะ

จากผลการทดลองแสดงให้เห็นถึงกระบวนการเข้าใช้งานระบบที่มีตัวกลางในการส่งต่อการเข้าใช้งานระบบเพื่อให้เข้าถึงทรัพยากรได้ ดังนั้นในอนาคตถ้านำต้นแบบนี้ไปพัฒนาต่อจะสามารถเข้าใช้งานระบบจัดการทรัพยากรหรือเข้าใช้ทรัพยากรในเครื่องเซิร์ฟเวอร์อื่น ๆ โดยการเข้าใช้งานครั้งเดียวได้

รายการอ้างอิง

1. Dheere, T. *Cloud-Based Tools*. [cited 2015 25 Dec]; Available from: https://tomdheere.com/voiceovers-stop-guessing-442017.
2. จตุชัย แพงจันทร์, อ.ว., เจาะระบบ *Network 3rd Edition*. 2555, นนทบุรี: บริษัท ไอดีซี พรีเมียร์ จำกัด 523.
3. Rouse, M. *X.500*. 2005 [cited 2016 12 April]; Available from: http://searchnetworking.techtarget.com/definition/X500
4. Ellrod, C. *LDAP Authentication*. [cited 2016 29 Jan]; Available from: https://www.citrix.com/blogs/2010/11/05/load-balancing-ldap-authentication
5. Library, M.M. *Active Directory*. [cited 2016 29 Jan]; Available from: https://msdn.microsoft.com/en-us/library/bb742424.aspx
6. (n.d.), I. *What's Shibboleth?* [cited 2016 24 Aug]; Available from: https://shibboleth.net/about/.
7. Rouse, M. *Secure Shell (SSH)*. 2016 [cited 2017 17 June]; Available from: http://searchsecurity.techtarget.com/definition/Secure-Shell.
8. VanDyke Software, I. *Secure Shell Overview*. 2008; Available from: http://vandyke.com/solution/ssh-overview/ssh-overview.pdf.
9. Daniel J. Barrett, R.E.S., *SSH, The Secure Shell*. 2001.
10. Rouse, M. *File Transfer Protocol (FTP)*. 2016; Available from: http://searchsecurity.techtarget.com/definition/File-Transfer-Protocol.
11. Courtney Powell, T.A., Masaharu Munetomo, *Design of an SSO authentication infrastructure for heterogeneous inter-cloud environments*, in *CloudNet*. 2014 2014 IEEE 3rd International Conference on Cloud Networking (CloudNet): Luxembourg, Luxembourg. p. 102 - 107.
12. Network, S.A.R.E. *Singapore Access Federation*. [cited 2016 03 Aug]; Available from: http://www.singaren.net.sg/SGAF.php.
13. Saley Mato Idrissa, K.D., Saley Bisso, Hamadou Saliah-Hassane *A secured resource access management in educational cloud computing environment*, in

2016 4th International Symposium on Digital Forensic and Security (ISDFS). 2016: Little Rock, AR, USA.

14. ศิริสารศักดา, น.ก. ปัจจัยเสี่ยงโรคเบาหวาน. Available from: http://yaandyou.net/content-view.php?conid=241.

15. สำนักโรคไม่ติดต่อ, ก., แนวการประเมินโอกาสเสี่ยงต่อการเกิดโรคหัวใจและหลอดเลือด.

ภาคผนวก

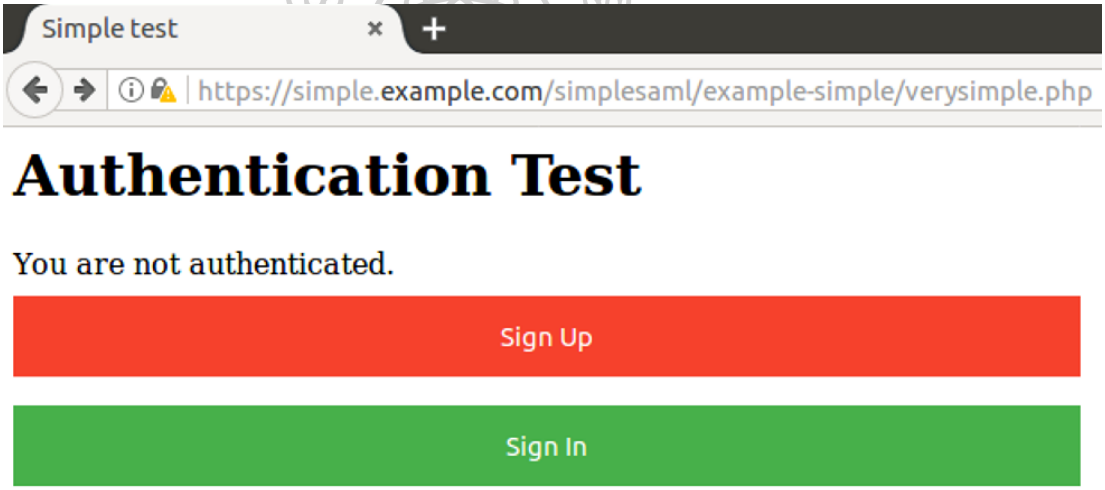
ภาคผนวก ก.

คู่มือการใช้งาน

คู่มือการใช้งานระบบ

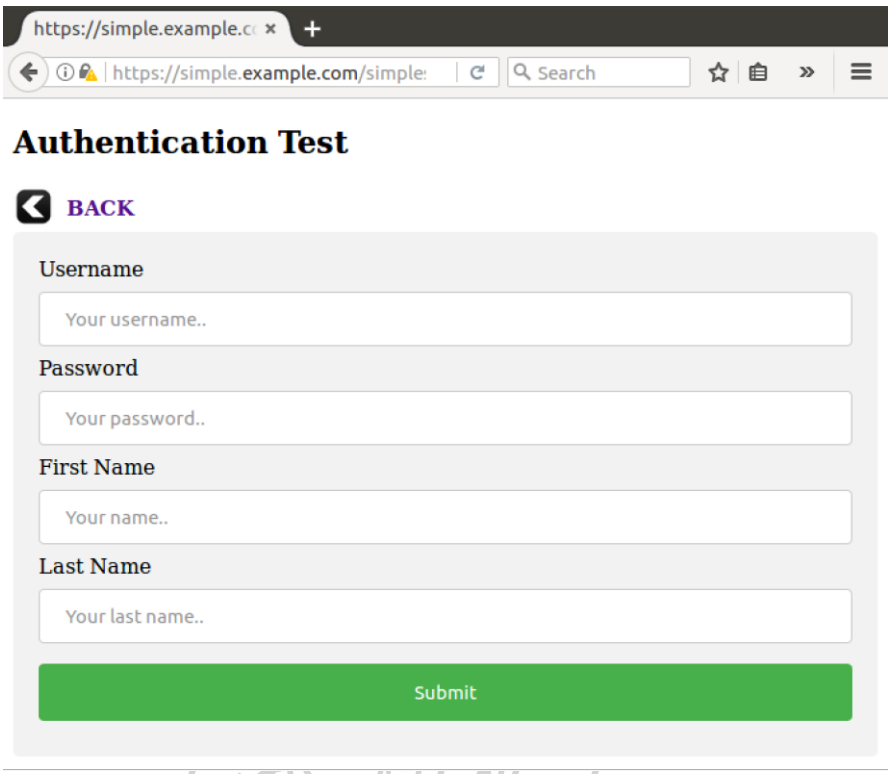
ในการพัฒนาต้นแบบระบบยืนยันตัวบุคคลบนระบบประมวลผลแบบกลุ่มเมฆได้มีหน้าจอแสดงผลการใช้งานดังนี้

1. เริ่มต้นการใช้งานจะเจอหน้าจอแสดงให้เลือกลงทะเบียนหรือเข้าสู่ระบบดังรูปที่ ก-1 หน้าจอแสดงเริ่มต้นการใช้งาน



รูปที่ ก-1 หน้าจอแสดงเริ่มต้นการใช้งาน

2. ในกรณีเลือกการลงทะเบียนจะเจอแบบฟอร์มของการลงทะเบียนดังรูปที่ ก-2 หน้าจอแสดงรายละเอียดลงทะเบียน เมื่อผู้ใช้ทำการลงทะเบียนข้อมูลจะถูกส่งไปบันทึกอัตโนมัติที่เครื่องวินโดวส์เซิร์ฟเวอร์และลินุกซ์เซิร์ฟเวอร์ด้วย

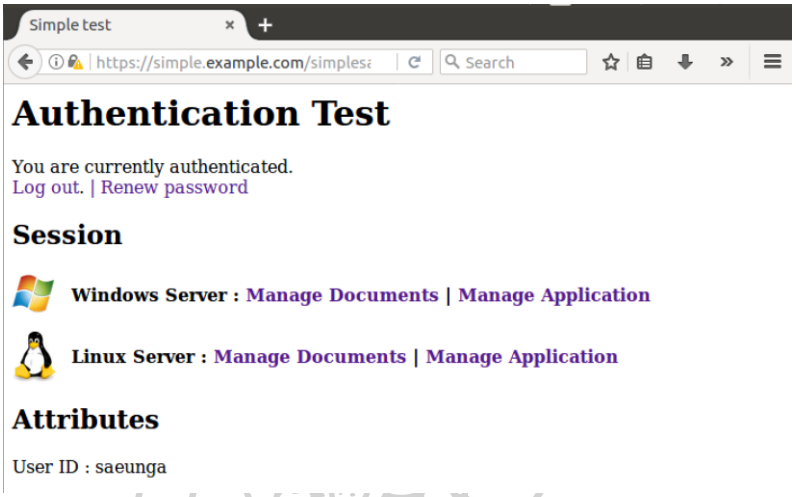


รูปที่ ก-2 หน้าจอแสดงรายละเอียดลงทะเบียน

3. เมื่อผู้ใช้มีอยู่ในระบบแล้วจะสามารถทำการเข้าใช้งานระบบได้ดังรูปที่ ก-3 หน้าจอแสดงการเข้าสู่ระบบ

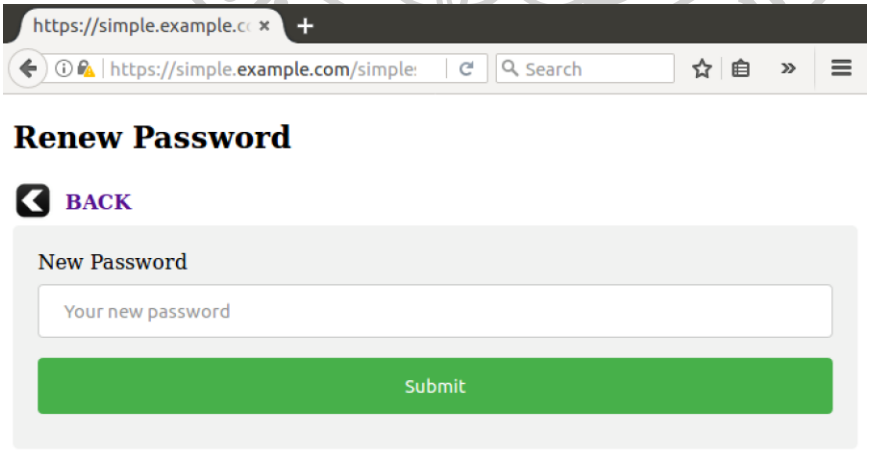
รูปที่ ก-3 หน้าจอแสดงการเข้าสู่ระบบ

4. เมื่อผู้ใช้เข้าสู่ระบบแล้วจะเจอหน้าจอแสดงข้อมูลที่จะเข้าสู่เครื่องวินโดวส์เซิร์ฟเวอร์และลินุกซ์เซิร์ฟเวอร์โดยผู้ใช้สามารถเลือกได้ว่าจะเข้าสู่ระบบบริหารจัดการทรัพยากรใด ดังรูปที่ ก-4 หน้าจอแสดงข้อมูลเมื่อเข้าสู่ระบบ



รูปที่ ก-4 หน้าจอแสดงข้อมูลเมื่อเข้าสู่ระบบ

5. ในส่วนนี้ผู้ใช้จะสามารถตั้งรหัสผ่านใหม่ของตนเองได้ จากเมนู Renew Password เมื่อกดเข้าไปจะสามารถเปลี่ยนรหัสผ่านได้ ดังรูปรูปที่ ก-5 หน้าจอแสดงการเปลี่ยนรหัสผ่าน



รูปที่ ก-5 หน้าจอแสดงการเปลี่ยนรหัสผ่าน

6. ผู้ใช้จะสามารถเลือกได้ว่าจะขอเข้าไปใช้ทรัพยากรบนเครื่องระบบปฏิบัติการใดดังรูปที่ ก-6 หน้าจอแสดงผลการใช้งานวินโดวส์แพลตฟอร์ม และสามารถกดปุ่มกลับไปและเข้าใช้งานที่เครื่องระบบปฏิบัติการลินุกซ์ ดังรูปที่ ก-7 หน้าจอแสดงผลการใช้งานลินุกซ์แพลตฟอร์ม

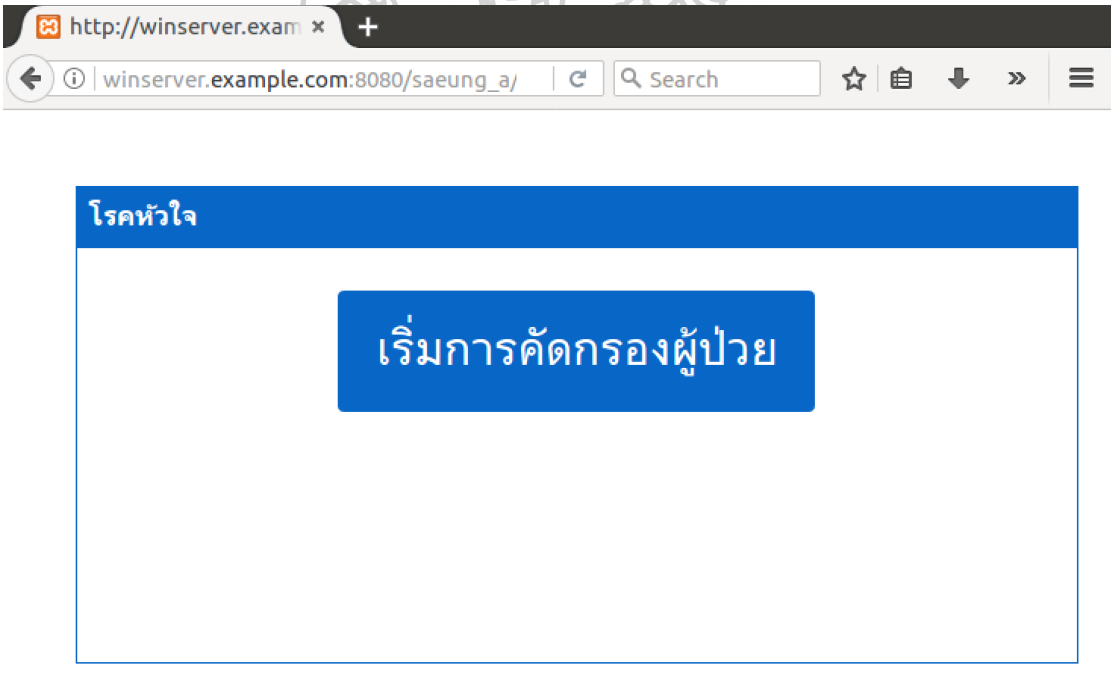
รูปที่ ก-6 หน้าจอแสดงผลการใช้งานวินโดวส์แพลตฟอร์ม

รูปที่ ก-7 หน้าจอแสดงผลการใช้งานลินุกซ์แพลตฟอร์ม

7. ในกรณีที่ผู้ใช้เลือกจัดการทรัพยากรแอปพลิเคชันผู้ใช้จะเจอหน้าจอแสดงรายละเอียดไฟล์ที่สามารถทำงานบนระบบปฏิบัติการได้ดังรูปที่ ก-8 แสดงไดเรกทอรีจัดการแอปพลิเคชัน

Name	Last modified	Size	Description
Parent Directory		-	
class/	2017-07-20 08:53	-	
css/	2017-07-20 09:18	-	
filterheart.php	2017-07-20 09:25	7.9K	
inc/	2017-07-20 08:55	-	
init.php	2017-07-20 08:57	625	
jquery/	2017-07-20 09:18	-	
script/	2017-07-20 08:55	-	
unset.php	2017-07-20 09:24	106	

รูปที่ ก-8 แสดงไดเรกทอรีจัดการแอปพลิเคชัน



รูปที่ ก-9 แสดงหน้าจอระบบคัดกรองผู้ป่วยโรคหัวใจ

ภาคผนวก ข.

คู่มือตั้งค่าระบบตรวจสอบการยืนยันตัวบุคคล

คู่มือตั้งค่าระบบตรวจสอบการยืนยันตัวบุคคล

ในส่วนของการตั้งค่าระบบตรวจสอบตัวตนนี้จะแบ่งออกเป็น 3 เครื่องเซิร์ฟเวอร์คือ

1. เครื่องหลักที่ใช้การตรวจสอบตัวตนโดย Shibboleth

. Shibboleth จะถูกติดตั้งลงในเครื่องหลักที่จะใช้ทำเป็นการเข้าสู่ระบบครั้งเดียว โดยจะแบ่งออกเป็นสองส่วนย่อยนั่นคือ ส่วนของผู้ให้บริการเครือข่าย (SP) และส่วนของผู้ให้บริการข้อมูล (IdP)

ติดตั้งและตั้งค่า IdP

ในส่วนของติดตั้ง IdP ในงานวิจัยนี้ได้ทำการติดตั้งลงบน CentOS 6.6 อุปกรณ์ที่ต้องเตรียมก่อนการติดตั้ง IdP คือ JAVA 1.7, Apache Tomcat เมื่อติดตั้งแล้วให้ทำการตั้งค่าสภาพแวดล้อมก่อนเริ่ม Tomcat

```
#export JAVA_HOME=/usr/local/src/jdk1.7
#export PATH=$JAVA_HOME/bin;$PATH
#export CATALINA_HOME=/usr/local/src/tomcat7
#export CATALINA_BASE=/usr/local/src/tomcat7
```

ในการตั้งค่าต่อมาจะทำการเรียก Java Virtual Machine โดยแก้ไขที่ TOMCAT_HOME/bin/catalina.sh โดยการเพิ่มบรรทัด

```
JAVA_OPTS="-Djava.awt.headless=true –Xmx512M
–XX:MaxPermSize=128M –Dcom.sun.security.enableCRLDP=true"
```

ทำการเริ่มต้น Tomcat : #TOMCAT_HOME/bin/catalina.sh start

ตรวจสอบโดยการเข้าเว็บเบราเซอร์และพิมพ์ http://localhost:8080

การติดตั้ง Shibboleth IdP

a) ทำการดาวน์โหลด Idp เวอร์ชันล่าสุดที่ (http://shibboleth.net/downloads/identity-provider) เมื่อดาวโหลดแล้วแตกไฟล์และติดตั้งในขั้นตอนนี้จะต้องกำหนดรหัสเพื่อไปใช้ระบุในส่วนของการตั้งค่า SOAP ให้จำรหัสที่ตั้งเอาไว้

```
# curl -O http://shibboleth.net/downloads/identity-provider/2.3.8/shibboleth-identityprovider-2.3.8-bin.zip
# unzip shibboleth-identityprovider-2.3.8-bin.zip
# cd shibboleth-identityprovider-2.3.8
# chmod u+x install.sh
# cp -r endorsed/ /usr/local/src/tomcat6
# export JAVA_ENDORSED_DIRS=/usr/local/src/tomcat6/endorsed
# ./install.sh
```

b) ตั้งค่าการรองรับ SOAP

โดยการดาวน์โหลด tomcat6-dta-ssl-1.0.0.jar ไปไว้ที่ TOMCAT_HOME/lib/ และเพิ่มจุดเชื่อมต่อโดยการตั้งค่าที่ไฟล์ TOMCAT_HOME/conf/server.xml และแก้ไข

```
<Connector port="8443"
  protocol="org.apache.coyote.http11.Http11Protocol"
  SSLImplementation="edu.internet2.middleware.security.tomcat6.
  DelegateToApplicationJSSEImplementation"
  scheme="https" SSLEnabled="true" clientAuth="true"
  keystoreFile="/opt/shibboleth-idp/credentials/idp.jks"
  keystorePass="yourPassword" />
```

c) การใช้ IdP WAR ไฟล์ โดยไฟล์นี้จะอยู่ใน IDP_HOME/war/ จะต้องทำการคัดลอกไฟล์มาไว้ยัง Tomcat webapps/ และทำการสร้างไฟล์ใหม่ชื่อ idp.xml ที่ /usr/local/src/tomcat7/conf/Catalina/localhost/idp.xml เพื่อที่จะให้เรียกการเข้าใช้งานหน้าเว็บจาก IdP

```
<Context docBase="/opt/shibboleth-idp/war/idp.war"
        privileged="true" antiResourceLocking="false"
        antiJARLocking="false" unpackWAR="false"
        swallowOutput="true" />
```

การเปิดใช้ SSL สำหรับ IdP

สำหรับการที่ยังไม่มี keystore เลยจำเป็นต้องสร้างขึ้นมาโดย

```
# keytool -genkey -alias tomcat -keyalg RSA -keystore /home/yourHomeDir/idpself.keystore
```

และทำการกำหนดใช้พอร์ต 443 โดยการเข้าไปแก้ไขที่ TOMCAT_HOME/conf/ server.xml

```
<Connector port="443"
  protocol="HTTP/1.1" scheme="https"
  SSLEnabled="true" clientAuth="true"
  maxTherads="150" sslProtocol="TLS"
  keystoreFile="/home/yourHomeDir/idpself.keystore"
  keystorePass="yourPassword" />
```

ติดตั้งและตั้งค่า SP

ในส่วนของติดตั้ง SP ในงานวิจัยนี้ได้ทำการติดตั้งลงบน Ubuntu 16.04 และใช้ SimpleSAMLphp ที่ถูกพัฒนาโดยองค์กร UNINETT มาทำงานส่วนของ SP โดยเริ่มจาก

ดาวโหลดและติดตั้งเวอร์ชันล่าสุด ดาวโหลดที่ (https://simplesamlphp.org/doanload)

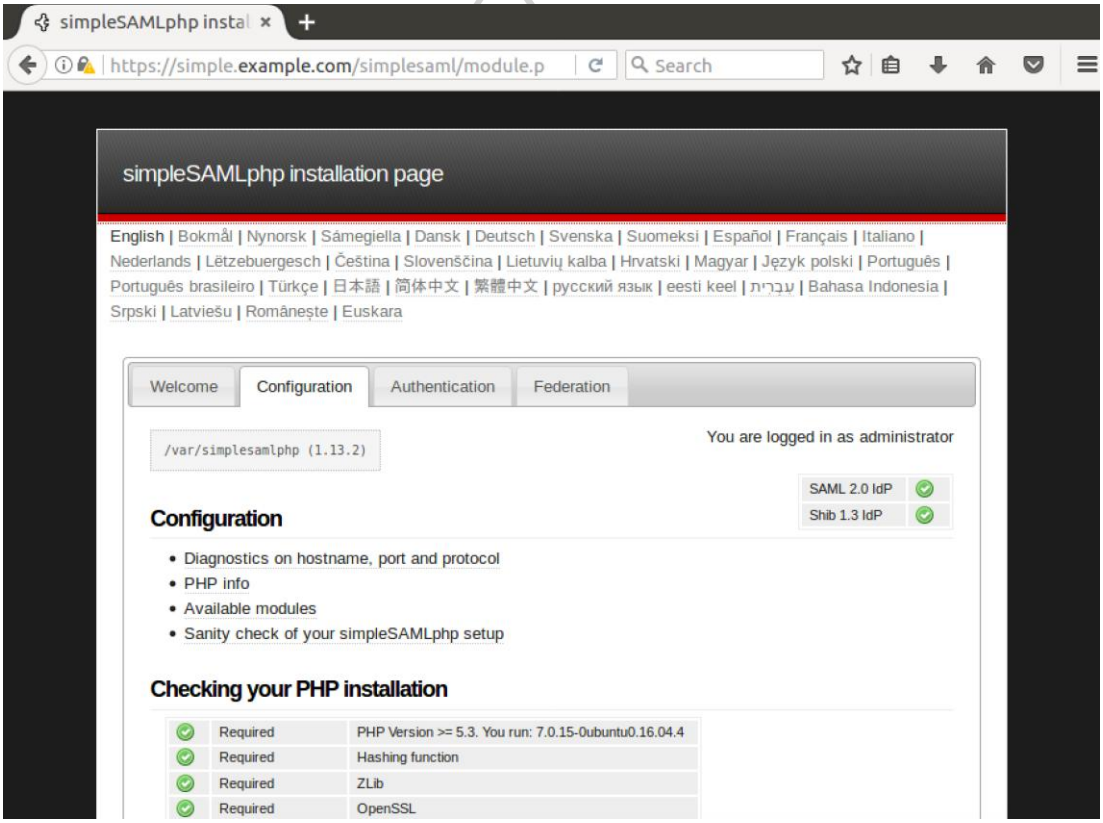
เมื่อติดตั้งเสร็จแล้วให้ทำการตั้งค่า secret salt

```
tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo
```

จะได้รหัสสุ่มมาให้คัดลอกเอาไว้และเข้าไปตั้งค่าที่ SIMPLESAMLPHP_HOME/config/config.php

```
'auth.administratorpassword'    =>    'setpasswordhere',
secretsalt'                     =>    'randombytesinserthere',
'timezone'                      =>     'Asia/Bangkok',
```

เมื่อตั้งค่าเสร็จสิ้นให้เข้าเว็บเบราว์เซอร์ http://[server_name]/simplesaml ดังรูปที่ ข-1 แสดงหน้าจอการเข้า simplesamlphp ในขั้นตอนการติดตั้ง SP ให้เข้าไปที่แถบของ Federation และอัพโหลดไฟล์ SAML 2.0 SP Metadata

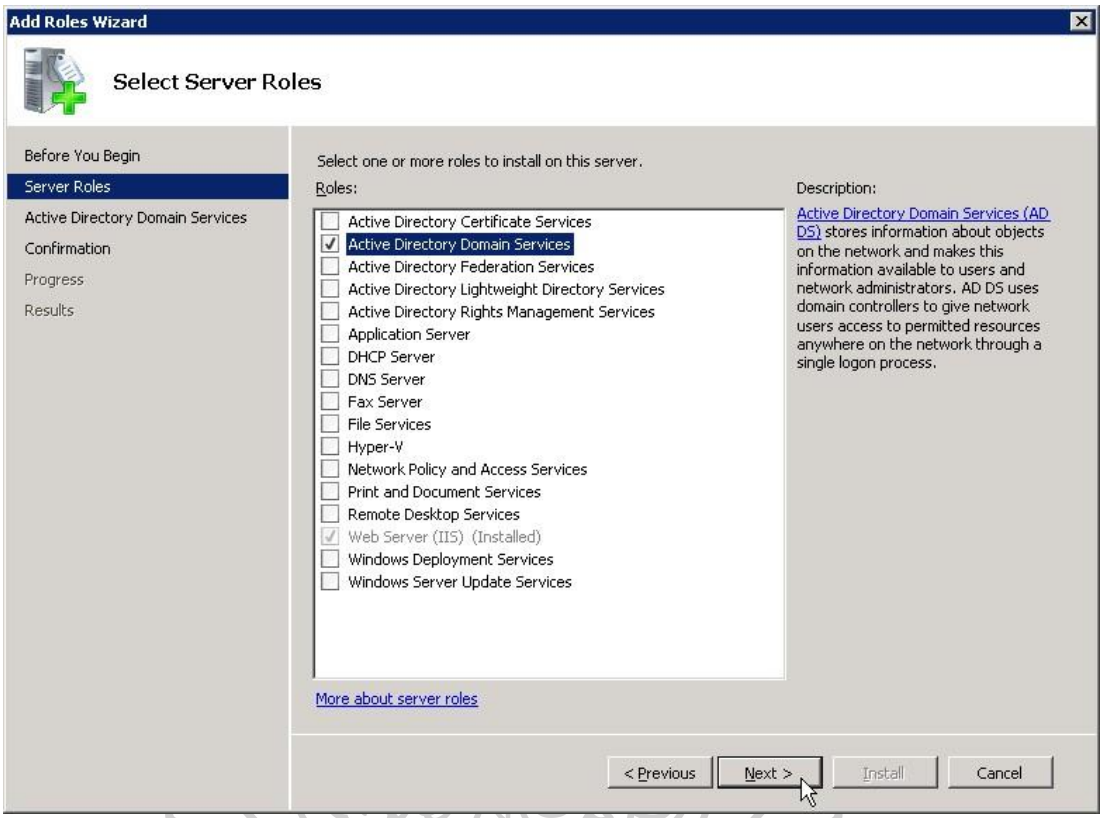


รูปที่ ข-1 แสดงหน้าจอการเข้า simplesamlphp

2. เครื่องให้ทรัพยากรที่ใช้การตรวจสอบตัวตนโดย Active Directory

ในงานวิจัยนี้เครื่องที่ใช้ทดสอบคือ Windows Server 2008 R2

เริ่มจากเข้ามาที่ Server Manager เลือก Add Roles จากนั้นจะเจอหน้าจอให้เลือก Role ให้ทำการเลือก Active Directory Domain Services ดังรูปที่ ข-2 แสดงการเลือก Roles กด Next ไปจนถึง Finish



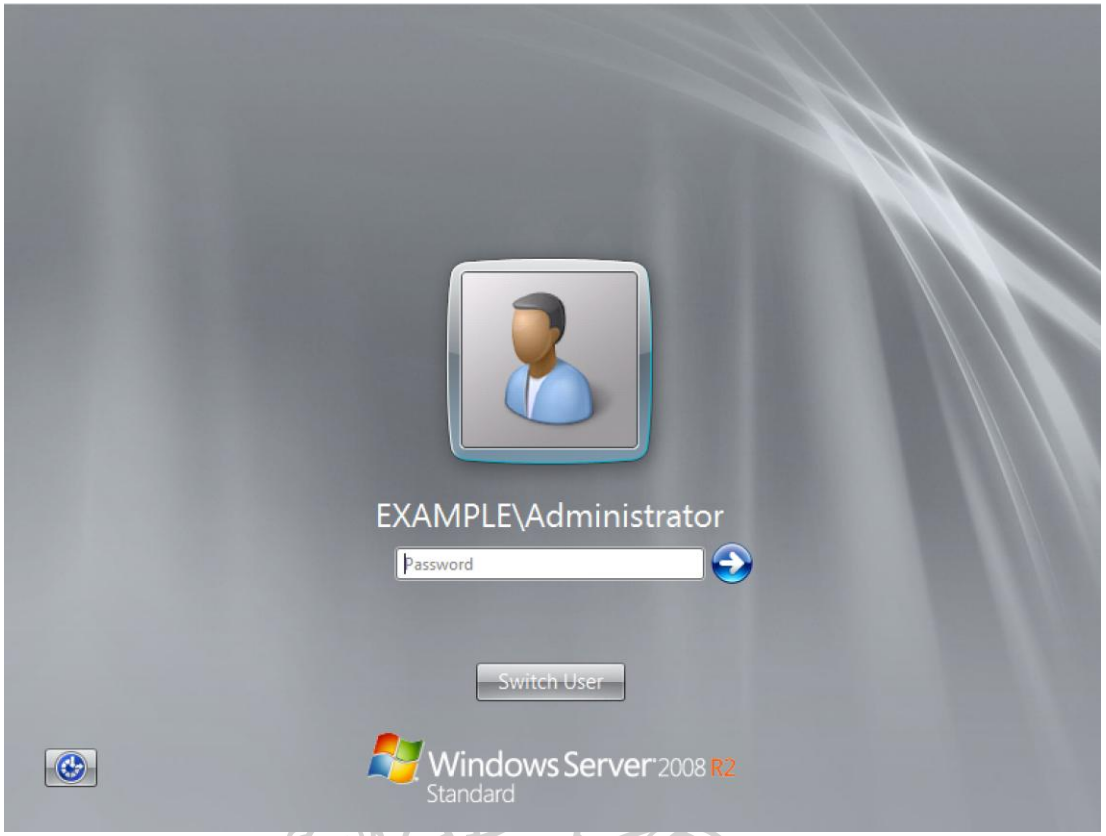
รูปที่ ข-2 แสดงการเลือก Roles

เมื่อติดตั้งเสร็จแล้วยังไม่สามารถใช้ได้ ให้มาที่ Start แล้วพิมพ์คำว่า dcpromo กดเลือกเข้าไปจะให้ตั้งค่าของ AD ดังรูปที่ ข-3 หน้าจอแสดงการใช้คำสั่ง dcpromo

รูปที่ ข-3 หน้าจอแสดงการใช้คำสั่ง dcpromo

- กด Next จะเจอหน้า Choose a Deployment Configuration .
- เลือก “Create a new domain in a new forest” และกด Next
- เมื่อเจอหน้า Name the Forest Root Domain ให้พิมพ์ชื่อโดเมนที่ต้องการใช้ กด Next
- จะเจอหน้าที่ให้เลือกเวอร์ชันเครื่องให้เลือก “Windows Server 2008 R2” กด Next
- เมื่อเจอหน้าที่ให้ตั้งรหัสผ่านให้ตั้งรหัสผ่านสำหรับ Administrator

ถ้าติดตั้งเสร็จสมบูรณ์จะเจอหน้าเจอให้เข้าใช้งานดังรูปที่ ข-4 หน้าจอแสดงการเข้าใช้งาน AD



รูปที่ ข-4 หน้าจอแสดงการเข้าใช้งาน AD

3. เครื่องให้ทรัพยากรที่ใช้การตรวจสอบตัวตนโดย OpenLDAP

ในงานวิจัยนี้เครื่องที่ใช้ทดสอบคือ Ubuntu 16.04

a) ทำการติดตั้งแพ็คเก็จของ LDAP

```
# apt-get install slapd ldap-utils
```

b) ตั้งค่าแพ็คเก็จของ slapd

```
# dpkg-reconfigure slapd
```

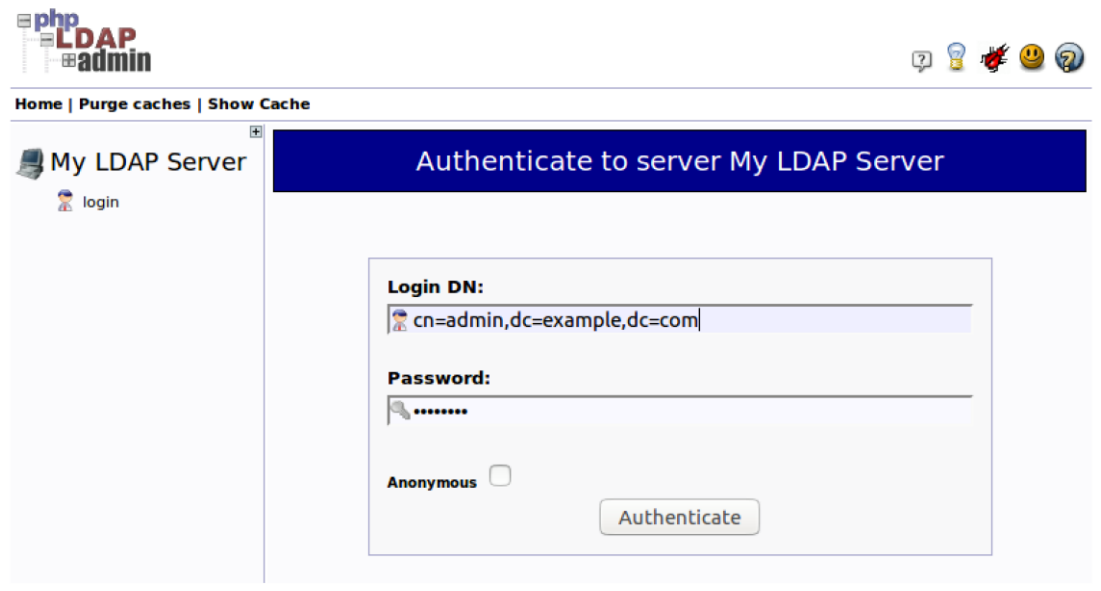
ในการตั้งค่าให้เลือกตั้งค่าตามนี้

- Omit OpenLDAP server configuration? No
- Organization name? ในที่นี่ใช้ SU
- Administrator password? ตั้งรหัสผ่านและยืนยัน
- Database backend? MDB
- Remove the database when slapd is purged? No
- Move old database? Yes
- Allow LDAPv2 protocol? No

c) เมื่อตั้งค่าเสร็จแล้วจะทำการติดตั้ง phpldapadmin

```
# apt-get install phpldapadmin
```

เมื่อติดตั้งเสร็จแล้วให้เข้าเว็บเบราว์เซอร์ https://localhosts/phpldapadmin ดังรูปที่ ข-5 แสดงหน้าจอการเข้าใช้งาน phpldapadmin



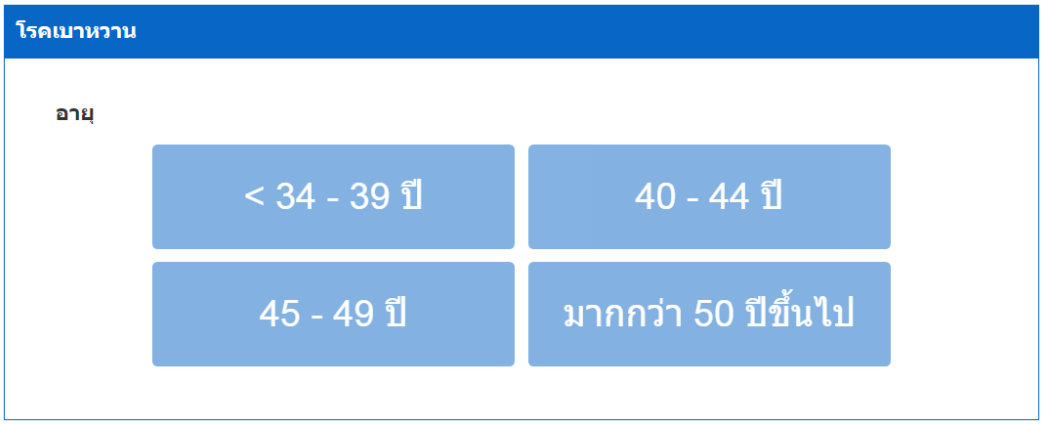
รูปที่ ข-6 แสดงหน้าจอการเข้าใช้งาน phpldapadmin

ภาคผนวก ค.

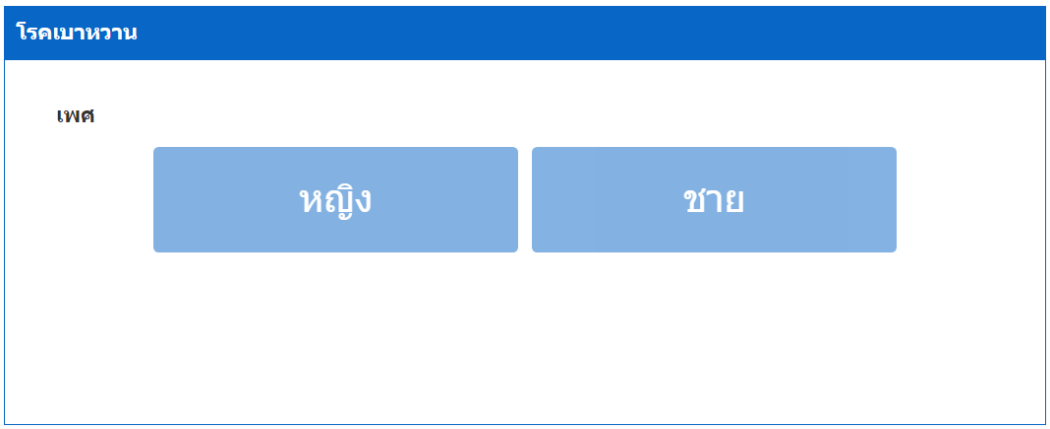
ระบบคัดกรองผู้ป่วย

ระบบคัดกรองผู้ป่วยโรคเบาหวาน

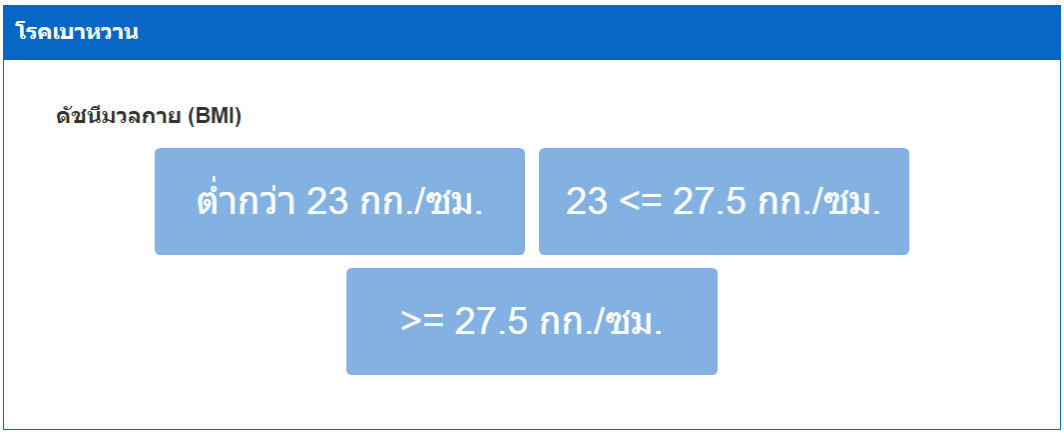
เมื่อเริ่มเข้าสู่ระบบคัดกรองผู้ป่วยโรคเบาหวานจะเจอคำถามดังต่อไปนี้



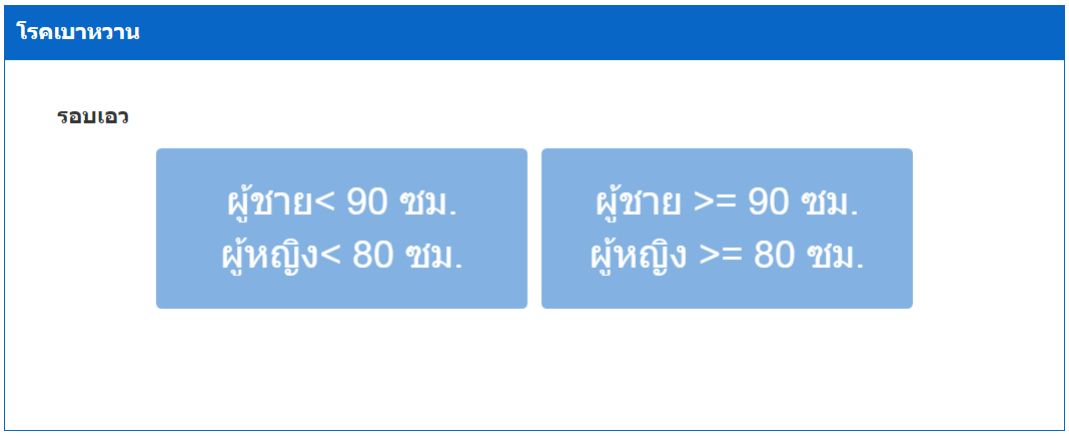
รูปที่ ค-1 แสดงหน้าจอถามช่วงอายุของผู้ป่วย



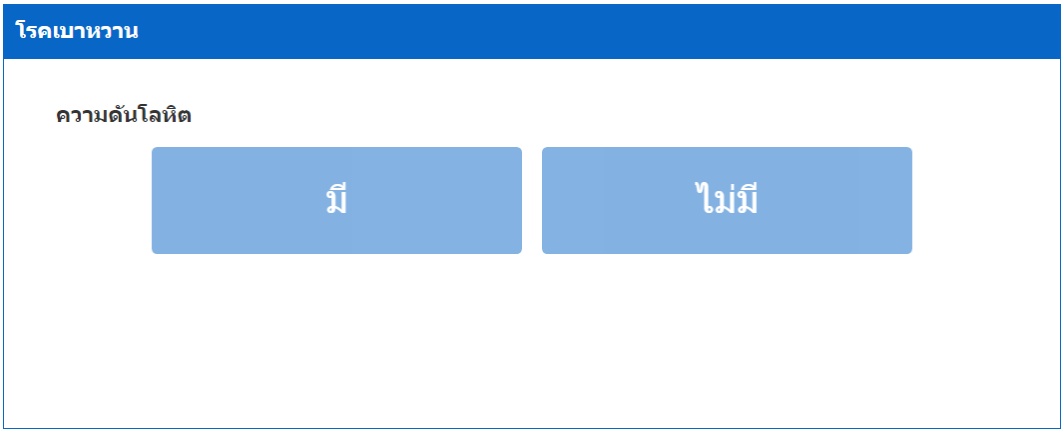
รูปที่ ค-2 แสดงหน้าจอถามเพศของผู้ป่วย



รูปที่ ค-3 แสดงหน้าจอถามค่า BMI ของผู้ป่วย

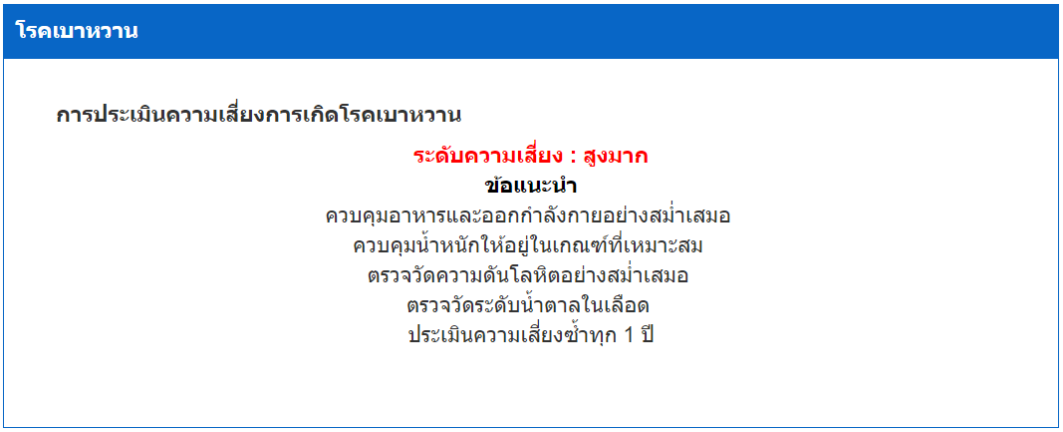


รูปที่ ค-4 แสดงหน้าจอถามรอบเอวของผู้ป่วย



รูปที่ ค-5 แสดงหน้าจอถามความดันโลหิตของผู้ป่วย

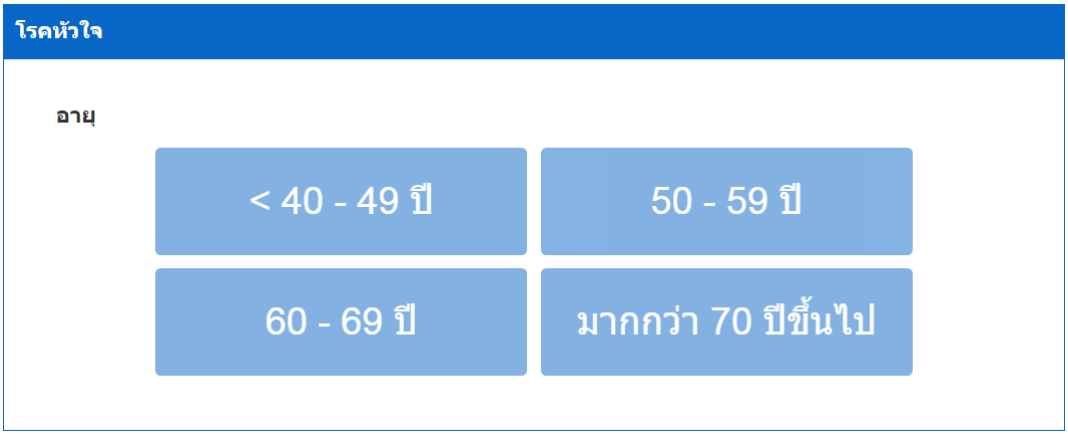
เมื่อผู้ป่วยได้ตอบคำถามครบทุกข้อแล้วหน้าจอจะแสดงผลของการวินิจฉัยเบื้องต้นออกมาเป็นค่าการประเมินความเสี่ยงการเกิดโรคเบาหวานดังรูปที่ ค-6 แสดงหน้าจอสรุปผลการวิเคราะห์โรคเบาหวาน



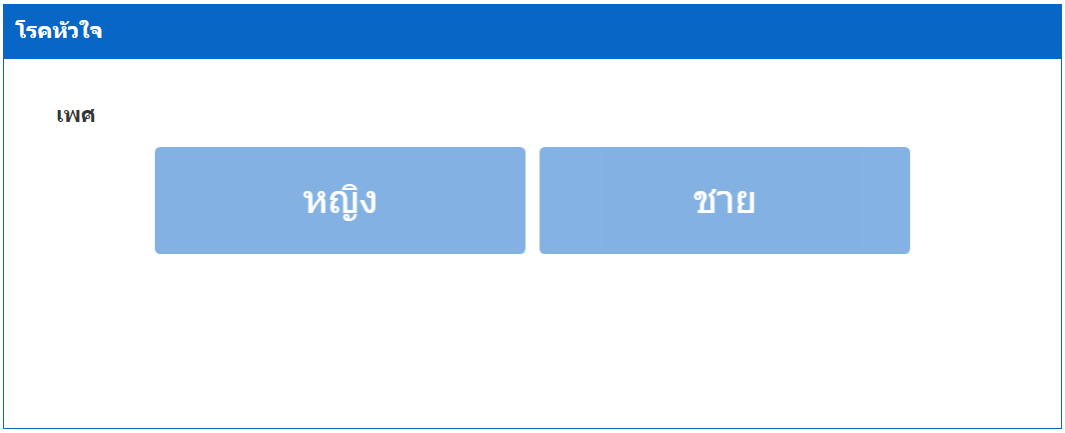
รูปที่ ค-6 แสดงหน้าจอสรุปผลการวิเคราะห์โรคเบาหวาน

ระบบคัดกรองผู้ป่วยโรคหัวใจ

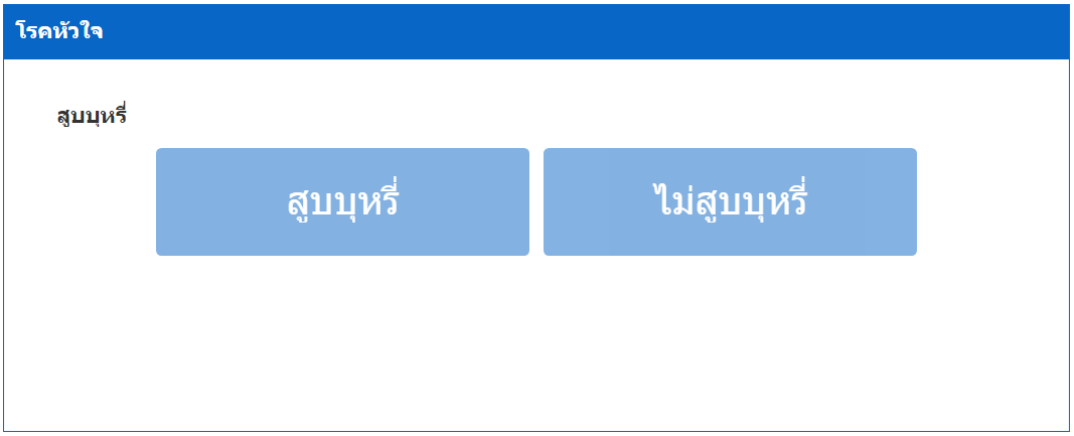
เมื่อเริ่มเข้าสู่ระบบคัดกรองผู้ป่วยโรคหัวใจจะเจอคำถามดังต่อไปนี้



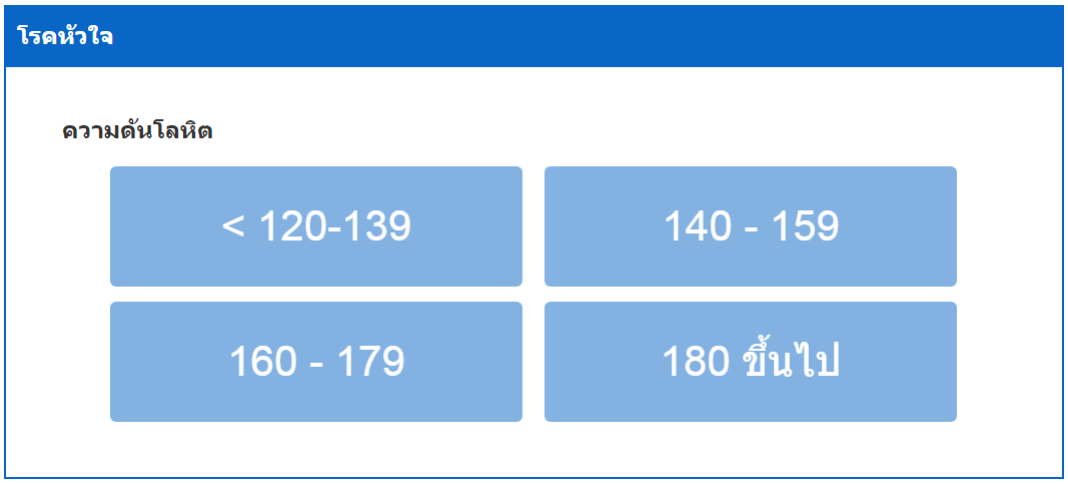
รูปที่ ค-7 แสดงหน้าจอถามช่วงอายุของผู้ป่วย



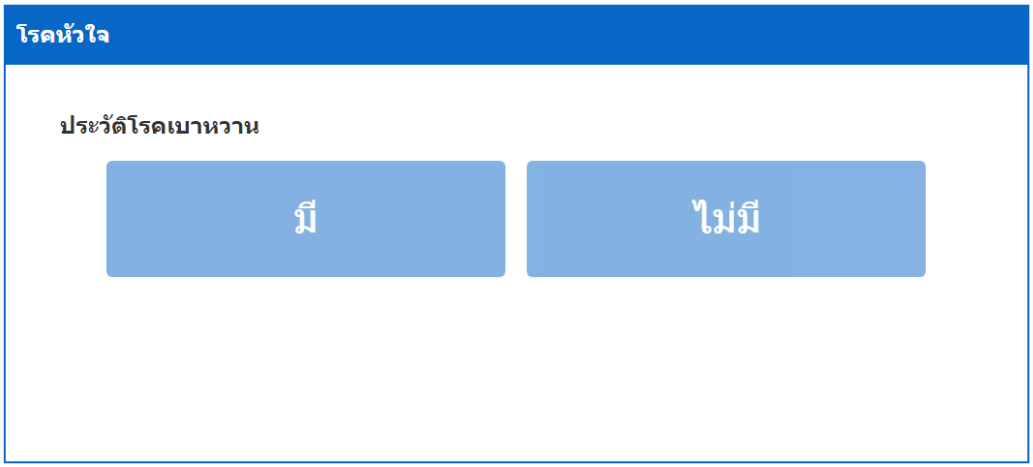
รูปที่ ค-8 แสดงหน้าจอถามเพศของผู้ป่วย



รูปที่ ค-9 แสดงหน้าจอของการสูบบุหรี่ผู้ป่วย

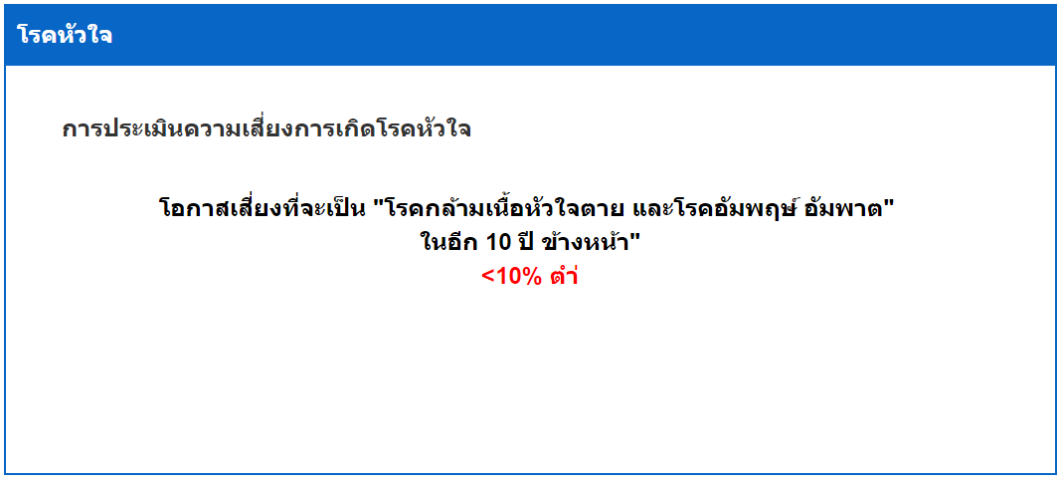


รูปที่ ค-10 แสดงหน้าจอของค่าความดันโลหิตผู้ป่วย



รูปที่ ค-11 แสดงหน้าจอประวัติการเป็นเบาหวานของผู้ป่วย

เมื่อผู้ป่วยได้ตอบคำถามครบทุกข้อแล้วหน้าจอจะแสดงผลของการวินิจฉัยเบื้องต้นออกมาเป็นค่าการประเมินความเสี่ยงการเกิดโรคเบาหวานดังรูปที่ ค-12 แสดงหน้าจอสรุปผลการวิเคราะห์โรคหัวใจ



รูปที่ ค-12 แสดงหน้าจอสรุปผลการวิเคราะห์โรคหัวใจ

ประวัติผู้เขียน

ชื่อ-สกุล	อัจฉริยา แซ่อึ้ง
วัน เดือน ปี เกิด	02 กุมภาพันธ์ 2534
วุฒิการศึกษา	พ.ศ. 2551 สำเร็จการศึกษามัธยมศึกษาตอนปลาย โรงเรียนพระปฐมวิทยาลัย จังหวัดนครปฐม
	พ.ศ. 2555 สำเร็จการศึกษาปริญญาตรี วิทยาศาสตรบัณฑิต (วท.บ.) สาขาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร
	พ.ศ. 2557 ศึกษาต่อระดับปริญญามหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร
ที่อยู่ปัจจุบัน	เลขที่ 566 ถนนทางรถไฟตะวันตก ตำบลพระปฐมเจดีย์ อำเภอเมือง จังหวัดนครปฐม รหัสไปรษณีย์ 73000