ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

ระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

Secure Authentication Gateway System

โดย

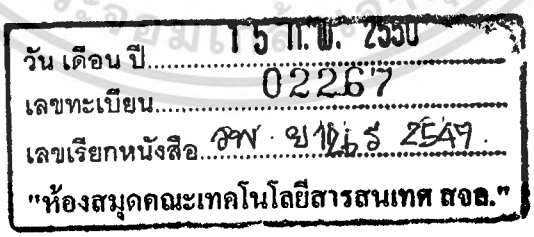
ยงยุทธ ชูชัยเจริญ

รหัส 45061630

H002267

อาจารย์ที่ปรึกษา

ผศ.ดร. โชติพัชร์ ภรณวลัย



b11701205
i1897234

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2547

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อหัวข้อ	ระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง
นักศึกษา	นาย ยงยุทธ ชูชัยเจริญ
อาจารย์ที่ปรึกษา	ผศ.ดร. โชติพัชร์ ภรณวลัย
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2547

บทคัดย่อ

เนื่องจากในปัจจุบันการใช้งานผ่านเครือข่ายไร้สายมีมากขึ้น ความปลอดภัยจึงเป็นเรื่องสำคัญในการใช้งาน เพราะข้อมูลที่มีการรับส่งผ่านเครือข่ายไร้สายอาจถูกนำไปใช้ในทางที่ไม่ดีได้ โครงงานระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงจึงถูกพัฒนาขึ้นมาเพื่อสร้างความปลอดภัยในการใช้งานผ่านเครือข่ายไร้สาย อีกทั้งภายในระบบยังสามารถที่จะตรวจสอบการใช้งานของผู้ใช้บริการและการคำนวณค่าใช้จ่ายในการใช้งานได้อีกด้วย

ในการพัฒนาโครงงานนี้ได้มีการนำเอาโอเพ่นซอฟท์แวร์ 2 ส่วนมาพัฒนาและปรับปรุงเพื่อให้เข้ากับความต้องการในการใช้งาน โดยส่วนแรกคือ NoCatAuth เป็นส่วนที่ใช้สำหรับทำการจัดการในเรื่องของการพิสูจน์ตัวจริงในการเข้าใช้งานในระบบ และอีกส่วนคือ OpenVPN เป็นส่วนที่ใช้สำหรับการสร้างการเชื่อมต่อในระบบ VPN เพื่อเพิ่มความปลอดภัยในการรับ-ส่งข้อมูล โดยระบบที่ได้จากการพัฒนาของโอเพ่นซอฟท์แวร์ 2 ส่วนนี้คือ ระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง และนอกจากนี้ภายในโครงงานยังมีการพัฒนาระบบตรวจสอบการใช้งานสำหรับผู้ใช้บริการและระบบควบคุมดูแลสำหรับผู้ดูแลระบบ เพื่อทำหน้าที่จัดการดูแลข้อมูลการใช้งานต่าง ๆ ของผู้ใช้บริการและการคำนวณการใช้งานของผู้ใช้บริการ โดยการคำนวณจะคิดจากจำนวนแพ็คเก็ทที่ผู้ใช้ได้ใช้งานจริง

ระบบทั้งหมดจะทำงานภายใต้เว็บเซิร์ฟเวอร์ที่ใช้โปรแกรม Apache และมีการใช้โปรแกรมภาษา PHP โปรแกรมภาษา Perl และโปรแกรมภาษา Shell Script สำหรับการพัฒนาระบบ นอกจากนี้ ยังมีการใช้โปรแกรม MySQL เป็นฐานข้อมูล และโปรแกรม Freeradius สำหรับส่วนที่ใช้ในการติดต่อระหว่างตัวระบบกับฐานข้อมูลในการพิสูจน์ตัวจริง (Authentication) และการเก็บจำนวนการใช้งาน (Accounting) โดยระบบทั้งหมดที่พัฒนาขึ้นสามารถทำงานได้อย่างมีประสิทธิภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title	Secure Authentication Gateway System
Student	Mr. Yongyuth Choochaijaroen
Advisor	Asst. Prof. Dr. Chotipat Pornavalai
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2004

Abstract

At present usage on wireless network has increasingly. So security system is important because hacker can find many way to sniff packets that transfer on wireless network and may bring its use to malicious. So Secure Authentication System have developed for solve a security problem on wireless network. In addition to solving this project can to check usage data and also calculate it to cost.

For development project will use two open source program. The First one is the NoCatAuth program which is the authentication system. And the second one is OpenVPN which is a VPN system for create tunnel for security of data transmission between client and server after authentication is passed. Other development are system for user, control & management system for administrator that manage user information and usage data. The usage data that is calculated to cost for each user in byte-based format.

This project work on apache web server and develop by PHP, Perl and shell script language. MySQL is database system and Radius uses FreeRadius for authentication and accounting system.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ผู้จัดทำโครงการได้รับความช่วยเหลือและสนับสนุนจากหลายฝ่ายในการศึกษาและพัฒนาระบบงาน ซึ่งถ้าไม่มีบุคคลเหล่านี้การศึกษาและพัฒนาระบบงานคงไม่สำเร็จลงได้ จึงใคร่ขอขอบพระคุณ

ผศ.ดร. โชติพัชร์ ภรณวลัย ซึ่งเป็นอาจารย์ที่ปรึกษาโครงงาน ที่ช่วยให้คำแนะนำในการจัดทำโครงงาน ให้คำปรึกษาในด้านเนื้อหาที่เป็นประโยชน์

คุณสมเจิด โพธิ์ทอง สำหรับการปรึกษาเรื่องระบบการพิสูจน์ตัวจริงที่ใช้โปรแกรม NoCat

คุณบุษบา สุดสน สำหรับคำแนะนำเรื่องของรูปแบบ Interface ที่ใช้ในระบบและกำลังใจ

คุณประภาศรี ขจรเดชและคุณจิตราภรณ์ แซ่โง้ว ที่ให้คำปรึกษาเรื่องของโปรแกรมภาษาที่ใช้ในการพัฒนาระบบคือ PHP , Perl และ JavaScript

ขอบคุณเพื่อนๆ ที่ให้คำแนะนำและกำลังใจที่ดีตลอดมา

สุดท้ายขอกราบขอบพระคุณ บิดา มารดา ผู้มีพระคุณสูงสุดที่ให้การสนับสนุนตลอดระยะเวลาที่ศึกษา

ยงยุทธ ชูชัยเจริญ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 ที่มาของโครงงาน

เนื่องด้วยในยุคปัจจุบันนี้ การใช้งานภายในระบบเครือข่ายไม่ว่าจะเป็นเครือข่าย Wireless LAN หรือ Wired LAN นั้น ความปลอดภัยเป็นสิ่งจำเป็นต่อระบบ ระบบการพิสูจน์ตัวจริงผ่านเว็บเบราเซอร์ก็เป็นส่วนหนึ่งที่จะช่วยในการสร้างระบบเครือข่ายให้มีความปลอดภัย แต่ก็ไม่เพียงพอต่อความปลอดภัยภายในระบบเครือข่าย เนื่องจากระบบดังกล่าวเป็นเพียงระบบที่ช่วยสร้างความปลอดภัยในการที่จะมิให้ผู้ที่มีสิทธิ์ เข้ามาใช้งานในระบบเท่านั้น แต่การรับ-ส่งข้อมูลหลังจากการพิสูจน์ตัวจริงยังไม่ปลอดภัย ซึ่งอาจมีผู้ไม่ประสงค์ดีสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์ที่มิชอบได้

ดังนั้นโครงงานนี้จึงมุ่งเน้นในด้านการพัฒนาและออกแบบระบบพิสูจน์ตัวจริงผ่านเว็บเบราเซอร์ให้มีความปลอดภัยมากขึ้น โดยมีการเพิ่มความปลอดภัยในการใช้งานโดยการนำเครือข่าย VPN เข้ามาประยุกต์ใช้ในการรับ-ส่งข้อมูลหลังจากการพิสูจน์ตัวจริงผ่านเว็บเบราเซอร์ ซึ่งจะทำให้ระบบมีความปลอดภัยมากขึ้น

นอกจากการพัฒนาระบบพิสูจน์ตัวจริงให้มีความปลอดภัยโดยการนำเครือข่าย VPN มาใช้ภายในระบบยังมีการออกแบบและพัฒนาระบบให้สามารถที่จะคำนวณการใช้งานของผู้ใช้ในรูปแบบที่ใช้งานจริงเป็นแพ็คเก็ท (Byte-based) ได้อีกด้วย เพื่อสามารถที่จะนำระบบนี้ไปใช้งานในส่วนที่ต้องการเก็บเงินกับผู้ใช้งานได้

1.2 วัตถุประสงค์ของโครงงาน

- เพื่อสร้างระบบให้สามารถใช้งานระบบการพิสูจน์ตัวจริง ในการลงทะเบียนขอรหัสผู้ใช้งานและรหัสผ่านด้วยเว็บเบราเซอร์ที่มีการเข้ารหัสรักษาความปลอดภัยได้
- เพื่อสร้างความปลอดภัยภายในระบบเครือข่ายให้มีความปลอดภัยมากขึ้น โดยการนำเครือข่าย VPN เข้ามาใช้งาน หลังจากที่มีการพิสูจน์ตัวจริงของผู้ใช้งานผ่านเว็บเบราเซอร์
- เพื่อสร้างระบบที่สามารถคำนวณการใช้งานของผู้ใช้ได้

1.3 ขอบเขตของการพัฒนาโครงงาน

- สร้างระบบพิสูจน์ตัวจริงของผู้ใช้งาน ผ่านเว็บเบราเซอร์ที่มีความปลอดภัยได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- สร้างระบบความปลอดภัยในการรับ-ส่งข้อมูลหลังจากผู้ใช้มีการพิสูจน์ตัวจริงเรียบร้อยแล้วด้วยเครือข่าย VPN
- สร้างระบบคำนวณการใช้งานของผู้ใช้งานในรูปแบบแพ็คเก็ท (Byte-based) ได้
- สร้างระบบสำหรับให้ผู้ใช้งานสามารถตรวจสอบการใช้งานของตัวเองได้
- สร้างระบบสำหรับผู้ดูแลระบบหรือเจ้าหน้าที่ให้สามารถมอนิเตอร์การใช้งานของผู้ใช้ได้
- สร้างระบบสำหรับผู้ดูแลระบบหรือเจ้าหน้าที่ให้การตรวจสอบอนุญาตให้ผู้ใช้สามารถเข้าใช้งานในระบบได้
- สร้างระบบสำหรับผู้ดูแลระบบหรือเจ้าหน้าที่ให้สามารถควบคุมและจัดการระบบผ่านเว็บเบราเซอร์ได้
- โปรแกรมจะได้รับการพัฒนา สามารถติดตั้งลงในระบบปฏิบัติการลีนุกซ์ได้

1.4 ประโยชน์ที่คาดว่าจะได้รับ

สามารถนำระบบนี้ไปใช้งานได้จริงในปัจจุบัน เพื่อช่วยเพิ่มประสิทธิภาพทางด้านความปลอดภัยภายในระบบเครือข่าย ไม่ว่าจะเป็นเครือข่าย Wireless LAN หรือ Wired LAN ได้ และนอกจากนี้ ยังสามารถที่จะนำระบบนี้ไปใช้ในการเรียกเก็บเงินจากผู้ใช้จากการคำนวณการใช้งานของผู้ใช้ได้อีกด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
การพัฒนาระบบรักษาความปลอดภัยเครือข่ายไร้สาย

2.1 ระบบเครือข่ายไร้สาย

2.1.1 โครงสร้างการทำงานของระบบเครือข่ายไร้สาย

ในระบบเครือข่ายไร้สาย IEEE 802.11 นั้นจะแบ่งระดับชั้นของเทคโนโลยีออกเป็นสี่ระดับ นั่นคือ ชั้นกายภาพ (Physical Layer) ตัวควบคุมการเข้าถึงสื่อ (Media Access Controller) ระบบปฏิบัติการ (Operating System) และแอพพลิเคชั่น (Application) โดยชั้นกายภาพคือ ส่วนของฮาร์ดแวร์ที่แบ่งมาตรฐานออกเป็น a, b และ g โดยหากเลือกต่างชนิดกันก็ไม่สามารถสื่อสารกันได้รู้เรื่อง เพราะเป็นความถี่ที่ต่างกันจะติดต่อรับส่งข้อมูลกันไม่ได้ โดยปัจจุบันในส่วนของชั้นกายภาพนี้มีอยู่ทั้งสิ้น สี่ มาตรฐาน คือ a, b, g และอินฟราเรด (IR)

ส่วนต่อมาคือ ตัวควบคุมการเข้าถึงสื่อเป็นส่วนของการทำงานเกี่ยวกับระบบรักษาความปลอดภัยของเครือข่าย การจัดการโครงสร้างหรือรูปแบบของข้อมูล การแปลงข้อมูล ซึ่งมาตรฐาน IEEE 802.11 นั้นใช้มาตรฐานตัวควบคุมการเข้าถึงสื่อเดียวกันทั้งหมด คือ ได้กำหนดทางเลือกของการเข้ารหัสไว้ก่อนทำการส่งข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสแบบ 40 บิตซึ่งรู้จักกันในชื่อ RC4 นอกจากนั้นผู้ผลิตบางรายก็ยังเสนอให้มีการตรวจสอบก่อนใช้งานโครงข่ายด้วยวิธีการที่เรียกว่า Wired Equivalent Privacy (WEP) shared-key อันเดียวกันจะใช้ในการตรวจสอบก่อนที่จะทำการเข้ารหัสหรือถอดรหัสข้อมูล ซึ่งจะมีเพียงผู้ใช้งานที่ถูกต้องเท่านั้นจึงจะมี shared-key ที่ถูกต้องในการถอดรหัสข้อมูลออกมาได้ นอกจากเรื่องความน่าเชื่อถือกับเรื่องความปลอดภัยแล้ว มาตรฐาน 802.11 ในส่วนตัวควบคุมการเข้าถึงสื่อยังมีโหมดสนับสนุนการจัดการพลังงานอีก สอง รูปแบบ คือ Continuous Aware Mode และ Power Saving Polling Mode โดยโหมดแรกสัญญาณวิทยุจะส่งอยู่ตลอดและทำให้สูญเสียพลังงาน ในขณะที่โหมดต่อมาสัญญาณวิทยุจะอยู่ในภาวะนอนหลับหรือ sleep เพื่อที่จะถนอมพลังงาน

ส่วนของระบบปฏิบัติการและแอพพลิเคชั่นคือ ระบบปฏิบัติการภายในเครื่องและแอพพลิเคชั่นควบคุมการสื่อสาร ซึ่งใช้งานเหมือนกับเครือข่ายแบบมีสายในปัจจุบัน

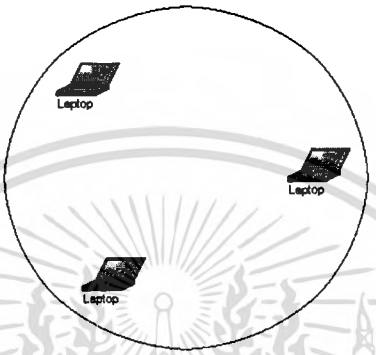
2.1.2 รูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สาย

รูปแบบการเชื่อมต่อของมาตรฐาน 802.11 สามารถทำได้สองรูปแบบ คือ

- การเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราว (Basic Service Set)
- การเชื่อมต่อกับระบบเครือข่ายเดิมโดยผ่านจุดเชื่อมต่อ (Extended Service Set)

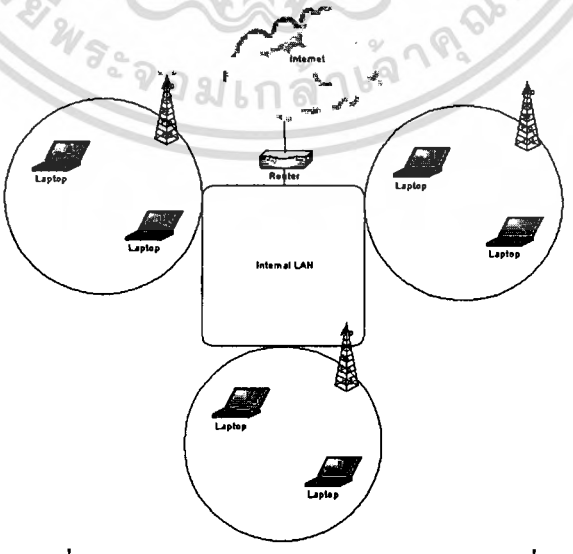
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราวหรือที่เรียกว่าการเชื่อมต่อแบบ Ad hoc นั้น สามารถทำได้โดยการสร้างวงเครือข่ายโดยวิธีการติดต่อกันโดยตรงระหว่างเครื่องที่ต้องการสื่อสารกันในวงเครือข่ายชั่วคราวนั้นๆ เหมาะสำหรับการนำไปใช้ในการสร้างระบบเครือข่ายแบบชั่วคราว มีรูปแบบในการเชื่อมต่อแสดงได้ดังรูปที่ 2.5



รูปที่ 2.1 แสดงการเชื่อมต่อเป็นระบบเครือข่ายแบบชั่วคราว (Basic Service Set)

การเชื่อมต่อกับระบบเครือข่ายเดิมนั้นจะต้องใช้อุปกรณ์จุดเชื่อมต่อ (Access Point) เพื่อทำหน้าที่เป็นตัวเชื่อมต่อระบบส่วนที่เป็นการเชื่อมต่อแบบไร้สายเข้ากับเครือข่ายเดิม โดยจุดที่เชื่อมต่อนี้จะเป็นเสมือนช่องทางที่ใช้ในการสื่อสารระหว่างส่วนที่เป็นการสื่อสารแบบไร้สายกับส่วนที่เป็นการสื่อสารโดยใช้สาย มีรูปแบบการเชื่อมต่อดังแสดงในรูปที่ 2.6



รูปที่ 2.2 แสดงการเชื่อมต่อกับระบบเครือข่ายเดิมโดยผ่านจุดเชื่อมต่อ (Extended Service Set)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบเครือข่ายไร้สาย เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดเล็ก ที่ประกอบไปด้วยอุปกรณ์ไม่มากนัก และมักจำกัดอยู่ในอาคารหลังเดียวหรืออาคารในบริเวณเดียวกัน การใช้งานที่น่าสนใจที่สุดของเครือข่ายไร้สายก็คือ ความสะดวกสบายที่ไม่ต้องติดอยู่กับที่ ผู้ใช้สามารถเคลื่อนที่ไปมาได้โดยที่ยังสื่อสารอยู่ในระบบ

2.2 ระบบความปลอดภัยสำหรับระบบเครือข่ายไร้สาย

ระบบความปลอดภัยสำหรับระบบเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 นั้น มีอยู่ด้วยกันหลายส่วน ที่จะทำงานร่วมกัน โดยแบ่งออกได้ดังต่อไปนี้ คือ

- Extended Service Set ID (ESSID)
- Access Lists
- Authentication and Association
- Wired Equivalent Privacy (WEP)

2.2.1 Extended Service Set ID (ESSID)

หลักการทำงานของ ESSID คือ การให้หมายเลขประจำตัวสำหรับทุกจุดเชื่อมต่อ (Access Point) และไคลเอนต์ทั้งหมดที่อยู่ในระบบเครือข่ายไร้สาย โดยการกำหนดในลักษณะนี้ จะเหมือนกับการกำหนดชื่อของระบบเครือข่ายนั่นเอง แต่โดยทั่วไปแล้วผู้ผลิตอุปกรณ์ระบบเครือข่ายแบบไร้สายจะกำหนดค่ามาตรฐานไว้ ดังนั้นเมื่อนำมาใช้งาน จึงควรเปลี่ยนค่าของ ESSID โดยทันที

2.2.2 Access Lists

การใช้งาน Access Lists นี้จะกระทำที่จุดเชื่อมต่อ (Access Point) โดยที่จะกำหนดรายการของค่า MAC address ของไคลเอนต์แบบไร้สาย ที่ได้รับอนุญาตให้สามารถเชื่อมต่อกับระบบได้ ถ้า MAC address ของไคลเอนต์ใดที่ไม่อยู่ในรายการของจุดเชื่อมต่อ ก็จะไม่สามารถเชื่อมต่อเข้ากับระบบเครือข่ายได้

2.2.3 Authentication and Association

กระบวนการในการรับรองสิทธิ์และการเข้าใช้งานในระบบเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 นี้จะแบ่งออกเป็น สอง รูปแบบ คือ

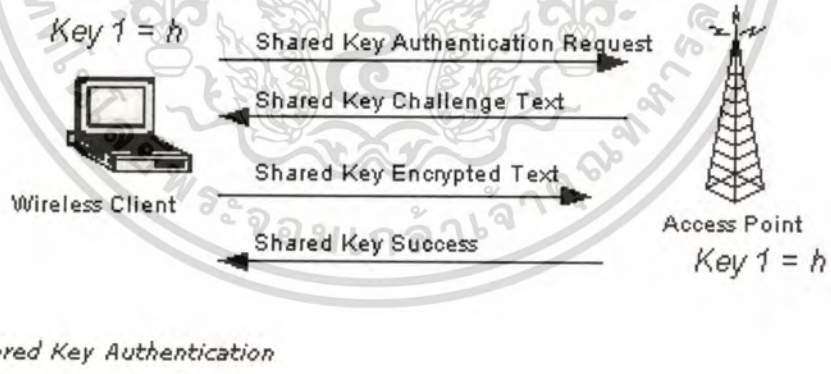
- ระบบเปิด (Open System Authentication)
- กุญแจร่วม (Shared Key Authentication)

การใช้กระบวนการรับรองสิทธิ์แบบระบบเปิดจะเป็นกระบวนการพื้นฐานที่สุด กล่าวคือ จะไม่มีการใช้กุญแจในขั้นตอนการรับรองสิทธิ์ และมีขั้นตอนทั้งหมดในการแสดงสิทธิ์เพียง สองขั้นตอนเท่านั้น ดังแสดงในรูปที่ 2.13

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 2.3 แสดงระบบเปิด (Open System Authentication)

การใช้กระบวนการรับรองสิทธิ์แบบใช้กุญแจร่วมนี้ จะต้องมีการใช้งานกุญแจที่ใช้งานร่วมกันระหว่างไคลเอนต์และจุดเชื่อมต่อโดยกุญแจดังกล่าวนี้จะใช้เป็นเครื่องมือในการเข้าและถอดรหัสข้อความที่ใช้แสดงตัวของไคลเอนต์ ดังนั้นจะมีเพียงไคลเอนต์ที่มีกุญแจที่ถูกต้องเท่านั้น ที่จะสามารถทำการถอดรหัสได้ โดยขั้นตอนดังกล่าวจะอยู่ในช่วงขั้นตอนที่ สอง และ สาม ของกระบวนการในการรับรองสิทธิ์ ดังแสดงในรูปที่ 2.14



รูปที่ 2.4 แสดงระบบกุญแจร่วม (Shared Key Authentication)

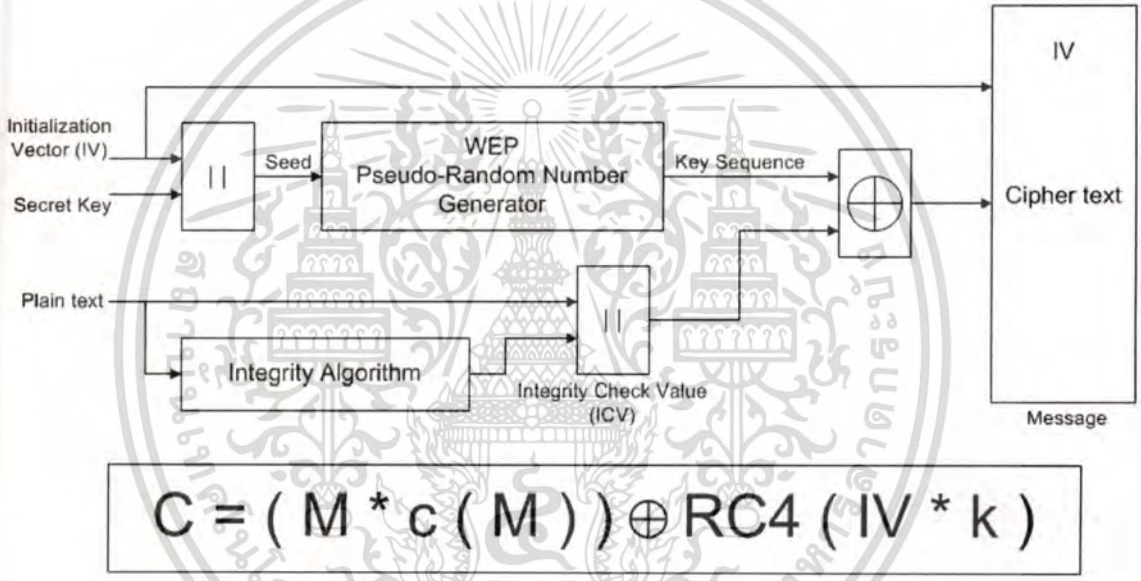
กระบวนการในการรับรองสิทธิ์แบบใช้กุญแจร่วมนี้ จะใช้ Wired Equivalent Privacy (WEP) ซึ่งถูกกำหนดไว้ในมาตรฐานการเชื่อมต่อระบบเครือข่ายไร้สาย IEEE 802.11 โดยใช้เป็นเครื่องมือในการเข้าและถอดรหัสของข้อมูลที่สื่อสารกันผ่านระบบเครือข่ายไร้สาย การใช้งานระบบกุญแจร่วมนี้ จะเป็นตัวเลือกให้ใช้งาน ไม่ได้ถูกกำหนดมาเป็นค่ามาตรฐานในการเชื่อมต่อ ดังนั้น ถ้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต้องการที่จะใช้งานระบบแบบกุญแจร่วมแล้ว จะต้องทำการกำหนดตัวเลือกในการใช้งานให้ถูกต้องด้วย

2.2.4 Wired Equivalent Privacy (WEP)

กลไกการทำงานของโพรโตคอล WEP นี้จะเป็นกระบวนการที่ใช้ในการเข้าและถอดรหัสข้อมูลที่ผู้รับและผู้ส่งสื่อสารกัน เพื่อทำการเพิ่มความปลอดภัยให้กับข้อมูล โดยที่มีจุดประสงค์ให้มีลักษณะและประสิทธิภาพการทำงานได้เช่นเดียวกันกับที่ใช้ในระบบเครือข่ายแบบใช้สาย ซึ่งจะมีการทำงาน ดังแสดงในรูปที่ 2.15



รูปที่ 2.5 แสดงการทำงานของ Wired Equivalent Privacy (WEP)

ขั้นตอนการทำงานของ WEP ที่มาตรฐาน IEEE 802.11 ใช้นั้นจะใช้กลไกการเข้าและถอดรหัสแบบอาร์ซีโฟร์ โดยที่อาร์ซีโพร์นี้จะมีส่วนประกอบอยู่ด้วยกัน สอง ส่วนคือ

- ส่วนที่ใช้ในการกำหนดกุญแจที่จะใช้งาน (Key Scheduling Algorithm)
- ส่วนที่ใช้ในการสร้างผลลัพธ์ (Output Generator)

ส่วนการกำหนดกุญแจขึ้นมาใช้งานนั้น WEP ที่มีใช้อยู่ในปัจจุบันจะมีรูปแบบการทำงานในส่วนนี้อยู่สองรูปแบบคือ การใช้ 64-bit packet key (40-bit secret key + 24-bit IV) และ 128-bit packet key (104-bit secret key + 24-bit IV) ซึ่งถ้าจำนวนบิตที่ใช้ในการสร้างกุญแจยิ่งมากก็จะทำให้ระบบมีความปลอดภัยมากขึ้นด้วย ส่วนการทำงานในส่วนของการสร้างผลลัพธ์นั้นจะใช้วิธีการเรียงสับเปลี่ยน (Permutation) ซึ่งจะได้ผลลัพธ์เป็นลำดับของข้อมูลที่ถูกเรียงสับเปลี่ยนแล้ว จากรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ที่ 2.15 ข้างต้นจะอธิบายขั้นตอนการทำงานของ WEP ได้ดังนี้คือ นำเอาข้อมูลที่ต้องการส่งมาทำการเข้ากระบวนการเข้ารหัสเพื่อตรวจสอบความถูกต้องของข้อมูลระหว่างผู้รับกับผู้ส่ง (Integrity Check Value) จะได้ผลลัพธ์เป็น M * c(M) จากสมการข้างต้น M คือข้อมูลที่ต้องการส่ง นำมาต่อกับ c(M) ซึ่งคือการสร้าง ICV เพื่อทำการตรวจสอบ ทำการสร้างลำดับของกุญแจ (Key Sequence) จากสมการข้างต้นโดยการใช้กุญแจ k และค่า IV (Initialization vector) มาเชื่อมต่อกันและทำการเรียงสับเปลี่ยนโดยใช้วิธีการของอาร์ซีโฟร์และมีความยาวของข้อมูลเท่ากับส่วนของ M * c (M) โดยที่ค่า IV ที่ใช้จะเป็นค่าที่ได้จากการสุ่มและไม่ซ้ำกันในการส่งแต่ละครั้ง ทำการเข้ารหัสข้อมูลโดยการนำข้อมูลที่ได้ทั้งสองส่วนมาทำการ XOR กัน แล้วส่งไปยังผู้รับ เมื่อผู้รับได้รับข้อมูลแล้วจะทำการถอดรหัสโดยใช้กุญแจร่วมและจะสามารถทำการตรวจสอบผู้ส่งได้จากค่า ICV ที่ได้เพิ่มไปในตอนต้นด้วย

2.2.5 ระบบการพิสูจน์ตัวจริงผ่านเว็บ (Web Authentication)

ระบบการพิสูจน์ตัวจริงผ่านเว็บก็เป็นอีกวิธีหนึ่งที่ช่วยสร้างความปลอดภัยให้กับเครือข่ายไร้สาย โดยส่วนใหญ่แล้วระบบนี้จะถูกติดตั้งในส่วนที่เป็นตัวเกตท์เวย์ในการเชื่อมต่อไปยังเครือข่ายอินเตอร์เน็ท โดยผู้ใช้ที่ต้องการใช้บริการจะต้องทำการลงทะเบียนในระบบเสียก่อน ซึ่งข้อมูลของผู้ใช้จะถูกเก็บอยู่ในระบบฐานข้อมูล ซึ่งวิธีเป็นวิธีที่สามารถจะเก็บข้อมูลการใช้งานของผู้ใช้ได้จึงเหมาะกับระบบที่ต้องการคิดค่าใช้จ่ายกับผู้ใช้งาน ในปัจจุบันมีซอฟท์แวร์ที่พัฒนาเป็นระบบการพิสูจน์ตัวจริงผ่านเว็บมากมาย มีทั้งในรูปแบบที่เป็นระบบเปิด (Open System) ที่ผู้พัฒนาสามารถที่จะเข้าไปทำการแก้ไข เพิ่มเติมการทำงานได้ ซึ่งส่วนใหญ่ระบบพวกนี้จะมีการทำงานอยู่บนแพล็ตฟอร์ม Linux และระบบปิด ที่ต้องมีการเสียค่าใช้จ่ายโดยจะมาในรูปแบบที่เป็นอุปกรณ์ (Appliance Device)

2.2.6 ระบบเครือข่าย Virtual Private Network (VPN)

ในการสร้างระบบรักษาความปลอดภัยให้กับเครือข่ายไร้สายนั้น เท่าที่กล่าวมาข้างต้นความปลอดภัยในการรับ-ส่งข้อมูลก็เป็นสิ่งจำเป็น การเข้ารหัสด้วยวิธี WEP ไม่มีความปลอดภัยแล้ว เนื่องจากในปัจจุบันได้มีผู้พัฒนาโปรแกรมสำหรับทำการถอดรหัสข้อมูลที่เข้ารหัสด้วยวิธี WEP ได้แล้ว เพราะฉะนั้นจึงมีการนำระบบเครือข่าย VPN เข้ามาใช้ในการรับ-ส่งข้อมูลในเครือข่ายไร้สาย นอกจากนี้ระบบเครือข่าย VPN ยังช่วยป้องกันมิให้ผู้ที่ไม่มีสิทธิ์ในการใช้งานเข้ามาใช้ในระบบได้ โดยการใช้ IPSec (Internet Protocol Security) ซึ่งเป็นโปรโตคอลที่ถูกกำหนดโดย IEEE โดยใช้การเข้ารหัสข้อมูลแบบ DES และ 3DES และใช้อัลกอริทึ่มสำหรับคีย์แฮช เช่น HMAC,

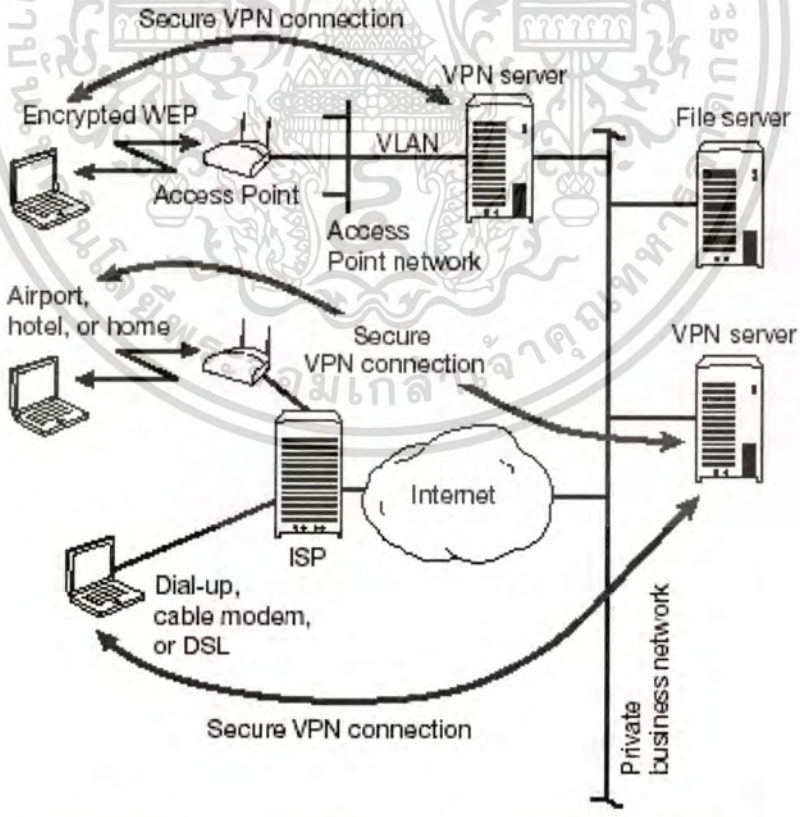
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

MD5 หรือ SHA สำหรับทำการพิสูจน์ตัวจริง และยังมีการใช้งาน Digital Signature เพื่อทำการตรวจสอบคีย์สาธารณะให้ถูกต้องด้วย ระบบ VPN รองรับวิธีการพิสูจน์ตัวจริงหลายรูปแบบเช่น RADIUS, SecureID และDigital Certificates โดยวิธีเหล่านี้เป็นวิธีที่นิยมใช้ในปัจจุบัน

โปรโตคอล IPSec จะมีรูปแบบอยู่ 2 ส่วนหลัก คือ

- Authentication Header (AH) รูปแบบนี้ใช้สำหรับการพิสูจน์ตัวจริง โดยจะมีการรวมข้อมูลของการพิสูจน์ตัวจริงเข้าไปยัง Header ในส่วนของ IP Diagram แต่ไม่ได้ทำการรวมข้อมูลของแพ็คเก็ท
- Encapsulation Security Payload (ESP) รูปแบบนี้จะมีการรวมข้อมูลของการพิสูจน์ตัวจริงและข้อมูลของแพ็คเก็ททั้งหมดไว้ด้วยกัน โดยจะมีการเข้ารหัสข้อมูลเหล่านี้ ซึ่งมี 2 โหมด คือ Tunnel และ Transport

นอกจากนี้ในโปรโตคอล IPSec ยังมีส่วนที่สำคัญอีกส่วนคือ Internet Key Exchange (IKE) ซึ่งเป็นส่วนที่ใช้ในการจัดการเรื่องของคีย์ โดยจะมีการใช้อัลกอริทึ่ม Diffie-Hellman ในการแลกเปลี่ยนคีย์ที่ใช้ในการเข้ารหัส ไม่ว่าจะเป็นรูปแบบของ AH และ ESP



รูปที่ 2.6 ตัวอย่างการใช้งานระบบ VPN บนเครือข่ายไร้สาย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3 ระบบความปลอดภัย OpenVPN

OpenVPN เป็นระบบ VPN ที่ใช้ในการเข้า-ถอดรหัสข้อมูล โดยมีโหมดในการพิสูจน์ตัวจริงอยู่ 2 โหมดคือ

- Static key จะมีการใช้คีย์ที่เป็นแบบ Pre-shared
- TLS จะใช้การทำงานของ SSL/TLS รวมกับ Certificate ในการพิสูจน์ตัวจริงและการแลกเปลี่ยนคีย์

โดยในรูปแบบของ Static key จะมีการสร้างคีย์ขึ้นมาหรือที่เรียกว่า Static key เพื่อใช้งานระหว่างเครื่องที่ต้องการสร้างการเชื่อมต่อในรูปแบบ VPN โดยภายใน Static key จะถูกใช้ในการทำงานที่ไม่ขึ้นต่อกันอยู่ 4 ส่วนคือ HMAC send, HMAC receive, encrypt และ decrypt โดยค่าดีฟอลต์ของ Static key จะมี HMAC key และ encrypt/decrypt ที่เหมือนกันระหว่างเครื่องที่ต้องการสร้างการเชื่อมต่อ

ส่วนรูปแบบ SSL/TLS นั้นมีการทำงานคือ SSL จะมีถูกสร้างขึ้นมาเพื่อใช้ในการพิสูจน์ตัวจริงแบบสองทาง (Bidirectional authentication) โดยถ้ามีการพิสูจน์ตัวจริงผ่าน encrypt/decrypt และ HMAC key จะมีการสุ่มสร้างขึ้นมา ในระหว่างที่ SSL/TLS ทำการเปลี่ยนคีย์ (rekey) จะใช้เวลาที่นาน เพราะรูปแบบ SSL/TLS นั้น ถูกออกแบบให้ทำงานบน Reliable Transport ซึ่งอยู่บนสุดของ UDP

สำหรับการเข้ารหัสข้อมูลนั้น แพ็คเก็ทที่ถูกเข้ารหัสเรียบร้อยแล้วจะประกอบด้วย 3 ส่วน คือ HMAC, Explicit IV และข้อมูลที่ถูกปิดผนึก (Encrypted Envelope) ซึ่งภายในข้อมูลที่ถูกปิดผนึกจะมีข้อมูล 2 ส่วนคือคือ Sequence number ที่มีขนาด 64 บิต และข้อมูลของแพ็คเก็ท (Payload data)

ฟังก์ชั่นของ HMAC, การเข้ารหัส และถอดรหัส จะถูกกำหนดโดยโปรแกรม OpenSSL รวมทั้งการเลือก arbitrary cipher, ขนาดของคีย์ และ message digest ของ HMAC โดยค่าดีฟอลต์ของ cipher คือ Blowfilsh และ SHA1 เป็นค่าดีฟอลต์ของ message digest

2.4 สิ่งที่ต้องคำนึงถึงในการสร้างระบบรักษาความปลอดภัยในเครือข่ายไร้สาย

- Risk ระดับความเสี่ยงในการที่จะถูกโจมตีเป็นปัจจัยสำคัญในการที่จะเลือกนำระดับของเทคโนโลยีทางด้านการรักษาความปลอดภัยในเครือข่ายไร้สายมาใช้งาน
- Technology ในปัจจุบันการพัฒนาระบบรักษาความปลอดภัยบนเครือข่ายไร้สายนั้นมีหลากหลายรูปแบบ เพราะฉะนั้นผู้สร้างจึงควรที่จะมีการศึกษาเทคโนโลยีเหล่านั้นด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Network Organization เรื่องของรูปแบบระบบเครือข่ายไร้สายภายในองค์กรเป็นสิ่งที่จะเลือกลักษณะของเทคโนโลยีการรักษาความปลอดภัยที่จะนำมาใช้งานได้
- Cost ต้นทุนของระบบก็เป็นปัจจัยหนึ่งที่จะทำให้การสร้างระบบความปลอดภัยมีประสิทธิภาพหรือไม่มี โดยจะสังเกตได้จากบริษัทขนาดใหญ่ที่มีการลงทุนในเรื่องของระบบความปลอดภัยสูง ก็จะได้ระบบที่มีประสิทธิภาพทางด้านความปลอดภัยสูงเช่นกัน
- Scalability เรื่องของการรองรับการปรับขนาดของเครือข่ายไร้สายเป็นสิ่งที่ยากในการที่จะกำหนดได้อย่างชัดเจน แต่ก็เป็นปัจจัยที่มีผลในการที่จะเลือกนำเทคโนโลยีในการรักษาความปลอดภัยมาใช้เช่นกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3
การวิเคราะห์และออกแบบระบบ

3.1 ปัญหาด้านความปลอดภัย

ปัญหาทางด้านความปลอดภัยที่เกิดขึ้นก็คือระบบไวร์เลสแลนนั้นจะใช้ SSID (Service Set Identifier) ความยาวไม่เกิน 32 ตัวอักษร ในการกำหนดเป็นชื่อของ Network Name ที่เป็นไวร์เลสแลนดังนั้นเครื่องลูกข่ายไวร์เลสแลนทุกตัวที่ต้องการต่อเชื่อมกับไวร์เลสแลนต้องอ้างถึง SSID ค่าเดียวกันทั้งหมด ค่า SSID สามารถถูกโปรแกรม Sniffer แบบไวร์เลสแลนดักจับได้ง่ายเพราะค่า SSID นั้นเป็น Plain Text ที่ไม่ได้เข้ารหัสแต่อย่างใด จริงๆแล้วไวร์เลสแลนนั้นมีโปรโตคอลในการเข้ารหัสข้อมูลที่เรียกว่า WEP (Wired Equivalent Privacy) แต่พบว่ามีแค่เพียง 25 เปอร์เซ็นต์ เท่านั้นที่ใช้ WEP นอกนั้นก็ใช้แบบ Plain Text ธรรมดาแถมยังใช้ค่า Default SSID ที่มากับอุปกรณ์ไวร์เลสแอคเซสพอยท์ต่างหาก เช่นค่า Default SSID ของ CISCO Aironet ไวร์เลสแอคเซสพอยท์ คือ Tsunami ทำให้แฮกเกอร์สามารถสแกนพบได้โดยง่าย

ถึงแม้ว่าเราจะใช้ WEP ในการเข้ารหัสแต่ WEP มีการเข้ารหัสบนพื้นฐาน RC4 Algorithm การเข้ารหัสแบบ RC4 นั้นมีช่องโหว่ (Vulnerability) ที่แฮกเกอร์สามารถเจาะได้ (WEP ใช้ 40 Bit Secret Key ในการเข้ารหัส) โดยใช้เทคนิคที่เรียกว่า Known Plain Text Attack หลักการก็คือ แฮกเกอร์จะใช้ Sniffer ดักจับ Packet ข้อมูลที่ถูกเข้ารหัสโดย WEP จำนวนหนึ่งซึ่งมากพอที่จะ Crack WEP ได้ ตัวอย่างโปรแกรม Sniffer ที่ใช้ในการ Crack WEP ได้แก่ AirSnort และ Wepcrack ซึ่งสามารถที่จะถอดรหัส WEP ได้

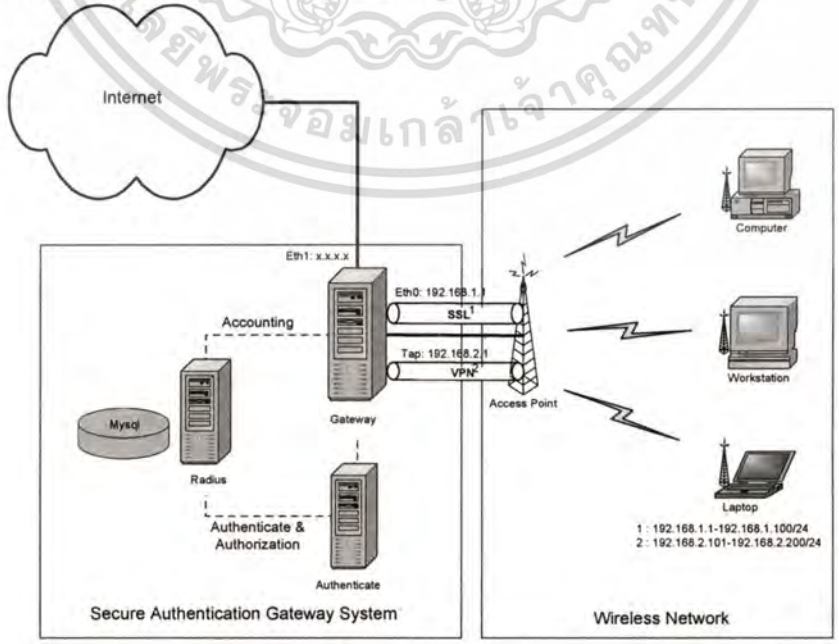
กลยุทธ์ของแฮกเกอร์ที่จะแอบใช้งานระบบไวร์เลสแลนของเราก็คือ Wardriving และ Warchalking ล่าสุดมีกลุ่มของแฮกเกอร์ ในเมือง Pittsburgh ใช้เทคนิคนี้ในการเจาะระบบไวร์เลสแลนกล่าวคือ แฮกเกอร์จะขับรถไปในเมืองผ่านบริเวณที่มีการใช้งานไวร์เลสแลน แล้วแฮกเกอร์จะใช้ Notebook ที่ต่อกับ การ์ดไวร์เลสแลน ที่ Support IEEE 802.11b จากนั้นก็จะใช้โปรแกรมชื่อ Netstrumbler ตรวจหาระบบ ไวร์เลสแลน ที่แฮกเกอร์ ได้ขับรถผ่านเข้าไปใกล้รัศมีการทำงานของแอคเซสพอยท์ จากนั้นก็จะ Mark ตำแหน่งของจุดที่มี WLAN เปิดใช้งานอยู่เรียกว่า Warchalking ในเมือง Pittsburgh นั้น กลุ่มของแฮกเกอร์ได้สร้างแผนที่ของเมืองแสดงตำแหน่งของ ไวร์เลสแลน แล้วแฮกเกอร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ก็สามารถเข้ามาในระบบแลน ของเราที่ แอคเซสพอยท์ เชื่อมต่ออยู่ได้โดยง่ายโดยเฉพาะเครือข่ายที่ไม่ได้เปลี่ยนค่า Default SSID หรือ ไม่ได้เข้ารหัสด้วย WEP ถึงเข้ารหัสด้วย WEP ก็ยังถูกถอดรหัสได้อยู่ดี ดังนั้นจะเห็นว่าไวร์เลสแลนนั้นมีจุดอ่อนด้าน Security อยู่พอสมควร

3.2 การแก้ปัญหาด้านความปลอดภัย

ในปัจจุบันก็ได้มีการแก้ปัญหาด้านความปลอดภัยของไวร์เลสแลนมากมาย ผู้ผลิตอุปกรณ์ทางด้านความปลอดภัยของระบบเครือข่ายหลายรายได้หันมาให้ความสนใจในการผลิตอุปกรณ์ที่ช่วยสร้างความปลอดภัยให้กับเครือข่ายไวร์เลสแลน แต่อุปกรณ์เหล่านี้ ก็มีราคาค่อนข้างสูงซึ่งไม่เหมาะกับองค์กรขนาดกลางและขนาดเล็กที่มีจำนวนการใช้งานของระบบไม่มาก ดังนั้นระบบนี้จึงเกิดขึ้นเพื่อช่วยสร้างความปลอดภัยให้กับเครือข่ายไวร์เลสแลน โดยระบบนี้ประกอบไปด้วยการนำระบบที่ช่วยสร้างความปลอดภัยให้กับระบบเครือข่าย 2 ระบบคือ ระบบพิสูจน์ตัวจริง (Authentication Gateway System) และระบบเครือข่าย Virtual Private Network (VPN network System) โดยระบบแรกจะนำมาช่วยในการป้องกันผู้ที่ไม่มีสิทธิ์ใช้งาน ไม่ให้เข้ามาใช้งานภายในระบบ และระบบที่สองคือระบบเครือข่าย VPN จะนำมาช่วยในการสร้างความปลอดภัยในการรับ-ส่งข้อมูลหลังจากที่มีการพิสูจน์ตัวจริงผ่านแล้ว โดยการเชื่อมต่อของระบบเครือข่าย VPN จะใช้งานผ่านระบบ VPN ประเภท Secure Sockets Layer (SSL) VPN ซึ่งระบบที่จะดำเนินการพัฒนานั้น มีชื่อว่าระบบรักษาความปลอดภัยความปลอดภัยในการพิสูจน์ตัวจริง (Secure Authentication Gateway System) โดยมีการทำงานตามรูปที่ 3.1



รูปที่ 3.1 แสดงการทำงานของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำหรับการทำงานของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงที่จะดำเนินการพัฒนานั้น จะแบ่งออกเป็น 2 ส่วนใหญ่คือ ส่วนของระบบที่สร้างความปลอดภัย และส่วนของการพัฒนาระบบเพื่อตรวจสอบการใช้งานของผู้ใช้และระบบการควบคุมดูแลสำหรับผู้ดูแลระบบ โดยส่วนของระบบที่สร้างความปลอดภัยที่ได้กล่าวไปข้างต้นนั้น จะใช้ระบบการพิสูจน์ตัวจริง และระบบเครือข่าย VPN โดยในส่วนของระบบพิสูจน์ตัวจริงจะใช้เครื่องมือที่เรียกว่า NoCatAuth โดยในส่วนนี้จะมีการสร้างความปลอดภัยโดยการนำ PGP และ SSL มาช่วยในการทำงาน ทำให้การรับ-ส่งข้อมูลในการพิสูจน์ตัวจริง (Authentication) มีความปลอดภัยมากขึ้น

ในการทำงานของตัวระบบ NoCatAuth จะเป็นตัวกลางในการควบคุมการทำงานของระบบทั้งหมด โดยภายในระบบ NoCatAuth จะประกอบด้วยระบบย่อย 2 ส่วนคือระบบพิสูจน์ตัวจริงและระบบเกตเวย์ โดยการทำงานของระบบเกตเวย์จะมีหน้าที่ในการควบคุมการเข้าออกของข้อมูลโดยอาศัยโปรแกรมต่าง ๆ เช่น ใช้โปรแกรม iptables เข้ามาทำหน้าที่เป็นไฟร์วอลล์ในการกำหนดการเข้าออกของผู้ใช้และทำหน้าที่เป็น Network Translation Address (NAT) สำหรับเครื่องผู้ใช้ที่จะทำการเชื่อมต่อไปยังเครือข่ายอินเตอร์เน็ท โดยภายในตัวระบบ NoCatAuth จะมีการนำ PGP มาเข้ารหัสระหว่าง ระบบการพิสูจน์ตัวจริง กับระบบ เกตเวย์ เพื่อทำการตรวจสอบทั้งสองระบบ ว่าเป็นตัวจริงทั้งสองระบบ เพื่อป้องการปลอมระบบขึ้นมาในกรณีที่มีการแยกระบบการพิสูจน์ตัวจริงกับระบบเกตเวย์ออกจากกัน โดยมีการเข้ารหัส 1024 บิต ทั้งสองฝ่ายจะต้องมีคีย์ส่วนตัว ตัวเดียวกันในการถอดรหัส และการนำ SSL มาเพื่อทำหน้าที่เข้ารหัสระหว่าง เวบเซิร์ฟเวอร์กับ เวบบราวเซอร์ โดยทำการเข้ารหัส 128 บิต เพื่อป้องการการดักจับข้อมูลรหัสผ่าน ในระหว่างการดำเนินการพิสูจน์ตัวจริง (Authentication)

การทำงานในส่วนของระบบเครือข่าย Virtual Private Network (VPN) จะใช้เครื่องมือที่ชื่อว่า OpenVPN ซึ่งมีการทำงานในรูปแบบที่เป็น Secure Sockets Layer (SSL) VPN โดยจะช่วยสร้างความปลอดภัยในการรับ-ส่งข้อมูลในการเชื่อมต่อออกสู่ระบบอินเตอร์เน็ทหลังการพิสูจน์ตัวจริงผ่านแล้ว ซึ่งการทำงานในส่วนนี้ผู้ใช้จะต้องทำการติดตั้งโปรแกรมด้วย

ส่วนที่สองคือส่วนของการพัฒนาระบบตรวจสอบการใช้งานของผู้ใช้และระบบควบคุมดูแลสำหรับผู้ดูแลระบบ โดยในส่วนนี้จะมีหลักการทำงานคือเริ่มคือ ผู้ใช้งานจะต้องทำการล็อกอินเข้าสู่ระบบก่อน โดยในส่วนของระบบควบคุมดูแลสำหรับผู้ดูแลจะมีการออกแบบการทำงานเพิ่มโดยการเช็คหมายเลขไอพีของเครื่องที่จะเข้าสู่ระบบด้วย โดยเมื่อหลังจากทำการล็อกอินผ่านแล้ว ก็จะมีเมนูต่าง ๆ ให้ผู้ใช้หรือผู้ดูแลระบบสามารถที่จะเลือกทำได้ โดยแบ่งเป็นระบบตรวจสอบการใช้งานของผู้ใช้จะสามารถแก้ไขข้อมูลส่วนตัวของตัวเองได้ การดูประวัติการใช้งานที่ผ่านมา การเปลี่ยนแปลงรหัสผ่านในการเข้าระบบและการกรอกหมายเลขรหัสการใช้งาน ซึ่งจะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ได้รับจากผู้ดูแลระบบ และระบบควบคุมดูแลสำหรับผู้ดูแลระบบก็จะมีการทำงานหลัก ๆ ให้เลือกทำคือระบบที่หนึ่งระบบจัดการข้อมูลของผู้ใช้ โดยสามารถที่จะตรวจสอบข้อมูลส่วนตัวและลบข้อมูลส่วนตัวได้ ตรวจสอบประวัติการใช้งานของผู้ใช้ได้ ตรวจสอบผู้ใช้งานที่มีการออนไลท์อยู่ในระบบ รวมทั้งการสร้างหมายเลขรหัสการเข้าใช้งานของผู้ใช้ได้ ระบบที่สองระบบคำนวณการใช้งานของผู้ใช้ ในระบบนี้จะทำการกำหนดอัตราราคาในการใช้งานของผู้ใช้ และนำมาคำนวณการใช้งานของผู้ใช้ออกมาในรูปแบบที่ค่าใช้จ่ายในการใช้งานได้ ระบบที่สามคือระบบจัดการข้อมูลในการเข้าสู่ระบบดูแลนี้ โดยภายในระบบนี้จะมีการที่ให้ผู้ดูแลสามารถที่จะทำการเปลี่ยนรหัสผ่านได้ รวมถึงการกำหนดหมายเลขไอพีในการเข้าสู่ระบบควบคุมดูแลสำหรับผู้ดูแลด้วย และระบบสุดท้ายคือระบบจัดการคอนฟีกกรูเรชั่น ภายในระบบนี้ผู้ดูแลสามารถที่จะเลือกกำหนดหมายเลขไอพีและหมายเลขดีเอ็นเอส (DNS Server) ในส่วนที่ระบบทำการเชื่อมต่อสู่ระบบภายนอกหรือระบบอินเตอร์เน็ทได้

นอกจากระบบที่มีการพัฒนาขึ้นใหม่ในส่วนที่เป็นระบบตรวจสอบการใช้งานและระบบควบคุมดูแลสำหรับผู้ดูแลแล้ว ยังมีการพัฒนาระบบในส่วนย่อย ๆ อีก คือส่วนของการลงทะเบียนของผู้ใช้งาน ส่วนของการดาวน์โหลดโปรแกรม OpenVPN เพื่อให้ผู้ใช้ติดตั้งอีกด้วย

3.3 ภาพรวมการทำงานของระบบ

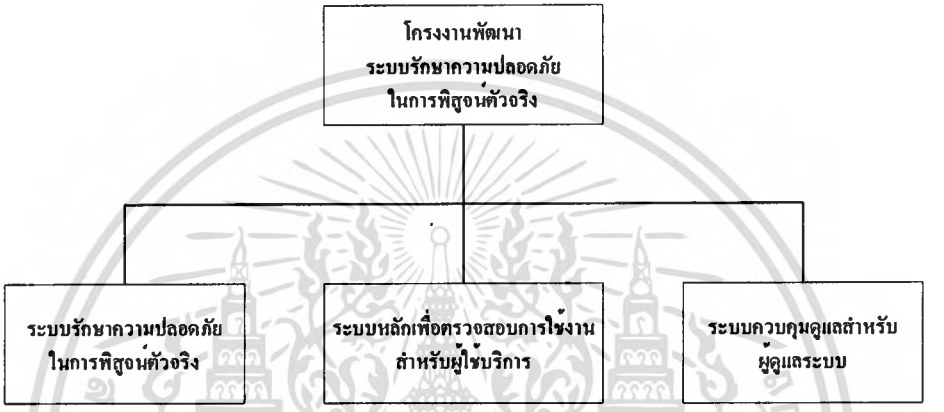
โครงงานที่ทำการพัฒนานี้เป็นระบบที่ทำหน้าที่ในการรักษาความปลอดภัยในการใช้งานบนเครือข่ายไร้สาย เพราะฉะนั้นการทำงานของระบบจะมีส่วนที่เป็นระบบที่ใช้ในการรักษาความปลอดภัยในการใช้งานบนเครือข่ายไร้สาย และในการออกแบบโครงงานนี้ยังมีการออกแบบให้คำนวณค่าใช้จ่ายในการใช้งานของผู้ใช้ได้ จึงจำเป็นต้องมีระบบที่ใช้ในการตรวจสอบการใช้งานของผู้ใช้ โดยระบบการให้บริการทั้งหมดจะอยู่ภายใต้การดูแลของผู้ดูแลระบบ ดังนั้นการทำงานทั้งหมดภายในโครงงานนี้ สามารถแบ่งออกเป็น 3 ระบบหลัก คือ

- ระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงเพื่อการใช้งานอินเตอร์เน็ท ในระบบนี้จะเป็นระบบที่ทำหน้าที่ให้บริการแก่ผู้ใช้บริการในการที่จะทำการเชื่อมต่อเพื่อออกสู่ระบบอินเตอร์เน็ท บนเครือข่าย Wireless LAN โดยจะมีการรับ-ส่งข้อมูลผ่านระบบเครือข่าย VPN
- ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ เป็นระบบที่ให้บริการแก่ผู้ใช้บริการในการตรวจสอบการใช้งาน ณ ปัจจุบัน และนอกจากการตรวจสอบการใช้งานแล้ว ในระบบยังสามารถที่จะให้ผู้ใช้บริการทำการเปลี่ยนแปลงข้อมูลส่วนตัว และรหัสผ่านได้อีกด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- ระบบควบคุมดูแลสำหรับผู้ดูแลระบบ เป็นระบบที่ให้บริการสำหรับผู้ดูแลระบบในการที่จะควบคุมจัดการระบบให้สามารถให้บริการแก่ผู้ใช้งานได้ โดยภายในระบบนี้จะสามารถให้ผู้ดูแลตรวจสอบการข้อมูลต่าง ๆ ที่เกี่ยวกับผู้ใช้บริการได้ รวมทั้งการคำนวณการใช้งานของผู้ใช้บริการได้อีกด้วย

รายละเอียดและขั้นตอนการทำงานของระบบย่อยของทั้ง 3 ระบบ จะมีการกล่าวในหัวข้อถัดไป



รูปที่ 3.2 แสดงภาพของระบบที่มีการพัฒนาภายในโครงงานพัฒนาระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

3.3.1 การทำงานของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงเพื่อการใช้งานอินเตอร์เน็ท

ขั้นตอนที่ 1 ผู้ใช้บริการทำการเชื่อมต่อเข้าสู่ระบบเครือข่ายไวร์เลสแลน

ขั้นตอนที่ 2 ผู้ใช้บริการจะได้รับหมายเลขไอพีชุดที่ 1 จากการให้บริการของระบบ DHCP โดยหมายเลขไอพีชุดที่ 1 จะไม่สามารถทำการเชื่อมต่อเพื่อออกสู่ระบบอินเตอร์เน็ทได้ แต่จะใช้สำหรับเชื่อมต่อเพื่อเข้าสู่เครื่องเซอร์ฟเวอร์เพื่อใช้บริการอื่น ๆ เท่านั้น

ขั้นตอนที่ 3 ผู้ใช้บริการทำการเปิดเว็บเบราเซอร์เพื่อเข้าสู่หน้าจอที่ใช้สำหรับการดาวน์โหลดโปรแกรม OpenVPN และ vpnClient ในการเชื่อมต่อเพื่อออกสู่ระบบอินเตอร์เน็ท โดยในขั้นตอนนี้ผู้ใช้งานจะถูก redirect หน้าจอมาเมื่อผู้ใช้จะทำการออกสู่ระบบอินเตอร์เน็ท หรือเข้าได้โดยตรง ในการติดตั้งโปรแกรม OpenVPN และ vpnClient นั้น ผู้ใช้สามารถดูคู่มือการติดตั้งได้จากหน้าจอนี้ด้วย

ขั้นตอนที่ 4 สำหรับผู้ใช้บริการใหม่จะต้องทำการลงทะเบียนข้อมูล โดยสามารถคลิกลิงค์เพื่อทำการลงทะเบียนได้จากหน้าจอที่ใช้สำหรับดาวน์โหลดโปรแกรม OpenVPN และ vpnClient ได้ โดยข้อมูลเหล่านี้จะถูกบันทึกลงระบบฐานข้อมูล ซึ่งผู้ใช้บริการจะต้องทำการกรอกข้อมูลให้ครบถ้วนด้วย แต่ถ้าเป็นผู้ใช้บริการที่เคยลงทะเบียนไว้แล้วก็สามารถผ่านขั้นตอนนี้ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

ขั้นตอนที่ 5 ผู้ใช้บริการจะต้องทำการติดต่อกับผู้ดูแลระบบเพื่อขอหมายเลขรหัสการใช้งาน (Activate Code) โดยถ้าเป็นผู้ใช้บริการใหม่นั้น หลังจากที่ทำการลงทะเบียนเสร็จเรียบร้อยแล้ว ระบบจะมีการแจ้งให้ผู้ใช้บริการทำการติดต่อกับผู้ดูแลระบบเพื่อขอหมายเลขรหัสการใช้งาน (Activate Code)

ขั้นตอนที่ 6 เมื่อผู้ใช้บริการได้รับหมายเลขรหัสการเข้าใช้บริการ (Activate Code) จากผู้ดูแลระบบเรียบร้อยแล้ว สามารถที่จะทำการกรอกหมายเลขนั้นได้ลิงค์ที่หน้าจอของการบันทึกข้อมูลที่ทำการลงทะเบียนหรือเข้าไปยังระบบตรวจสอบการใช้งานโดยตรง หรือที่ลิงค์ของหน้าจอของระบบการพิสูจน์ตัวจริงเพื่อใช้งานอินเตอร์เน็ทได้

ขั้นตอนที่ 7 หลังจากที่มีการกรอกหมายเลขรหัสการใช้บริการ (Activate Code) เรียบร้อยแล้ว ผู้ใช้บริการเริ่มการเชื่อมต่อเข้าสู่ระบบพิสูจน์ตัวจริงเพื่อออกสู่ระบบอินเตอร์เน็ท โดยการคลิกสตาร์ทที่ไอคอนบนหน้าจอ ซึ่งถูกสร้างเมื่อมีการติดตั้งโปรแกรม OpenVPN และ vpnClient เรียบร้อยแล้ว

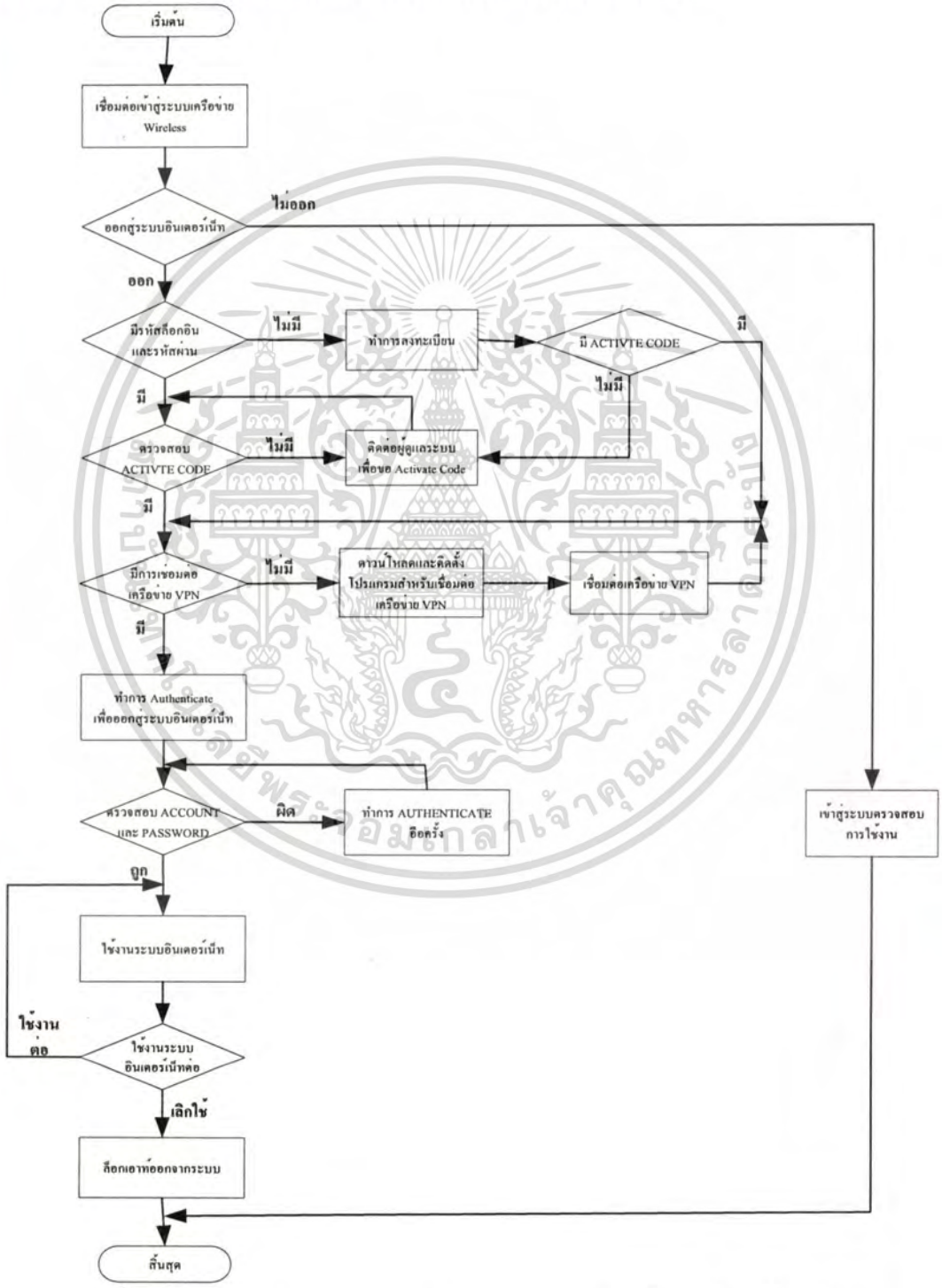
ขั้นตอนที่ 8 เมื่อเครื่องของผู้ใช้บริการทำการเชื่อมต่อระบบ VPN เรียบร้อยแล้ว เครื่องของผู้ใช้บริการจะได้หมายเลขไอพีชุดที่ 2 ซึ่งเป็นหมายเลขไอพีที่สามารถออกสู่ระบบอินเตอร์เน็ทได้

ขั้นตอนที่ 9 ผู้ใช้บริการเปิดเว็บเบราเซอร์เพื่อทำการเข้าสู่ระบบพิสูจน์ตัวจริง โดยจะถูก redirect มา เมื่อผู้ใช้ทำการออกสู่ระบบอินเตอร์เน็ท โดยเมื่อผู้ใช้ได้ทำการกรอกข้อมูลรหัสล็อกอินและรหัสผ่านถูกต้องเรียบร้อยแล้วระบบจะทำการ redirect ไปยังเว็บไซต์ที่ผู้ใช้บริการต้องการจะไป พร้อมทั้งระบบจะทำการสร้างเว็บเพจที่เป็น agent ในการเช็คสถานะการใช้งานของผู้ใช้บริการด้วย และในระหว่างที่ผู้ใช้บริการเชื่อมต่อออกสู่ระบบอินเตอร์เน็ท ข้อมูลที่รับ-ส่งระหว่างเครื่องของผู้ใช้บริการกับเครื่องเซอร์ฟเวอร์ของระบบจะถูกเข้ารหัสไว้เพื่อ SSL VPN ทำให้มีความปลอดภัยในการใช้งานในระบบ ซึ่งเมื่อผู้ใช้ต้องการที่จะทำการออกจากระบบสามารถคลิกที่ปุ่มล็อกเอาท์ที่เว็บเพจที่เป็น agent ซึ่งถือว่าเป็นการสิ้นสุดการใช้งานในระบบอินเตอร์เน็ท โดยข้อมูลต่าง ๆ ที่เกี่ยวกับการใช้งานของผู้ใช้บริการจะถูกบันทึกเพื่อนำไปคำนวณค่าใช้จ่ายต่อไป

นอกจากขั้นตอนการทำงานต่าง ๆ ข้างต้นที่ได้กล่าวมาของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง ยังมีการทำงานย่อย ๆ อื่น ๆ ที่จำเป็นต่อการใช้งานของผู้ใช้บริการอีก เช่น การทำงานของระบบตรวจสอบรหัสผ่านในกรณีที่ลืมรหัสผ่าน หรือระบบช่วยเหลือการติดตั้งโปรแกรม OpenVPN และ vpnClient โดยในระบบตรวจสอบรหัสผ่านในกรณีที่ลืมรหัสผ่านนั้นเป็นระบบที่ช่วยให้ผู้ใช้บริการสามารถตรวจสอบรหัสผ่านของตัวเองได้ในกรณีที่ลืมรหัสผ่าน แต่จะต้องมีการกรอกคำถามและคำตอบกันลืมก่อน โดยข้อมูลของคำถามและคำตอบกันลืมนั้นจะถูกกำหนดโดยผู้ใช้บริการเอง เมื่อผู้ใช้บริการได้ทำการกรอกข้อมูลเพื่อทำการลงทะเบียนในระบบครั้ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แรก ซึ่งถ้ามีการกรอกคำถามและคำตอบกันลืมภายในระบบตรวจสอบรหัสผ่านในกรณีที่ลืมรหัสผ่านถูกต้อง ระบบจะมีการแจ้งรหัสผ่านกลับมาให้ผู้ใช้บริการรับทราบ ส่วนระบบช่วยเหลือการติดตั้งโปรแกรม OpenVPN และ vpnClient นั้นจะเป็นระบบที่แสดงขั้นตอนการติดตั้งของทั้ง 2 โปรแกรม ให้ผู้ใช้สามารถดำเนินการตามได้ เพื่อความสะดวกในการใช้งาน



รูปที่ 3.3 แสดงการทำงานของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.2 การทำงานของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

ขั้นตอนที่ 1 ผู้ใช้บริการเข้าสู่ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ ผ่านเว็บเบราเซอร์ โดยสามารถเข้าได้จากหมายเลขไอพีชุดที่ 1 หรือหมายเลขไอพีชุดที่ 2 ได้ทั้งนั้น

ขั้นตอนที่ 2 ผู้ใช้บริการต้องทำการพิสูจน์ตัวจริงในการเข้าระบบ โดยต้องกรอกรหัสล็อกอินและรหัสผ่าน

ขั้นตอนที่ 3 เมื่อผู้ใช้บริการทำการรหัสล็อกอินและรหัสผ่านเรียบร้อยแล้ว จะสามารถเข้าสู่ระบบตรวจสอบการใช้งานได้ โดยภายในระบบนอกจากจะสามารถทำการตรวจสอบการใช้งานได้ยังมีการทำงานอื่น ๆ อีกคือ ระบบกรอกหมายเลขรหัสการใช้งาน ระบบแก้ไขข้อมูลส่วนตัว ระบบตรวจสอบประวัติการใช้งาน ระบบเปลี่ยนรหัสผ่าน

รูปที่ 3.4 แสดงภาพของระบบการทำงานย่อยที่อยู่ภายในระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

3.3.2.1 ระบบตรวจสอบการใช้งาน

ระบบนี้จะเป็นระบบที่ให้บริการแก่ผู้ใช้บริการที่การเข้าสู่ระบบตรวจสอบการใช้งานสำหรับผู้ใช้บริการ โดยตัวระบบถูกทำงานทุก ๆ 1 นาทีนับตั้งแต่มีการเข้าสู่ระบบ โดยข้อมูลที่แสดงจะเป็นข้อมูลการใช้งานของผู้ใช้บริการที่เป็นผู้เข้าสู่ระบบ

3.3.2.2 ระบบกรอกหมายเลขรหัสการใช้งาน

ระบบนี้จะเป็นระบบที่ให้ผู้ใช้บริการกรอกหมายเลขรหัสการใช้งาน ซึ่งได้รับจากผู้ดูแลระบบ เพื่อทำการใช้งานระบบอินเตอร์เน็ท โดยหมายเลขรหัสการใช้งาน (Activate Code) จะมีจำนวนทั้งหมด 12 หลัก แบ่งการสร้างตัวเลขออกเป็น 4 ชุด ๆ ละ 3 หลัก โดยใช้หลักการสุ่มตัวเลขที่ไม่ซ้ำกันเพื่อป้องกันหมายเลขที่ซ้ำกันระหว่างผู้ใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.2.3 ระบบแก้ไขข้อมูลส่วนตัว

ระบบนี้เป็นระบบที่ให้ผู้ใช้บริการสามารถทำการแก้ไขข้อมูลส่วนตัวที่ได้มีการลงทะเบียนไว้ โดยข้อมูลที่สามารถแก้ไขได้จะประกอบไปด้วย ชื่อ นามสกุล เพศ อายุ อาชีพ ที่อยู่ และอีเมลล์ เมื่อผู้ใช้บริการทำการแก้ไขข้อมูลเรียบร้อยแล้ว ระบบก็จะทำการอัพเดทข้อมูลในระบบฐานข้อมูล

3.3.2.4 ระบบตรวจสอบประวัติการใช้งาน

ระบบนี้เป็นระบบที่ให้ผู้ใช้บริการสามารถดูประวัติการใช้งานที่ผ่าน ๆ มาได้ โดยข้อมูลที่เป็นประวัติการใช้งานผู้ใช้จะเป็นข้อมูลที่ผู้ใช้ยังไม่ได้ดำเนินการจ่ายใช้งานและดำเนินการจ่ายค่าใช้งานแล้ว

3.3.2.5 ระบบเปลี่ยนรหัสผ่านของผู้ใช้บริการ

ระบบนี้เป็นระบบที่ให้ผู้ใช้บริการสามารถทำการเปลี่ยนแปลงรหัสผ่านได้ โดยข้อมูลที่ต้องกรอกคือข้อมูลของรหัสผ่านเดิมที่ใช้งานอยู่ และข้อมูลของรหัสผ่านใหม่ที่ต้องการจะเปลี่ยน พร้อมทั้งการยืนยันรหัสผ่านใหม่อีกครั้ง เมื่อผู้ใช้บริการทำการเปลี่ยนข้อมูลเรียบร้อยแล้ว ระบบจะทำการบันทึกข้อมูลนั้นลงระบบฐานข้อมูล

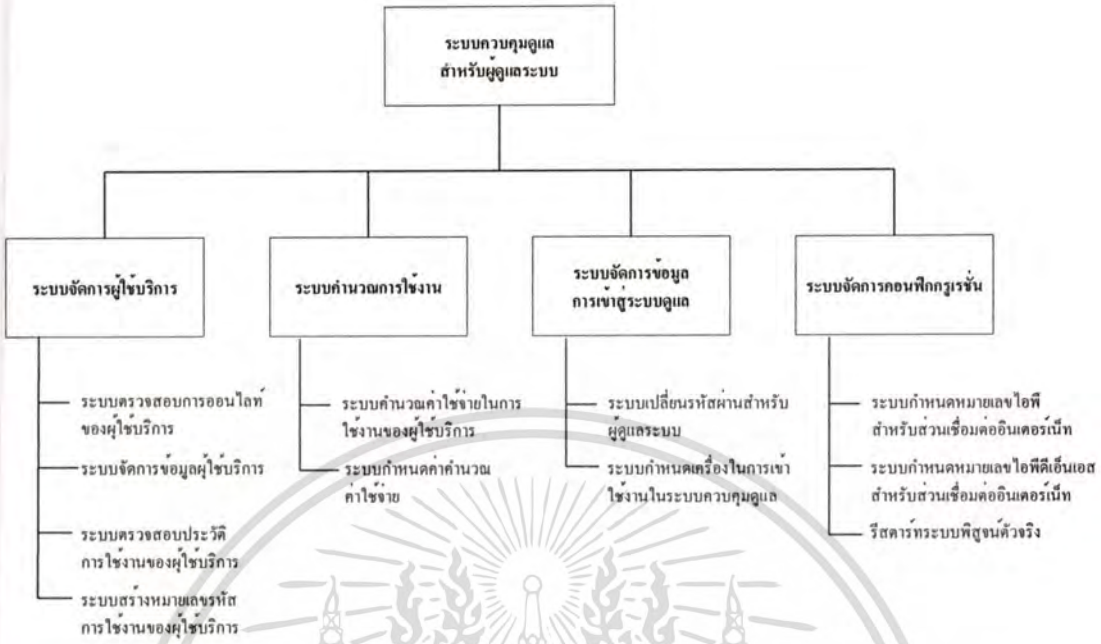
3.3.3 การทำงานของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

ขั้นตอนที่ 1 ผู้ดูแลระบบเข้าสู่ระบบการควบคุมดูแล ผ่านเว็บเบราเซอร์ โดยเครื่องที่จะเข้าสู่ระบบได้จะต้องเป็นหมายเลขไอพีที่มีการระบุสิทธิ์ให้เข้าได้เท่านั้น

ขั้นตอนที่ 2 ผู้ดูแลระบบต้องทำการพิสูจน์ตัวจริงในการเข้าระบบ โดยต้องกรอกรหัสล็อกอินและรหัสผ่าน

ขั้นตอนที่ 3 เมื่อผู้ดูแลระบบทำการรหัสล็อกอินและรหัสผ่านเรียบร้อยแล้ว จะสามารถเข้าสู่ระบบควบคุมดูแลได้ โดยภายในระบบจะมีการทำงานของระบบย่อย ๆ คือ ระบบจัดการผู้ใช้งาน ระบบคำนวณการใช้งาน ระบบจัดการข้อมูลในการเข้าสู่ระบบควบคุมดูแล ระบบจัดการข้อมูลคอนฟิกกูเรชั่นของระบบ โดยรายละเอียดของแต่ละระบบจะมีการกล่าวในหัวข้อถัดไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.5 แสดงการทำงานของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

3.3.3.1 ระบบจัดการผู้ใช้บริการ

ภายในระบบนี้ถูกแบ่งการทำงานออกเป็นระบบย่อย ๆ อีก 4 ระบบคือ ระบบตรวจสอบการออนไลท์ของผู้ใช้บริการ ระบบจัดการข้อมูลผู้ใช้บริการ ระบบตรวจสอบประวัติการใช้งานของผู้ใช้บริการ ระบบสร้างหมายเลขรหัสการใช้งานของผู้ใช้บริการ

- ***ระบบตรวจสอบการออนไลท์ของผู้ใช้บริการ*** เป็นระบบที่ใช้สำหรับให้ผู้ดูแลทำการเช็คจำนวนการออนไลท์ของผู้ใช้บริการในระบบที่เชื่อมต่อออกสู่ระบบอินเตอร์เน็ท ณ เวลาปัจจุบัน โดยจะมีการแสดงข้อมูลที่เป็นรหัสล็อกอิน จำนวนการใช้งานของการอัพโหลดข้อมูล ดาวน์โหลดข้อมูลและจำนวนรวม โดยข้อมูลเหล่านี้จะถูกแสดงในรูปแบบของตารางข้อมูล
- ***ระบบจัดการข้อมูลของผู้ใช้บริการ*** เป็นระบบที่ใช้สำหรับให้ผู้ดูแลระบบเลือกที่จะทำการตรวจสอบข้อมูลของผู้ใช้บริการหรือลบข้อมูลของผู้ใช้บริการออกจากระบบ โดยจะมีการยืนยันก่อนการลบข้อมูล ซึ่งข้อมูลของผู้ใช้บริการทั้งหมดจะถูกแสดงในรูปแบบของตารางข้อมูลให้ผู้ดูแลระบบสามารถเลือกทำงานได้
- ***ระบบตรวจสอบประวัติการใช้งานของผู้ใช้บริการ*** เป็นระบบที่ให้ผู้ดูแลระบบเลือกทำการตรวจสอบประวัติการใช้งานของผู้ใช้บริการ โดยข้อมูลที่แสดงจะเป็นรหัสล็อกอิน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อและนามสกุลของผู้ใช้บริการ ซึ่งถูกแสดงในรูปแบบของตารางข้อมูลให้ผู้ดูแลเลือกตรวจสอบได้

- ***ระบบสร้างหมายเลขรหัสการใช้งานของผู้ใช้บริการ*** เป็นระบบที่ให้ผู้ดูแลระบบทำการสร้างหมายเลขรหัสการเข้าใช้งานของผู้ใช้บริการ โดยทำการกรอกข้อมูลรหัสล็อกอินที่ต้องการสร้างหมายเลขรหัส หลังจากนั้นระบบจะดำเนินการสร้างรหัสหมายเลขขนาด 12 หลัก โดยในการสร้างรหัสหมายเลขจะถูกแบ่งการสร้างออกเป็น 4 กลุ่ม ๆ ละ 3 หมายเลข เพื่อป้องกันมิให้หมายเลขมีการซ้ำกันระหว่างผู้ใช้บริการ และในระหว่างการสร้างหมายเลขรหัสสำหรับผู้ใช้บริการนั้น ระบบจะทำการเช็คจากฐานข้อมูลเดิมว่ารหัสล็อกอินนี้ถูกมีการสร้างหมายเลขรหัสอยู่ก่อนหน้าหรือไม่ ถ้าไม่ก็จะทำการสร้างหมายเลขรหัสนั้นใหม่ แต่ถ้ามีอยู่แล้วระบบจะทำการดึงหมายเลขรหัสนั้นขึ้นมาแสดง อนึ่ง สำหรับการสร้างหมายเลขรหัสการเข้าใช้งานของผู้ใช้บริการจะสร้างได้ก็ต่อเมื่อเป็นผู้ใช้บริการนั้นเป็นผู้ใช้บริการใหม่ที่เพิ่งเข้ามาใช้งานในระบบครั้งแรก หรือเป็นผู้ใช้บริการที่มีการชำระค่าใช้งานเรียบร้อยแล้ว ต้องการใช้งานในระบบอีกครั้ง

3.3.3.2 ระบบคำนวณการใช้งานของผู้ใช้บริการ

ภายในระบบนี้ถูกแบ่งการทำงานออกเป็นระบบย่อย ๆ อีก 2 ระบบคือ ระบบคำนวณการใช้งานของผู้ใช้บริการ และระบบการตั้งค่าการคำนวณการใช้งาน

- ***ระบบคำนวณการใช้งานของผู้ใช้บริการ*** เป็นระบบที่ให้ผู้ดูแลระบบทำการคำนวณการใช้งานของผู้ใช้บริการออกมาเป็นจำนวนเงินที่ต้องจ่ายในการใช้งาน โดยจะมีการแสดงข้อมูลของผู้ใช้บริการที่เป็นรหัสล็อกอิน ชื่อและนามสกุลในรูปแบบของตารางข้อมูลให้ผู้ดูแลระบบทำการเลือกที่จะคำนวณ หลังจากที่ผู้ดูแลระบบทำการเลือกผู้ใช้บริการได้แล้วระบบจะทำการคำนวณการใช้งานตามอัตราส่วนที่มีการกำหนดในระบบการตั้งค่าการคำนวณการใช้งาน
- ***ระบบการตั้งค่าการคำนวณการใช้งาน*** เป็นระบบที่ให้ผู้ดูแลระบบทำการตั้งค่าการคำนวณการใช้งาน โดยข้อมูลอยู่ 3 ส่วนที่ต้องจำเป็นต้องกรอกให้ถูกต้องและครบถ้วน คืออัตราการใช้งาน หน่วย (มีให้เลือก 3 ประเภทคือ ไบต์ กิโลไบต์ เมกกะไบต์) และราคา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.3.3 ระบบจัดการข้อมูลที่เข้าสู่ระบบควบคุมดูแล

ภายในระบบนี้ถูกแบ่งการทำงานออกเป็นระบบย่อย ๆ อีก 2 ระบบคือ ระบบเปลี่ยนรหัสผ่านสำหรับผู้ดูแล และระบบการกำหนดเครื่องที่จะเข้าใช้งานในระบบควบคุมดูแล

- ***ระบบเปลี่ยนรหัสผ่านสำหรับผู้ดูแล*** เป็นระบบที่ให้ผู้ดูแลระบบสามารถทำการเปลี่ยนรหัสผ่านในการเข้าสู่ระบบควบคุมดูแลได้ โดยข้อมูลที่ต้องกรอกคือข้อมูลของรหัสผ่านเดิมที่ใช้งานอยู่ และข้อมูลของรหัสผ่านใหม่ที่ต้องการจะเปลี่ยน พร้อมทั้งการยืนยันรหัสผ่านใหม่อีกครั้ง เมื่อผู้ดูแลระบบทำการเปลี่ยนข้อมูลเรียบร้อยแล้ว ระบบจะทำการบันทึกข้อมูลนั้นลงระบบฐานข้อมูล
- ***ระบบกำหนดเครื่องที่จะเข้าใช้งานในระบบควบคุมดูแล*** เป็นระบบที่ให้ผู้ดูแลสามารถทำการกำหนด เปลี่ยนแปลงและลบข้อมูลของเครื่องที่จะเข้าใช้งานในระบบควบคุมดูแลได้ โดยข้อมูลที่ใช้งานในระบบนี้คือหมายเลขไอพีเพียงอย่างเดียว

3.3.3.4 ระบบจัดการข้อมูลคอนฟิกกูเรชั่นของระบบ

ภายในระบบนี้ถูกแบ่งการทำงานออกเป็น 3 ระบบย่อย ๆ คือ ระบบกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท ระบบการหมายเลขไอพีของดีเอ็นเอสสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ทและระบบสำหรับรีสตาร์ทระบบพิสูจน์ตัวจริง

- ***ระบบกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท*** เป็นระบบที่ให้ผู้ดูแลสามารถทำการกำหนดหมายเลขไอพีในส่วนเชื่อมต่อระบบอินเตอร์เน็ท โดยหลังจากที่ผู้ดูแลกำหนดหมายเลขไอพีเรียบร้อยแล้ว ระบบจะทำการบันทึกลงในไฟล์คอนฟิก แต่ระบบจะทำการเปลี่ยนไปใช้หมายเลขไอพีที่กำหนดก็ต่อเมื่อระบบมีการรีสตาร์ท ซึ่งระบบจะมีการแจ้งให้ผู้ดูแลทำการรีสตาร์ทระบบเพื่อใช้หมายเลขไอพีที่กำหนด
- ***ระบบกำหนดหมายเลขไอพีดีเอ็นเอสสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท*** เป็นระบบที่ให้ผู้ดูแลสามารถทำการกำหนดหมายเลขไอพีดีเอ็นเอสในส่วนเชื่อมต่อระบบอินเตอร์เน็ท โดยหลังจากที่ผู้ดูแลกำหนดหมายเลขไอพีเรียบร้อยแล้ว ระบบจะทำการบันทึกลงในไฟล์คอนฟิก แต่ระบบจะทำการเปลี่ยนไปใช้หมายเลขไอพีดีเอ็นเอสที่กำหนดก็ต่อเมื่อระบบมีการรีสตาร์ท ซึ่งระบบจะมีการแจ้งให้ผู้ดูแลทำการรีสตาร์ทระบบเพื่อใช้หมายเลขไอพีดีเอ็นเอสที่กำหนด
- ***ระบบสำหรับรีสตาร์ทระบบพิสูจน์ตัวจริง*** เป็นระบบที่ให้ผู้ดูแลสามารถทำการรีสตาร์ทระบบพิสูจน์ตัวจริง

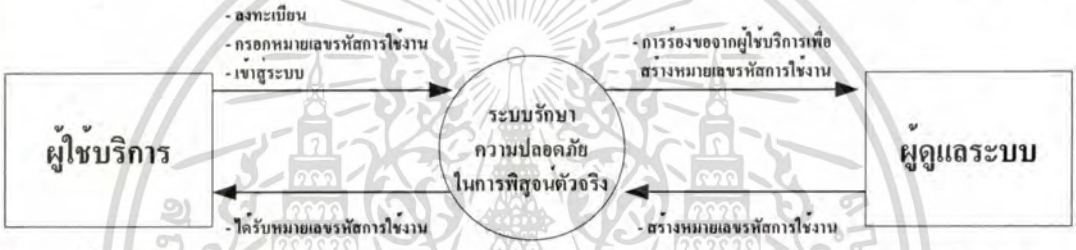
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.4 คอนเท็กซ์ไดอะแกรม ของโครงงานระบบ

การออกแบบโครงสร้างของโครงงานระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง สามารถเขียนให้อยู่ในรูปของคอนเท็กซ์ ไดอะแกรม ที่จะแสดงถึงขอบเขตของระบบงาน แสดงถึงสิ่งต่างๆ ที่เกี่ยวข้องกับระบบ และแสดงถึงการไหลของข้อมูลที่สัมพันธ์กันทั้งข้อมูลเข้าและออกจากระบบงาน โดยจะแบ่งออกเป็น 3 ระบบหลัก คือระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง ระบบหลักตรวจสอบการใช้งานของผู้ใช้บริการ และระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

3.4.1 รายละเอียดคอนเท็กซ์ไดอะแกรมของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

ดูคอนเท็กซ์ไดอะแกรมของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงได้จากรูปที่ 3.6



รูปที่ 3.6 แสดงคอนเท็กซ์ ไดอะแกรม ของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

คอนเท็กซ์ ไดอะแกรม ดังรูปที่ 3.6 แสดงให้เห็นว่า มีผู้ใช้บริการและผู้ดูแลระบบที่มีส่วนเกี่ยวข้องกับระบบงาน ซึ่งอธิบายได้ดังนี้

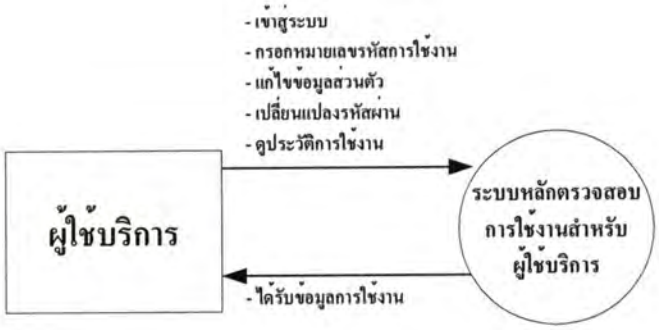
ผู้ใช้บริการ เป็นส่วนของผู้ใช้งานที่จะทำการร้องขอการรับบริการในการเข้าสู่ระบบ โดยจะมีการดำเนินการกับระบบที่เกี่ยวข้องคือ การลงทะเบียนเพื่อกำหนดรหัสล็อกอินและรหัสผ่านเข้าสู่ระบบด้วยตนเอง การกรอกหมายเลขรหัสการใช้งานที่ได้จากการติดต่อกับผู้ดูแลระบบ การเชื่อมต่อเข้าสู่ระบบเครือข่าย VPN โดยทำการดาวน์โหลดโปรแกรมที่ตัวระบบจัดไว้สำหรับผู้ใช้บริการใหม่

ผู้ดูแลระบบ เป็นส่วนของเจ้าหน้าที่ที่คอยทำการตรวจสอบการลงทะเบียนเพื่ออนุญาตให้เข้าใช้งานระบบโดยจะดำเนินการสร้างหมายเลขรหัสการใช้งานตามการร้องขอของผู้ใช้บริการ

3.4.2 รายละเอียดคอนเท็กซ์ไดอะแกรมของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

ดูคอนเท็กซ์ไดอะแกรมของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ ได้จากรูปที่ 3.7

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.7 แสดงคอนเท็กซ์ ไดอะแกรม ของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

คอนเท็กซ์ ไดอะแกรม ดังรูปที่ 3.7 แสดงให้เห็นว่า มีเพียงผู้ใช้บริการที่มีส่วนเกี่ยวข้องกับระบบงาน ซึ่งอธิบายได้ดังนี้

ผู้ใช้บริการ เป็นส่วนของผู้ใช้งานที่จะดำเนินการใช้งานภายในระบบ โดยการทำงานภายในระบบนั้น จะต้องมีการล็อกอินเพื่อเข้าสู่ระบบ หลังจากการเข้าสู่ระบบได้แล้ว ระบบจะมีการแจ้งจำนวนการใช้งานแก่ผู้ใช้บริการเมื่อผู้ใช้บริการได้เข้าใช้งานในระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงอยู่ ณ ขณะนั้น หรือจะเลือกที่จะทำงานอื่น ๆ ภายในระบบ คือ ดำเนินการกรอกหมายเลขรหัสการใช้งาน ดำเนินการแก้ไขข้อมูลส่วนตัว ดำเนินการเปลี่ยนรหัสผ่าน และดำเนินการเช็คดูประวัติการใช้งาน

3.4.3 รายละเอียดคอนเท็กซ์ไดอะแกรมของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

ดูคอนเท็กซ์ไดอะแกรมของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ ได้จากรูปที่ 3.8

รูปที่ 3.8 แสดงคอนเท็กซ์ ไดอะแกรม ของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

คอนเท็กซ์ ไดอะแกรม ดังรูปที่ 3.8 แสดงให้เห็นว่า มีเพียงผู้ดูแลระบบที่มีส่วนเกี่ยวข้องกับระบบงาน ซึ่งอธิบายได้ดังนี้

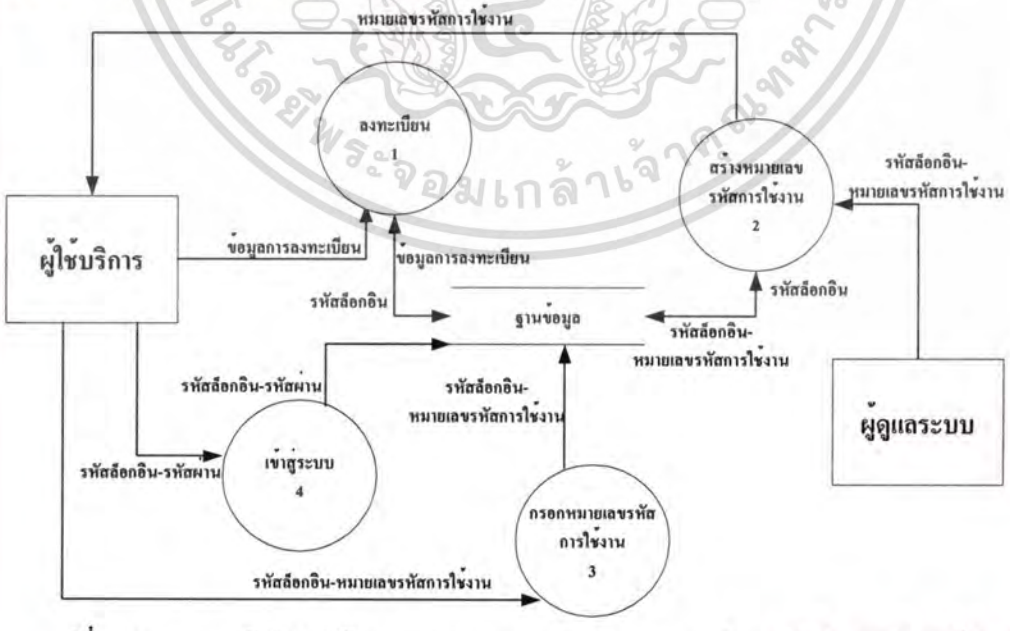
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ดูแลระบบ เป็นส่วนของผู้ที่จะดำเนินการใช้งานภายในระบบ โดยการทำงานภายในระบบนั้น จะต้องมีการล็อกอินเพื่อเข้าสู่ระบบ หลังจากการเข้าสู่ระบบได้แล้ว ผู้ดูแลระบบก็สามารถที่จะเลือกที่จะทำงานภายในระบบ คือ ดำเนินการตรวจสอบการออนไลท์ของผู้ใช้บริการ โดยระบบจะมีการแจ้งยอดการออนไลท์ ณ ขณะนั้น ให้ผู้ดูแลระบบได้ทราบ ดำเนินการเลือกตรวจสอบข้อมูลของผู้ใช้บริการ โดยข้อมูลที่ผู้ดูแลระบบจะได้รับเป็นข้อมูลที่ผู้ใช้บริการทำการลงทะเบียนไว้ ดำเนินการเลือกตรวจสอบประวัติการใช้งานของผู้ใช้บริการ โดยข้อมูลที่ดูแลระบบจะได้รับเป็นข้อมูลประวัติการใช้งานของผู้ใช้บริการที่ถูกเลือก ดำเนินการคำนวณยอดค่าใช้จ่ายในการใช้งาน โดยข้อมูลที่จะได้รับจะเป็นยอดค่าใช้จ่ายรวม ซึ่งคิดจากอัตราที่ผู้ดูแลระบบกำหนดรวมกับจำนวนการใช้งาน ดำเนินการเปลี่ยนรหัสผ่าน ดำเนินการกำหนดเครื่องที่สามารถเข้าสู่ระบบควบคุมดูแลได้ ดำเนินการกำหนดข้อมูลสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท

3.5 ดาต้าโฟลว์ ไดอะแกรม ของระบบงานที่ทำการพัฒนา

สำหรับภาพรวมการทำงานของทั้งระบบงานสามารถ แบ่งออกเป็น 3 ระบบหลัก โดยภายในแต่ละระบบจะมีส่วนงานย่อย ที่แสดงถึงความสัมพันธ์โดยรวมระหว่างโพรเซส กระแสข้อมูล และการจัดเก็บข้อมูล จากแผนภาพคอนเท็กซ์ ไดอะแกรมของระบบงานที่ออกแบบไว้

3.5.1 ดาต้าโฟลว์ไดอะแกรมของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

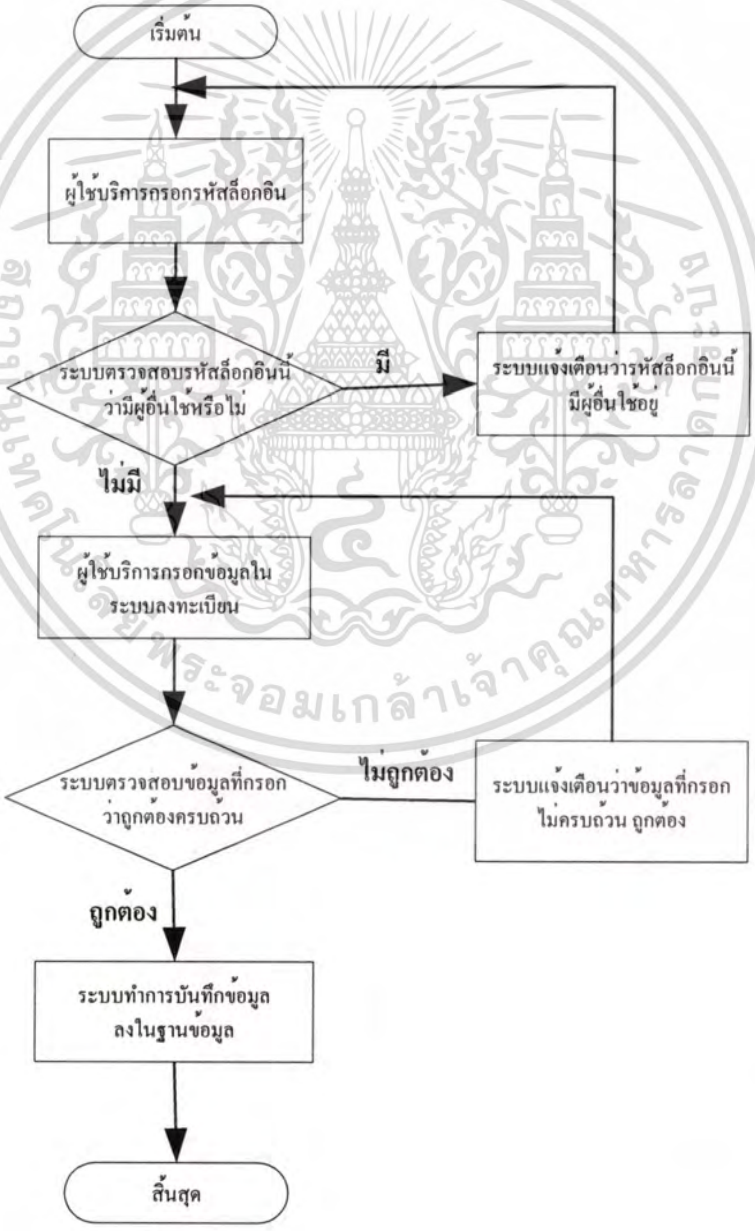


รูปที่ 3.9 แสดงดาต้าโฟลว์ ไดอะแกรมของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รายละเอียดของงานย่อยในแต่ละโพรเซสจากดาต้าโฟลว์ ไดอะแกรมในรูป 3.9 สามารถแสดงและอธิบายหน้าที่การทำงานได้ดังนี้

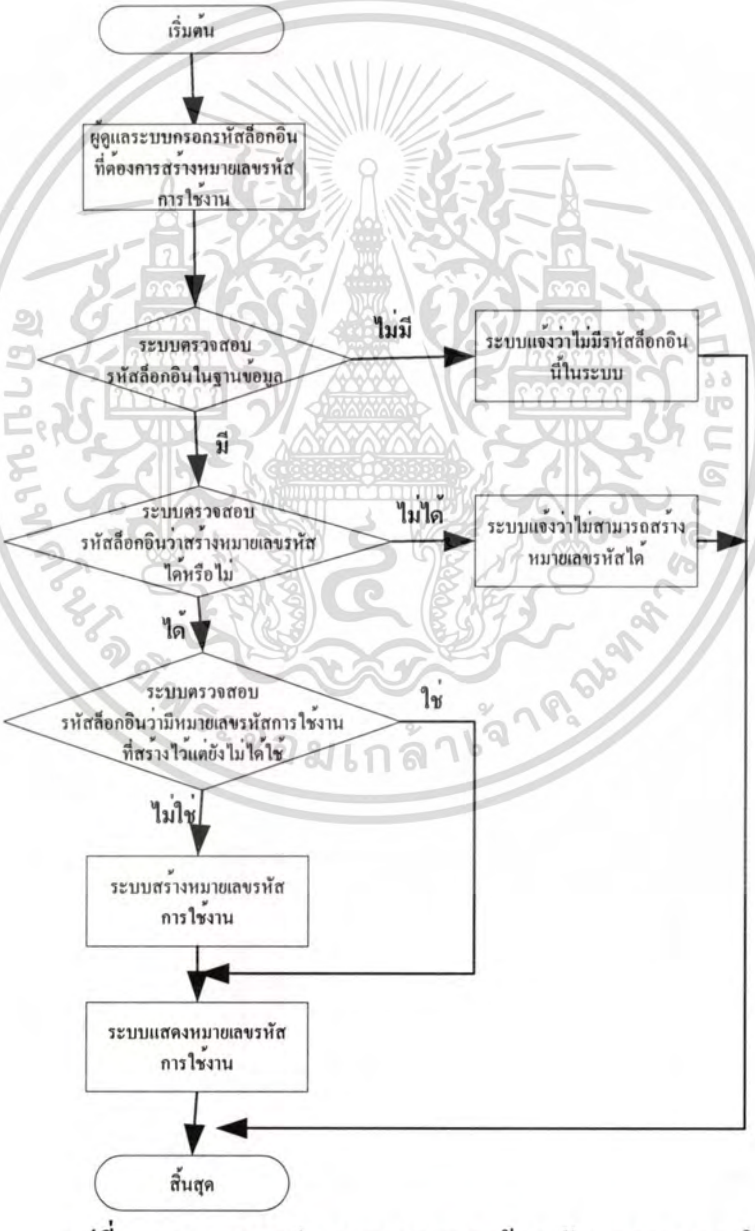
การลงทะเบียน ทำหน้าที่ในการบันทึกรับรายละเอียดข้อมูลของการลงทะเบียนจากผู้ใช้บริการ โดยระบบจะทำการตรวจสอบการรหัสล็อกอินของผู้ใช้บริการที่สามารถกำหนดเองได้ก่อนว่ามีผู้ใช้บริการอื่น ๆ ใช้รหัสล็อกอินนี้หรือไม่ ถ้ามีก็จะทำการแจ้งให้ผู้ใช้บริการได้ทราบ เพื่อเปลี่ยนไปใช้รหัสล็อกอินอื่น ๆ แทน แต่ถ้าไม่มีระบบก็จะทำการบันทึกข้อมูลการลงทะเบียนของผู้ใช้บริการ ดูรายละเอียดของการทำงานได้จากรูปที่ 3.10



รูปที่ 3.10 แสดงการทำงานของระบบลงทะเบียน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

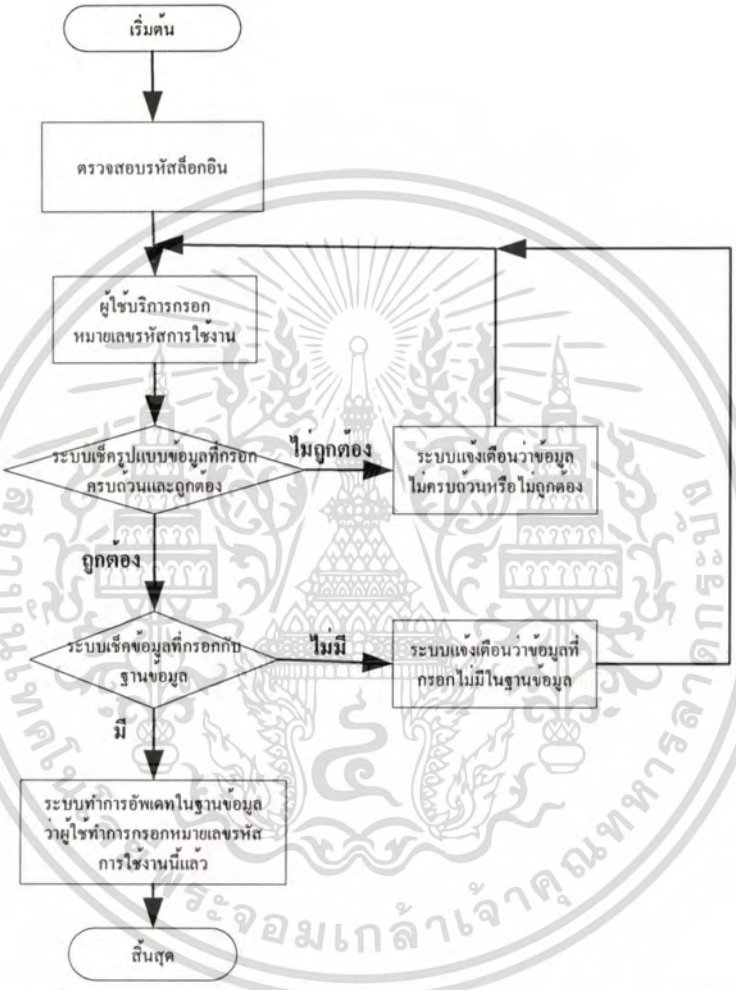
การสร้างหมายเลขรหัสการใช้งาน ทำหน้าที่ในการสร้างหมายเลขรหัสการเข้าใช้งานของผู้ขอใช้บริการ โดยผู้ดูแลระบบจะเป็นผู้สร้างหมายเลขรหัสนี้ขึ้นมา แต่ในการสร้างหมายเลขรหัสการใช้งานนี้ ระบบจะมีการตรวจสอบรหัสล็อกอินของผู้ใช้บริการว่ามีอยู่ในระบบหรือไม่ ถ้ามีระบบก็จะทำการสร้างหมายเลขรหัสการใช้งานขึ้นมาให้ แต่ถ้าไม่มีรหัสล็อกอินนั้น ๆ ระบบก็จะทำการแจ้งว่ารหัสล็อกอินนั้น ๆ ไม่สามารถสร้างหมายเลขรหัสการใช้งานได้ ดูรายละเอียดของการทำงานได้จากรูปที่ 3.11



รูปที่ 3.11 แสดงการทำงานของระบบสร้างรหัสหมายเลขการใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การกรอกหมายเลขรหัสการใช้งาน ทำหน้าที่ในการกรอกหมายเลขรหัสการใช้งานของผู้ใช้บริการ โดยผู้ใช้บริการจะกรอกหมายเลขรหัสการใช้งานที่ได้รับมาจากผู้ดูแลระบบ ดูรายละเอียดของการทำงานได้จากรูปที่ 3.12

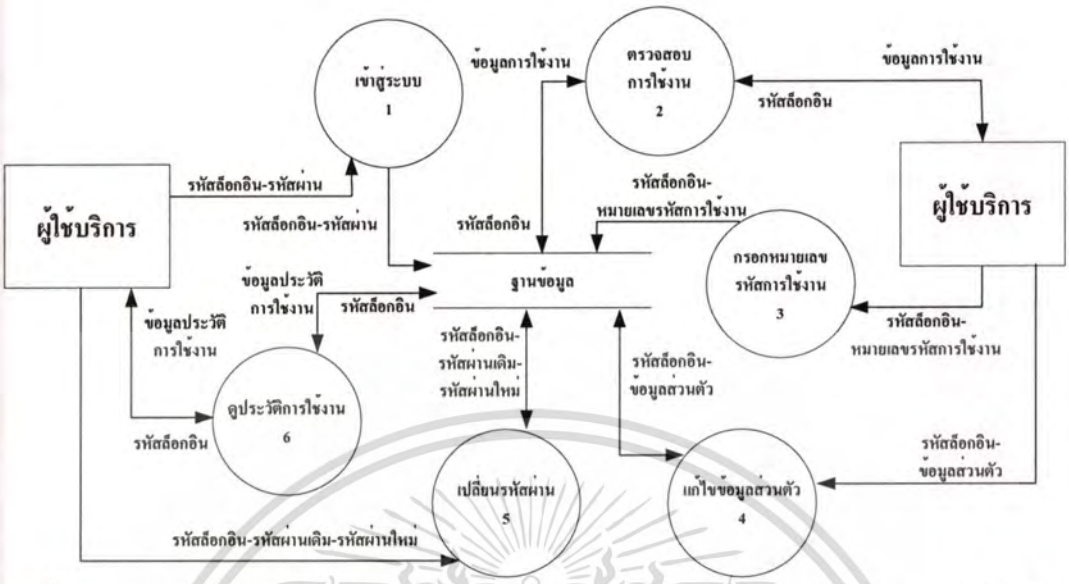


รูปที่ 3.12 แสดงการทำงานของการกรอกหมายเลขรหัสการใช้งาน

การเข้าสู่ระบบ ทำหน้าที่ในการตรวจสอบการเข้าสู่ระบบของผู้ใช้บริการจากข้อมูลที่ผู้ใช้บริการกรอกมาให้คือรหัสล็อกอินและรหัสผ่าน ถ้าระบบตรวจสอบข้อมูลว่าถูกต้องผู้ใช้บริการก็สามารถที่จะเข้าสู่ระบบเพื่อใช้งานระบบอินเตอร์เน็ทได้

3.5.2 ดาต้าโฟลว์ไดอะแกรมของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

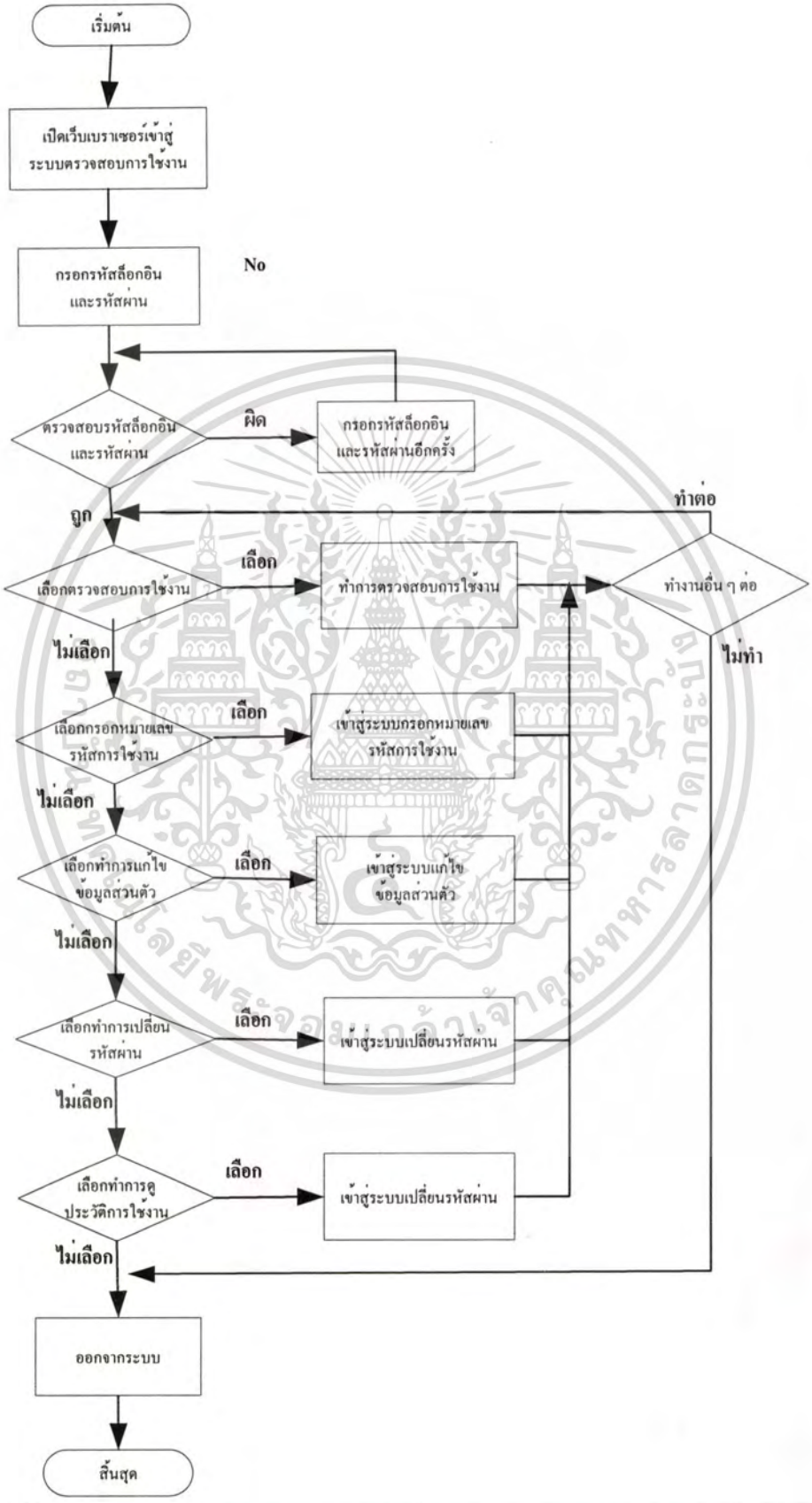


รูปที่ 3.13 แสดงดาต้าโฟลว์ ไดอะแกรมของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

รายละเอียดของงานย่อยในแต่ละโพรเซสจากดาต้าโฟลว์ ไดอะแกรมในรูป 3.13 สามารถแสดงและอธิบายหน้าที่การทำงานได้ดังนี้

การเข้าสู่ระบบ ทำหน้าที่ในการตรวจสอบการเข้าสู่ระบบของผู้ใช้บริการจากข้อมูลที่ผู้ใช้บริการกรอกมาให้คือรหัสล็อกอินและรหัสผ่าน ถ้าระบบตรวจสอบข้อมูลว่าถูกต้องผู้ใช้บริการก็สามารถที่จะเข้าสู่ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการได้ โดยมีการทำงานดังรูปที่ 3.14

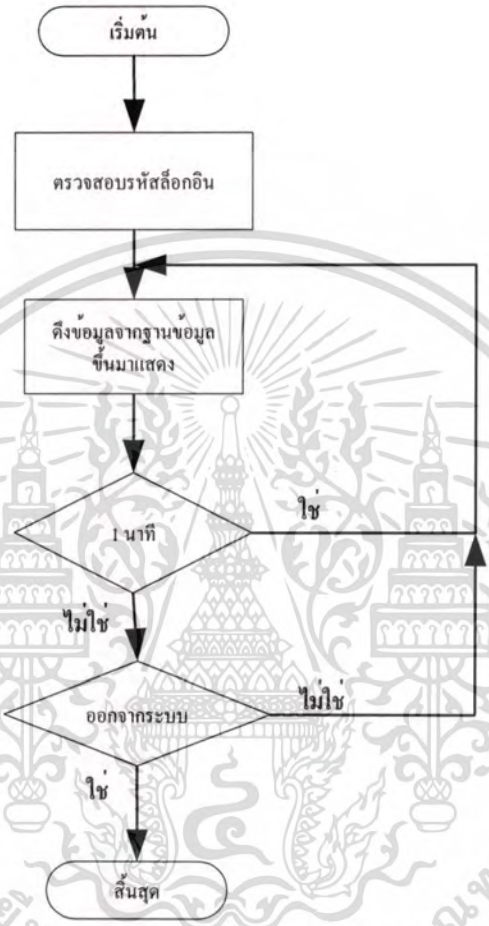
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.14 แสดงการทำงานของระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การตรวจสอบการใช้งาน ทำหน้าที่ในการตรวจสอบการใช้งานของผู้ใช้บริการ ณ ขณะที่ผู้ใช้บริการยังมีการใช้งานในระบบอินเตอร์เน็ทอยู่ ดูรายละเอียดการทำงานได้จากรูปที่ 3.15

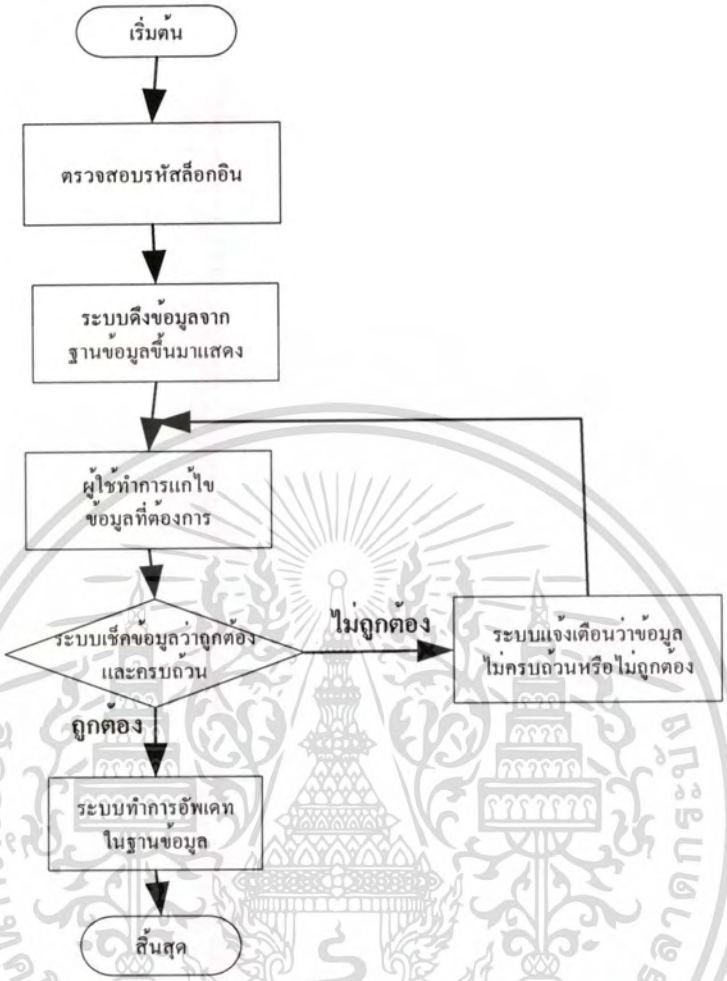


รูปที่ 3.15 แสดงการทำงานของการตรวจสอบการใช้งาน

การกรอกหมายเลขรหัสการใช้งาน ทำหน้าที่ในการกรอกหมายเลขรหัสการใช้งานของผู้ใช้บริการ โดยผู้ใช้บริการจะกรอกหมายเลขรหัสการใช้งานที่ได้รับมาจากผู้ดูแลระบบ ดูรายละเอียดการทำงานได้จากรูปที่ 3.12

การแก้ไขข้อมูลส่วนตัว ทำหน้าที่ในการให้ผู้ใช้บริการทำการแก้ไขข้อมูลส่วนตัวของผู้ใช้บริการเอง โดยระบบจะมีการแสดงข้อมูลเดิมให้ผู้ใช้บริการจะทำการแก้ไขข้อมูลส่วนตัวใหม่ ดูรายละเอียดการทำงานได้จากรูปที่ 3.16

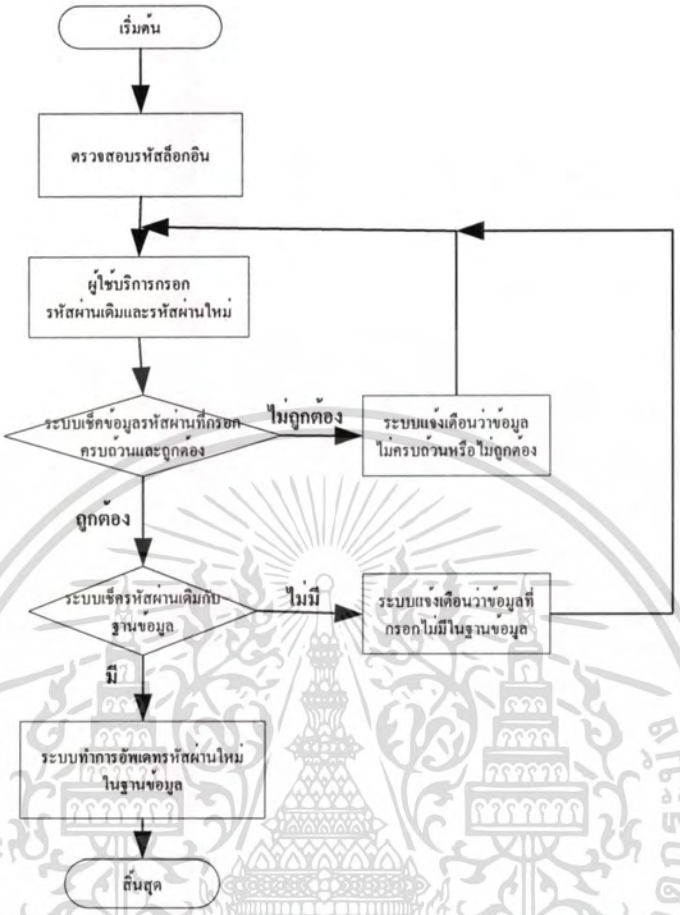
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.16 แสดงการทำงานของการแก้ไขข้อมูลส่วนตัว

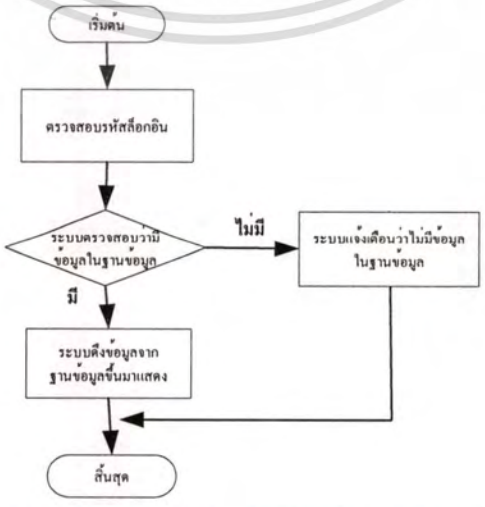
การเปลี่ยนรหัสผ่าน ทำหน้าที่ในการให้ผู้ใช้บริการทำการเปลี่ยนรหัสผ่านของผู้ใช้บริการเอง โดยผู้ใช้บริการจะต้องทำการกรอกข้อมูลรหัสผ่านเก่าและรหัสผ่านใหม่เข้าไป แล้วระบบจะทำการเช็ครหัสผ่านเดิมว่าถูกต้องหรือไม่ ถ้าถูกต้องระบบจะทำการแก้ไขข้อมูลรหัสผ่านเป็นข้อมูลใหม่ แต่ถ้าไม่ถูกต้องระบบจะมีการแจ้งเตือนให้ผู้ใช้บริการได้ทราบ ดูรายละเอียดการทำงานได้จากรูปที่ 3.17

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.17 แสดงการทำงานของการเปลี่ยนแปลงรหัสผ่านของผู้ใช้บริการ

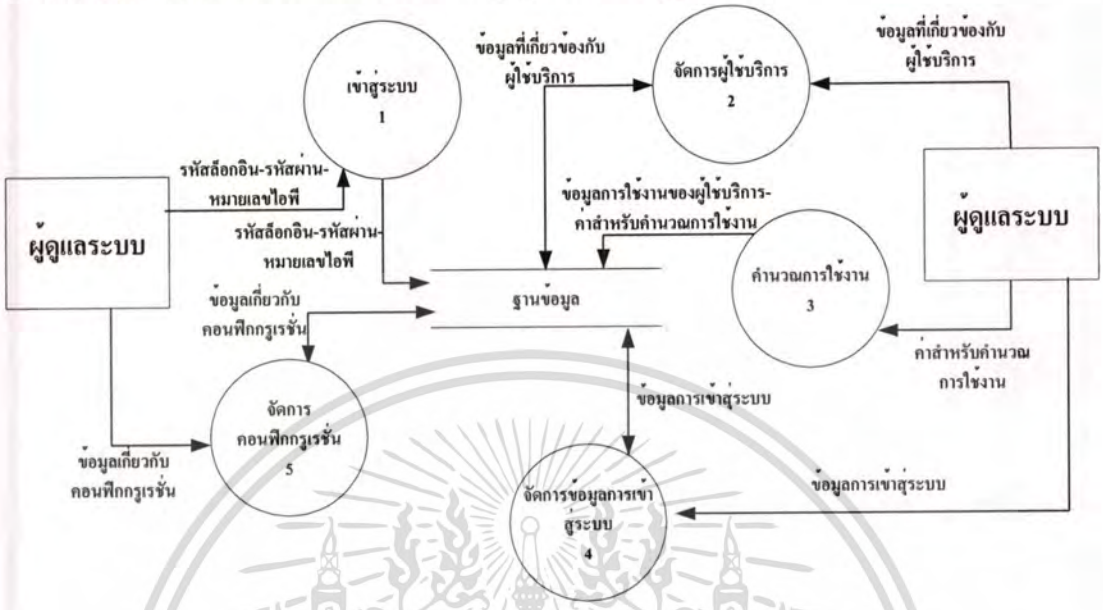
การดูประวัติการใช้งาน ทำหน้าที่ในการให้ผู้ใช้บริการตรวจสอบประวัติการใช้งานที่ผ่านมา โดยข้อมูลเหล่านี้ จะเป็นข้อมูลหลังจากการชำระค่าใช้งานแล้ว ดูรายละเอียดการทำงานได้จากรูปที่ 3.18



รูปที่ 3.18 แสดงการทำงานของการดูประวัติการใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5.3 ดาต้าโฟลว์ไดอะแกรมของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ



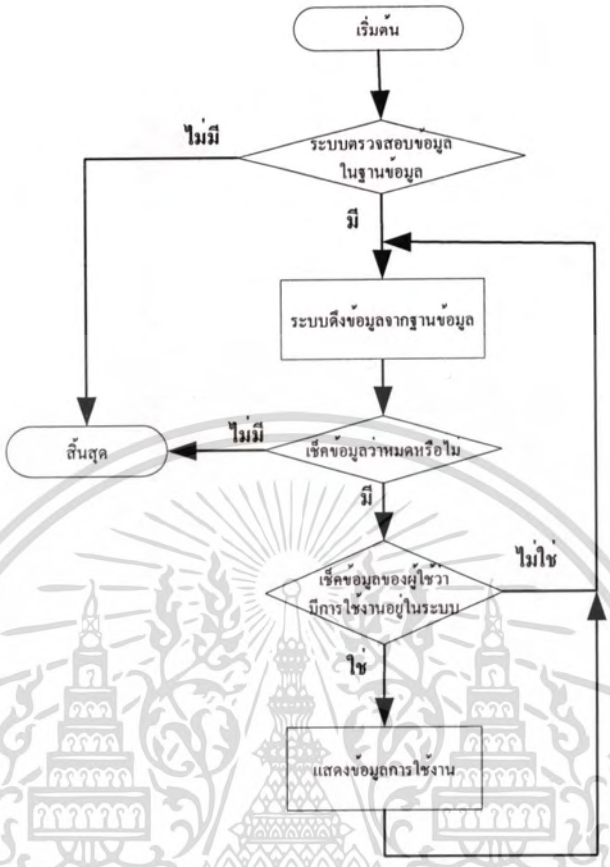
รูปที่ 3.19 แสดงดาต้าโฟลว์ ไดอะแกรมของระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

รายละเอียดของงานย่อยในแต่ละโพรเซสจากดาต้าโฟลว์ ไดอะแกรมในรูป 3.19 สามารถแสดงและอธิบายหน้าที่การทำงานได้ดังนี้

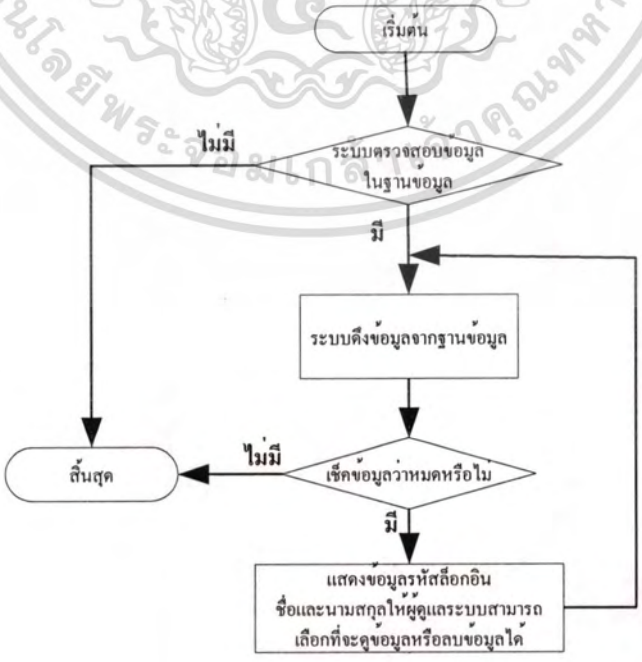
การเข้าสู่ระบบ ทำหน้าที่ในการตรวจสอบการเข้าสู่ระบบของผู้ดูแลระบบจากข้อมูลที่ผู้ใช้บริการกรอกมาให้คือรหัสล็อกอิน รหัสผ่านและหมายเลขไอพี ถ้าระบบตรวจสอบข้อมูลว่าถูกต้องผู้ใช้บริการก็สามารถที่จะเข้าสู่ระบบควบคุมดูแลสำหรับผู้ดูแลระบบได้

การจัดการข้อมูลผู้ใช้บริการ ทำหน้าที่ในการจัดการข้อมูลต่าง ๆ ของผู้ใช้บริการ โดยจะเป็นข้อมูลส่วนตัวของผู้ใช้บริการ ข้อมูลประวัติการใช้งานของผู้ใช้บริการ ข้อมูลการออนไลท์ของผู้ใช้บริการหรือ ข้อมูลหมายเลขรหัสการใช้งานของผู้ใช้บริการ ดูรายละเอียดการทำงานได้จากรูปที่ 3.20 – 3.22

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

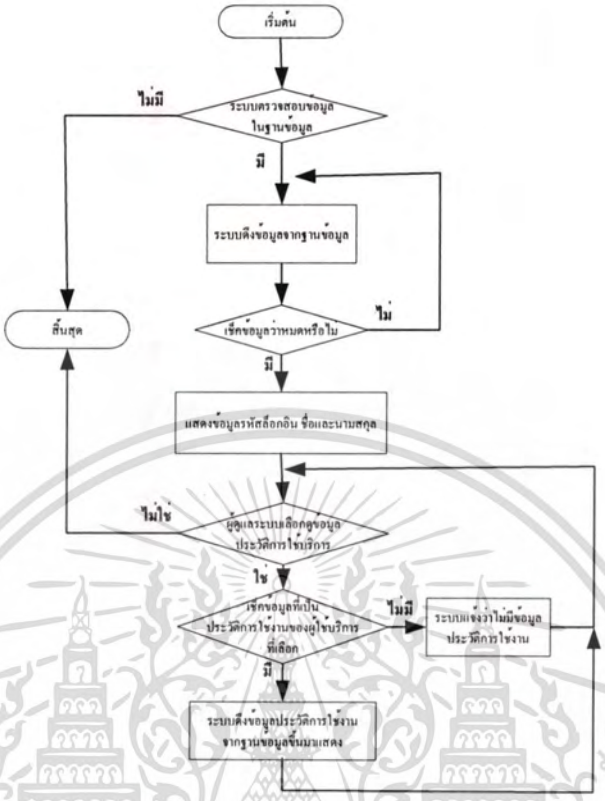


รูปที่ 3.20 แสดงการทำงานของระบบตรวจสอบการออนไลท์ของผู้ใช้บริการ



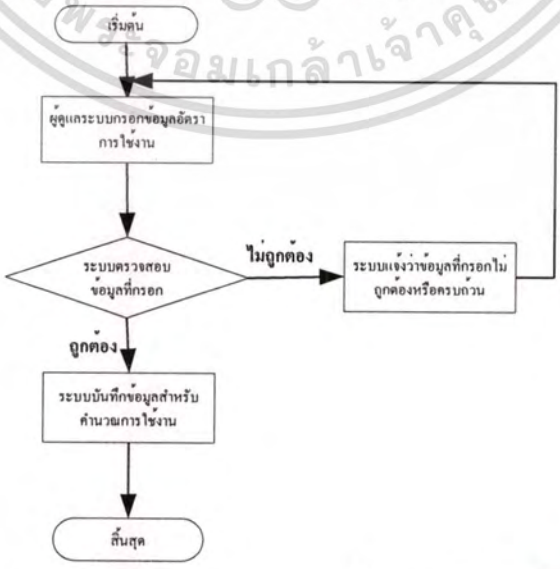
รูปที่ 3.21 แสดงการทำงานของระบบตรวจสอบข้อมูลของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



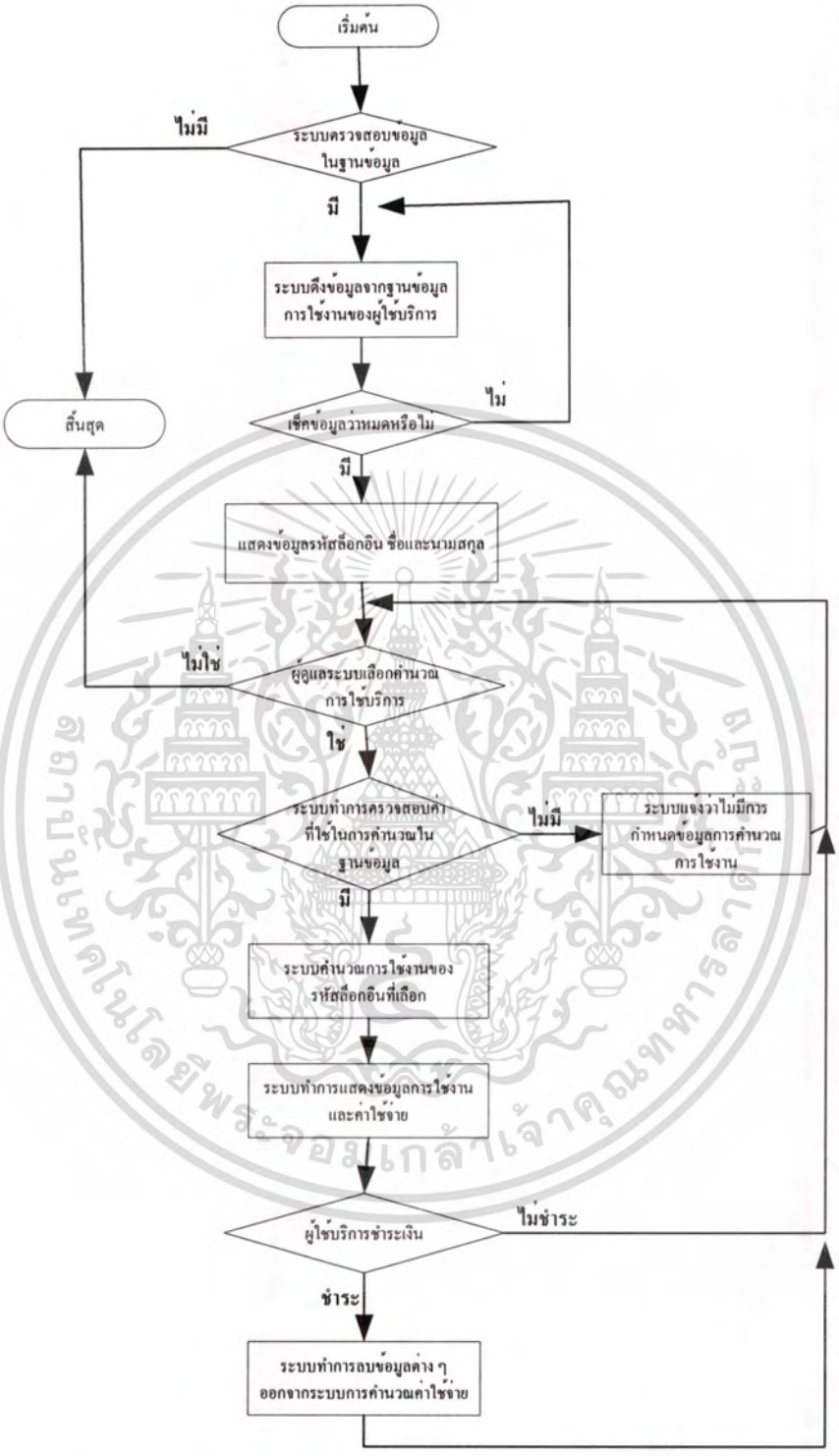
รูปที่ 3.22 แสดงการทำงานของระบบตรวจสอบประวัติการใช้งานของผู้ใช้บริการ

การคำนวณการใช้งาน ทำหน้าที่ในการคำนวณการใช้งานของผู้ใช้บริการออกมาเป็นค่าใช้จ่ายที่ผู้ใช้บริการจะต้องจ่าย โดยระบบจะคำนวณจากข้อมูลการใช้งานของผู้ใช้บริการกับค่าที่ใช้ในการคำนวณการใช้งาน ดูรายละเอียดการทำงานได้จากรูปที่ 3.23 – 3.24



รูปที่ 3.23 แสดงการทำงานของระบบการกำหนดค่าสำหรับคำนวณการใช้งาน

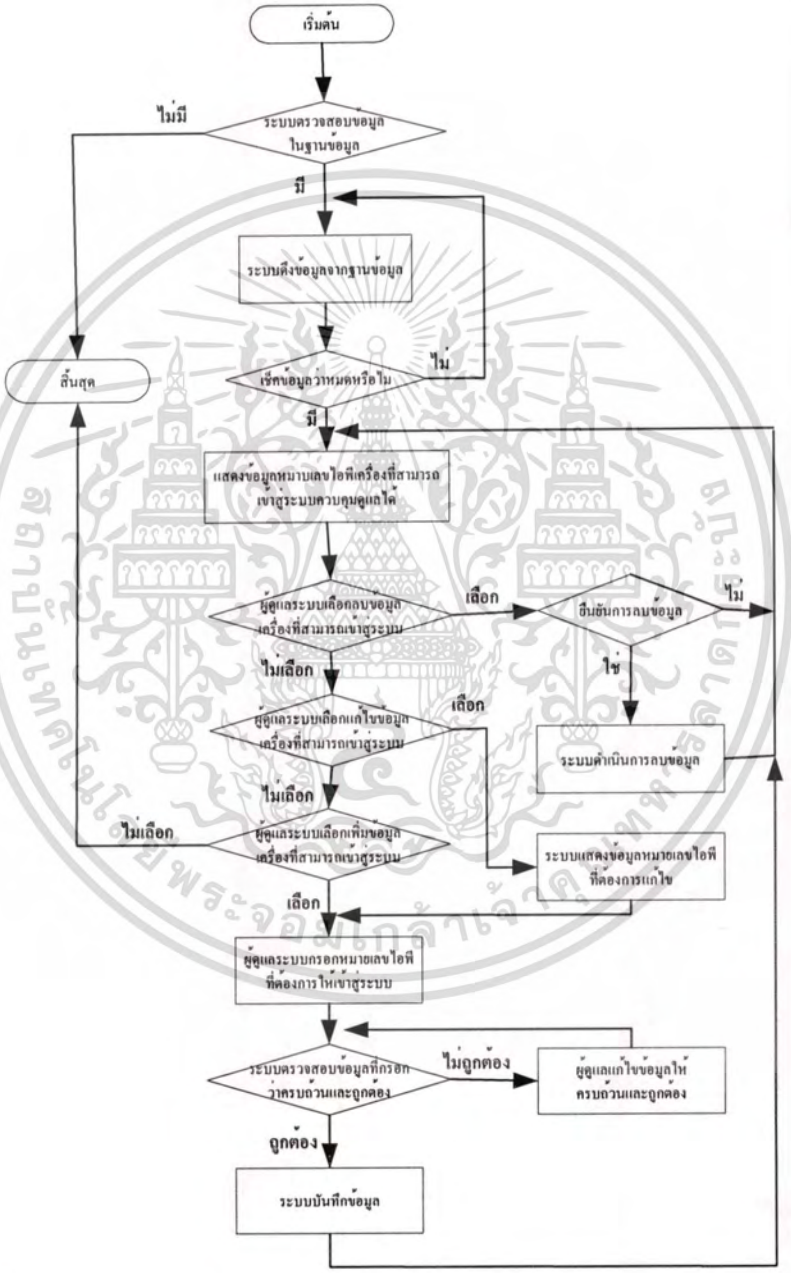
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.24 แสดงการทำงานของระบบการคำนวณการใช้งานของผู้ใช้บริการ

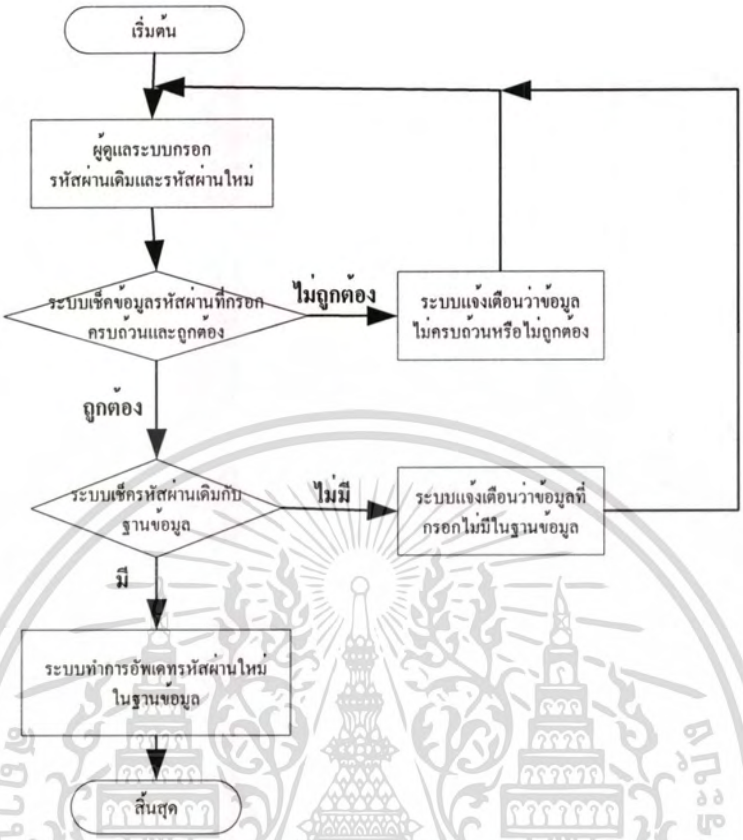
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การจัดการข้อมูลการเข้าสู่ระบบควบคุมดูแล โดยจะเป็นข้อมูลที่เกี่ยวกับรหัสผ่านของผู้ควบคุมดูแล และข้อมูลหมายเลขไอพีที่สามารถเข้าสู่ระบบควบคุมดูแลได้ ดูรายละเอียดการทำงานได้จากรูปที่ 3.25 – 3.26



รูปที่ 3.25 แสดงการทำงานของระบบกำหนดเครื่องที่เข้าสู่ระบบควบคุมดูแล

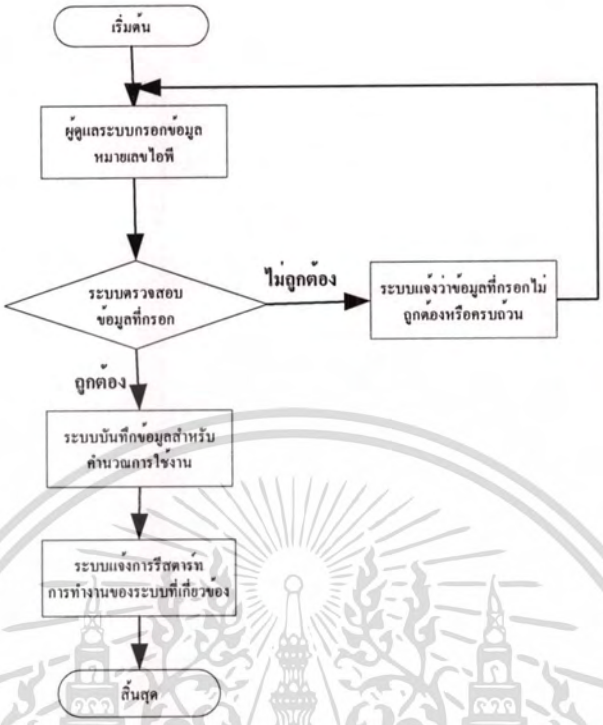
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



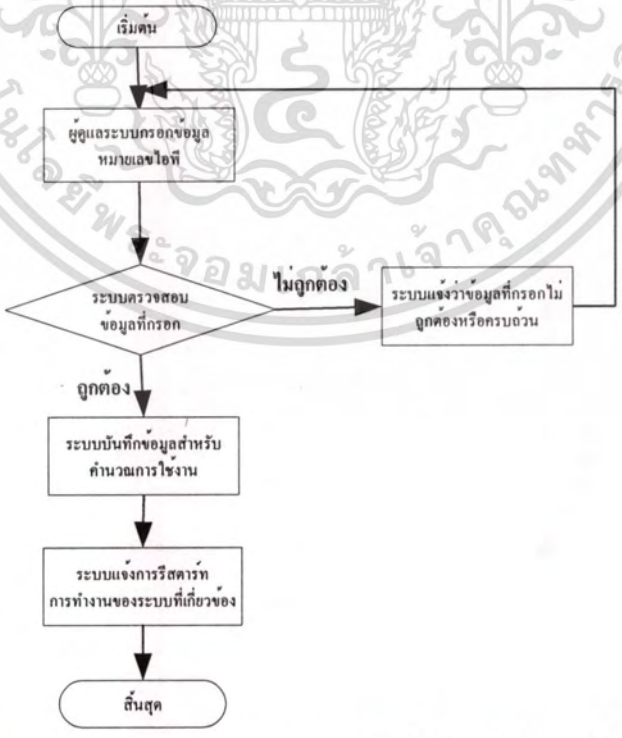
รูปที่ 3.26 แสดงการทำงานของระบบการเปลี่ยนรหัสผ่านสำหรับผู้ดูแลระบบ

การจัดการข้อมูลคอนฟิกกรูเรชั่นของส่วนเชื่อมต่อระบบอินเตอร์เน็ท โดยจะเป็นข้อมูลที่เป็นหมายเลขไอพีของอินเตอร์เฟสและหมายเลขไอพีของดีเอ็นเอสในส่วนที่ใช้ในการเชื่อมต่อระบบอินเตอร์เน็ท ดูรายละเอียดการทำงานได้จากรูปที่ 3.27 – 3.29

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.27 แสดงการทำงานของระบบกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ทของระบบ



รูปที่ 3.28 แสดงการทำงานของระบบกำหนดหมายเลขไอพีดีเอ็นเอสสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ทของระบบ

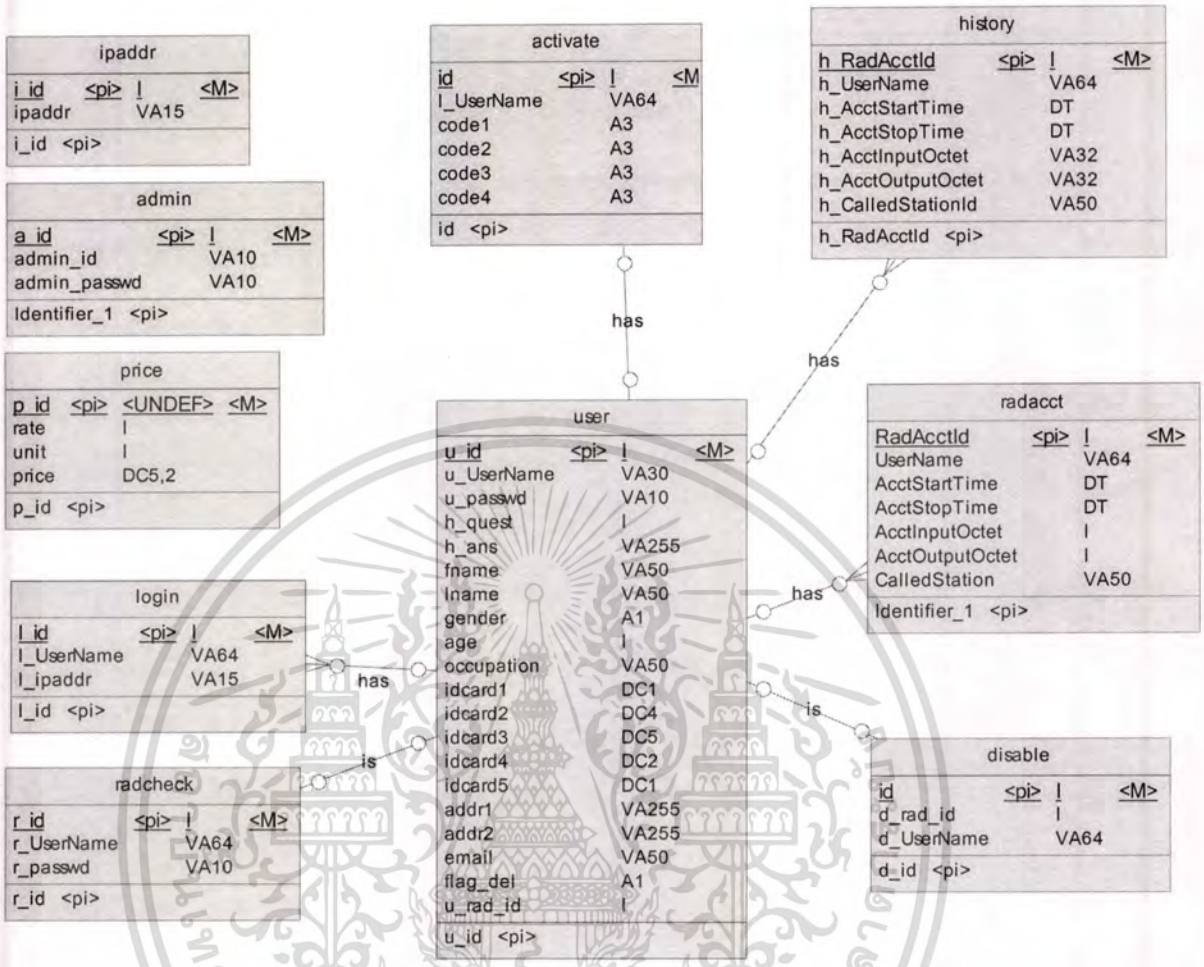
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 3.29 แสดงการทำงานของการรีสตาร์ทระบบพิสูจน์ตัวจริง

3.6 การออกแบบฐานข้อมูลของระบบงาน

จากการออกแบบภาพรวมของระบบงาน (Context Diagram) และการออกแบบความสัมพันธ์และการไหลของข้อมูลในระบบงาน (Data Flow Diagram) ที่ได้นำเสนอไป สามารถวิเคราะห์ออกแบบความสัมพันธ์ของข้อมูลภายในระบบงาน โดยนำเสนอในลักษณะที่เป็นแผนภาพรวมที่เรียกว่า แบบจำลอง E-R Model ได้ดังรูปที่ 3.30

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.30 แสดง E-R Diagram ของระบบงาน

จากภาพ 3.30 ซึ่งเป็นแผนภาพ E-R Diagram ที่แสดง ประกอบไปด้วยความสัมพันธ์ของเอนทิตี้ (Entity) ต่างๆ ซึ่งสามารถอธิบายรายละเอียดได้ดังนี้

ความสัมพันธ์ระหว่างข้อมูลผู้ใช้ (user) กับ ข้อมูลหมายเลขรหัสการใช้งาน (activate) เป็นแบบ one to one คือสมาชิกคนหนึ่งสามารถขอหมายเลขรหัสการใช้งานได้เพียงหมายเลขเดียวต่อการเข้าใช้บริการก่อนการชำระเงิน และข้อมูลหมายเลขรหัสการใช้งานจะถูกลบไปเมื่อผู้ใช้มีการกรอกรหัสนั้นไปแล้ว

ความสัมพันธ์ระหว่างข้อมูลผู้ใช้ (user) กับข้อมูลการห้ามเข้าสู่ระบบ (disable) เป็นแบบ one to one คือสมาชิกคนหนึ่งจะถูกห้ามเข้าสู่ระบบได้เพียงครั้งเดียว โดยจะเกิดขึ้นหลังจากการชำระเงินไปแล้ว และถ้าสมาชิกมีการกรอกหมายเลขรหัสการเข้าใช้งานถูกต้อง ข้อมูลที่อยู่ตารางการห้ามเข้าสู่ระบบ (disable) ก็จะถูกลบออกไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ความสัมพันธ์ระหว่างข้อมูลผู้ใช้ (user) กับข้อมูลประวัติการใช้งาน (history) เป็นแบบ one to many คือสมาชิกคนหนึ่งสามารถมีข้อมูลประวัติการใช้งานได้มากกว่า 1 ครั้ง โดยข้อมูลประวัติการใช้งานจะถูกเก็บหลังจากที่ผู้ใช้บริการมีการชำระค่าใช้งานเรียบร้อยแล้ว

ความสัมพันธ์ระหว่างข้อมูลผู้ใช้ (user) กับข้อมูลการใช้งาน (radacct) เป็นแบบ one to many คือสมาชิกคนหนึ่งสามารถมีการข้อมูลการใช้งานได้มากกว่า 1 ครั้ง โดยข้อมูลการใช้งานนี้จะนำไปใช้ในการคิดคำนวณค่าใช้งาน และจะถูกลบออกไปเมื่อผู้ใช้งานมีการชำระเงินเรียบร้อยแล้ว

ความสัมพันธ์ระหว่างข้อมูลผู้ใช้ (user) กับข้อมูลการล็อกอินออกสู่ระบบอินเตอร์เน็ท (radcheck) เป็นแบบ one to one คือ สมาชิกคนหนึ่งจะมีข้อมูลในการล็อกอินออกสู่ระบบอินเตอร์เน็ทเพียง 1 รหัสเท่านั้น

ความสัมพันธ์ระหว่างข้อมูลผู้ใช้ (user) กับข้อมูลการเข้าสู่ระบบตรวจสอบการใช้งาน (login) เป็นแบบ one to many คือสมาชิกคนหนึ่งสามารถที่จะทำการล็อกอินเข้าสู่ระบบตรวจสอบได้จากหลายเครื่อง แต่เมื่อมีการออกจากระบบตรวจสอบข้อมูลเหล่านี้จะถูกลบออกจากระบบทั้งหมด

นอกจากนี้ยังข้อมูลของผู้ดูแลระบบ (admin) และข้อมูลเครื่องที่สามารถเข้าใช้งานในระบบควบคุมดูแล ที่ไม่มีความสัมพันธ์กับข้อมูลใด ๆ เลย

จากแผนภาพ E-R Diagram สามารถนำมาสร้างออกมาเป็นตารางในการเก็บข้อมูลของระบบได้ดังนี้

ตารางที่ 3.1 แสดงรายชื่อตารางที่ใช้เก็บข้อมูลในการพัฒนาระบบ

ลำดับที่	ชื่อตาราง	รายละเอียด
1	activate	เก็บข้อมูลเกี่ยวกับหมายเลขรหัสการใช้งานและผู้ใช้บริการ
2	admin	เก็บข้อมูลเกี่ยวกับผู้ดูแลระบบ
3	disable	เก็บข้อมูลเกี่ยวกับการห้ามผู้ใช้บริการออกสู่ระบบอินเตอร์เน็ท
4	history	เก็บข้อมูลประวัติการใช้งานของผู้ใช้บริการ
5	Ipaddr	เก็บข้อมูลเกี่ยวกับเครื่องที่สามารถเข้าใช้งานในระบบควบคุมดูแล
6	Login	เก็บข้อมูลของผู้ใช้บริการที่เข้าสู่ระบบตรวจสอบการใช้งาน
7	Price	เก็บข้อมูลเกี่ยวกับค่าในการคำนวณการใช้งานของผู้ใช้บริการ
8	user	เก็บข้อมูลเกี่ยวกับรายละเอียดของผู้ใช้บริการ
9	radcheck	เก็บข้อมูลเกี่ยวกับรหัสล็อกอินและรหัสผ่านในการออกสู่ระบบอินเตอร์เน็ท
10	radacct	เก็บข้อมูลเกี่ยวกับรายละเอียดการใช้งานของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.2 แสดงโครงสร้างและรายละเอียดของตาราง activate

Field	Type	Length	Key	Description
id	int	11	PRI	ไอดีของข้อมูล
login_id	varchar	64		รหัสล็อกอินของผู้ใช้บริการ
code1	varchar	3		หมายเลขรหัสการใช้งาน ชุดที่ 1
code2	varchar	3		หมายเลขรหัสการใช้งาน ชุดที่ 2
code3	varchar	3		หมายเลขรหัสการใช้งาน ชุดที่ 3
code4	varchar	3		หมายเลขรหัสการใช้งาน ชุดที่ 4

ตารางที่ 3.3 แสดงโครงสร้างและรายละเอียดของตาราง admin

Field	Type	Length	Key	Description
user_id	varchar	10	PRI	รหัสล็อกอินของผู้ดูแลระบบ
passwd	varchar	10		รหัสผ่านของผู้ดูแลระบบ

ตารางที่ 3.4 แสดงโครงสร้างและรายละเอียดของตาราง disable

Field	Type	Length	Key	Description
id	int	11	PRI	ไอดีของข้อมูล
rad_id	int	11	FRK	ไอดีที่เชื่อมไปยังตาราง radcheck
UserName	varchar	64		ข้อมูลรหัสล็อกอินของผู้ใช้บริการ

ตารางที่ 3.5 แสดงโครงสร้างและรายละเอียดของตาราง ipaddr

Field	Type	Length	Key	Description
id	varchar	30	PRI	ไอดีของข้อมูล
ipaddr	varchar	15		หมายเลขไอพีของเครื่องที่อนุญาตให้เข้าระบบควบคุมดูแล

ตารางที่ 3.6 แสดงโครงสร้างและรายละเอียดของตาราง login

Field	Type	Length	Key	Description
login_id	varchar	30	PRI	รหัสล็อกอินของผู้ใช้บริการ
ipaddr	varchar	15		หมายเลขไอพีของเครื่องผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.7 แสดงโครงสร้างและรายละเอียดของตาราง history

Field	Type	Length	Key	Description
radacctid	Int	21	PRI	ไอดีของข้อมูล
UserName	varchar	64		ข้อมูลรหัสล็อกอินของผู้ใช้บริการ
AcctStartTime	datetime			ข้อมูลการเริ่มเข้าใช้งานในระบบ
AcctStopTime	datetime			ข้อมูลการออกจากระบบ
AcctInputOctets	varchar	50		ข้อมูลการใช้งานประเภทอัพโหลด
AcctOutputOctets	varchar	50		ข้อมูลการใช้งานประเภทดาวน์โหลด

ตารางที่ 3.8 แสดงโครงสร้างและรายละเอียดของตาราง price

Field	Type	Length	Key	Description
id	int	11	PRI	ไอดีของข้อมูล
rate	int	10		อัตราการใช้
unit	int	1		หน่วย
price	Int	6		ราคา

ตารางที่ 3.9 แสดงโครงสร้างและรายละเอียดของตาราง radacct

Field	Type	Length	Key	Description
radacctid	Int	21	PRI	ไอดีของข้อมูล
UserName	varchar	64		ข้อมูลรหัสล็อกอินของผู้ใช้บริการ
AcctStartTime	datetime			ข้อมูลการเริ่มเข้าใช้งานในระบบ
AcctStopTime	datetime			ข้อมูลการออกจากระบบ
AcctInputOctets	varchar	50		ข้อมูลการใช้งานประเภทอัพโหลด
AcctOutputOctets	varchar	50		ข้อมูลการใช้งานประเภทดาวน์โหลด

ตารางที่ 3.10 แสดงโครงสร้างและรายละเอียดของตาราง radcheck

Field	Type	Length	Key	Description
id	int	11	PRI	ไอดีของข้อมูล
UserName	varchar	64		รหัสล็อกอินของผู้ใช้บริการ
Value	varchar	10		รหัสผ่านของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3.11 แสดงโครงสร้างและรายละเอียดของตาราง user

Field	Type	Length	Key	Description
id	int	10	PRI	ไอดีของข้อมูล
login_id	varchar	30		รหัสล็อกอินของผู้ใช้บริการ
passwd	varchar	10		รหัสผ่านของผู้ใช้บริการ
h_quest	int	1		ประเภทของคำถามกันลืม
h_ans	varchar	255		คำตอบกันลืม
fname	varchar	50		ชื่อของผู้ใช้บริการ
lname	varchar	50		นามสกุลของผู้ใช้บริการ
gender	char	1		เพศของผู้ใช้บริการ
age	int	2		อายุของผู้ใช้บริการ
occupation	varchar	50		อาชีพของผู้ใช้บริการ
idcard1	int	1		หมายเลขบัตรประชาชนชุดที่ 1
idcard2	int	4		หมายเลขบัตรประชาชนชุดที่ 2
idcard3	int	5		หมายเลขบัตรประชาชนชุดที่ 3
idcard4	int	2		หมายเลขบัตรประชาชนชุดที่ 4
idcard5	int	1		หมายเลขบัตรประชาชนชุดที่ 5
addr1	varchar	255		ที่อยู่ของผู้ใช้บริการ
addr2	varchar	255		ที่อยู่ของผู้ใช้บริการ
rad_id	int	11		ไอดีที่เชื่อมไปยังตาราง radcheck

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

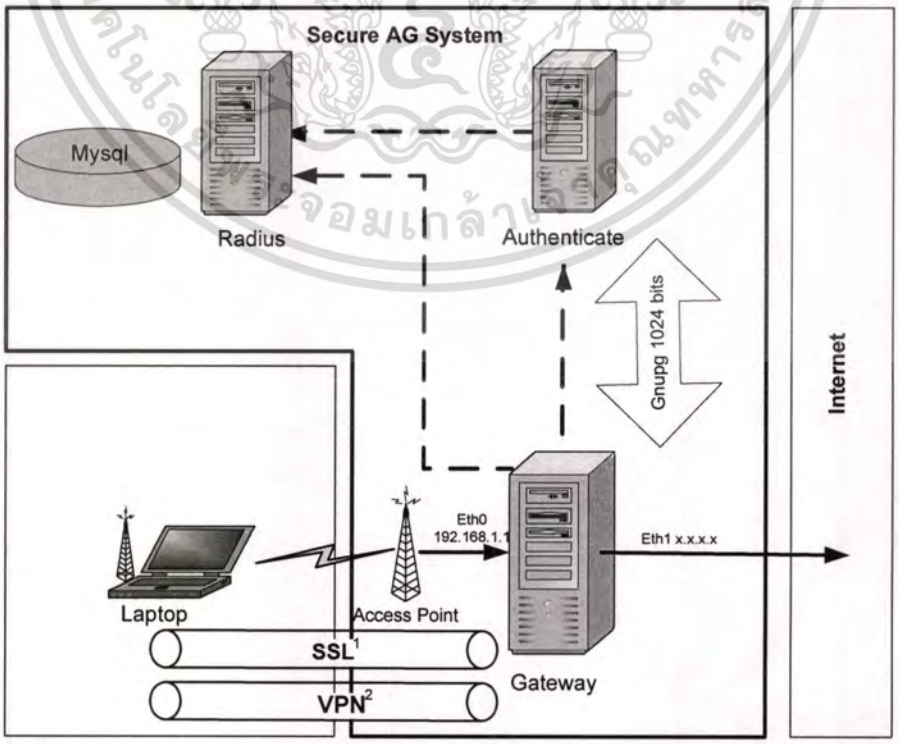
บทที่ 4
การสร้างระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

ในระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงนั้นมีการทำงานอยู่ 2 ส่วนหลัก ๆ คือ ส่วนที่หนึ่งเป็นระบบ VPN จะใช้ซอฟท์แวร์ OpenVPN ในการทำงานและส่วนที่สองเป็นระบบพิสูจน์ตัวจริง โดยภายในระบบพิสูจน์ตัวจริงยังมีการทำงานของระบบย่อย ๆ อีก 3 ส่วนคือ

- ระบบเกตเวย์ ทำหน้าที่เปิด-ปิดการให้บริการแก่ผู้ใช้งาน
- ระบบพิสูจน์ตัวจริง ทำหน้าที่พิสูจน์ตัวจริงของผู้ใช้งาน
- ระบบแอคเค้าท์ติ่ง ทำหน้าที่ติดต่อระบบฐานข้อมูล ในการทำการพิสูจน์ตัวจริงและทำในเรื่องของแอคเค้าท์ติ้ง

โดยการทำงานของระบบย่อยทั้ง 3 ส่วนจะมีการใช้ซอฟท์แวร์ 2 ตัว คือ ซอฟท์แวร์ NoCat สำหรับทำในส่วนที่เป็นระบบเกตเวย์และระบบพิสูจน์ตัวจริง และใช้ซอฟท์แวร์ Freeradius สำหรับทำการระบบแอคเค้าท์ติ่ง และใช้ซอฟท์แวร์ MySQL เป็นระบบฐานข้อมูล

ซึ่งการทำงานของระบบทั้งหมดจะมีการติดตั้งไว้ภายในเครื่อง ๆ เดียวกัน โดยการสร้างระบบจะต้องมีการเพิ่มและแก้ไขการทำงานของแต่ละซอฟท์แวร์ เพื่อให้สามารถใช้งานร่วมกันได้



รูปที่ 4.1 แสดงภาพ ของการทำการระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1 อุปกรณ์และเครื่องมือที่ต้องใช้

4.1.1 ซอฟต์แวร์

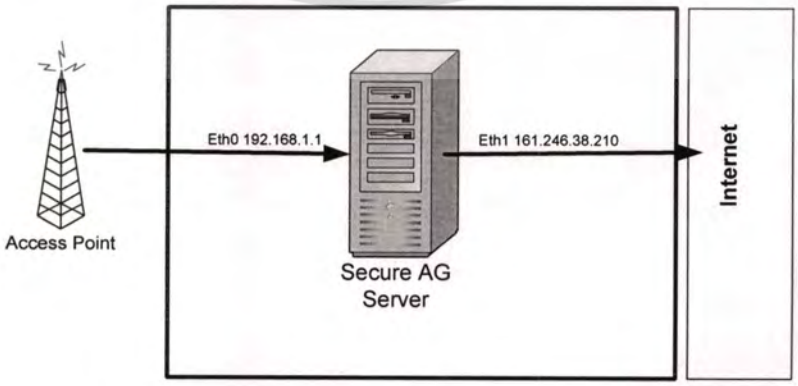
- เซิร์ฟเวอร์ ใช้ระบบปฏิบัติการ Linux RedHat 9.0
-เครื่องมือระบบ VPN ใช้ OpenVPN-2.0_beta10.tar.gz
- เครื่องมือการพิสูจน์ตัวจริงและเกตเวย์ ใช้ NoCatAuth-0.82.tar.gz
- เครื่องมือการเข้ารหัสข้อมูลใช้ gnupg-1.2.1-3
- เครื่องมือการในการทำ NAT ใช้ iptables 1.2.7a-2
- เครื่องมือการในการแจกไอพีอัตโนมัติ ใช้ Dhcp 3.0pl1-23
- เว็บเซิร์ฟเวอร์และการเข้ารหัสความปลอดภัยใช้โปรแกรม Apache-2.0.40-21+mod_ssl-2.0.40-21
- ภาษาที่ใช้ในการพัฒนาแอพพลิเคชั่นใช้ Perl 5.8.0-88
-เครื่องมือระบบเรเดียส ใช้ Freeradius-1.0.tar.gz
- ดาต้าเบสของระบบ ใช้ MySQL 3.23.54a

4.1.2 ฮาร์ดแวร์

- เครื่องคอมพิวเตอร์ที่ประกอบด้วยฮาร์ดแวร์ CPU Intel Pentium 4 2.4 GHz หน่วยความจำ 256 MB ฮาร์ดดิสก์ 20 GB
- การ์ดแลน 10/100 2 ใบ

4.2 ขั้นตอนการติดตั้ง

เมื่อติดตั้ง linux redhat 9 แล้วให้ทำการตรวจสอบการให้บริการ Service เหล่านี้ httpd dhcpd iptables ipchains mysqld และ radiusd แล้วทำการกำหนดค่า IP Address ดังรูปที่ 4.2



รูปที่ 4.2 แสดงภาพ การทำหนด IP Address eth1 และ eth0

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

DEVICE=eth0	DEVICE=eth1
BOOTPROTO=static	BOOTPROTO=static
BROADCAST=192.168.1.255	BROADCAST=161.246.38.255
IPADDR=192.168.1.1	IPADDR=161.246.38.210
NETMASK=255.255.255.0	NETMASK=255.255.255.0
NETWORK=192.168.1.0	NETWORK=161.246.38.0
ONBOOT=yes	ONBOOT=yes

4.2.1 การกำหนด DHCP ให้กับเครื่องลูกข่าย

เป็นการกำหนด IP Address ให้กับเครื่องลูกข่ายอัตโนมัติ โดยที่เครื่องลูกข่ายจะทำการร้องขอจาก DHCP Server ที่ให้บริการ ในการตั้งค่านั้นทำโดยการสร้างไฟล์ /etc/dhcpd.conf (ค่าต่าง ๆ สามารถดูได้ในภาคผนวก)

หลังจากนั้น เริ่มการทำงานของ DHCP ด้วยคำสั่ง

#/etc/rc.d/init.d/dhcp start

ตรวจสอบค่าให้ DHCP ทำงานโดยอัตโนมัติโดยพิมพ์คำสั่ง setup แล้วทำเครื่องหมายหน้า dhcpd แล้วทำการ Reboot เครื่องคอมพิวเตอร์ใหม่

4.2.2 ขั้นตอนการติดตั้ง NoCatAuth

ในการติดตั้งซอฟต์แวร์ทั้งหมดให้ทำสำเนามาไว้ในห้อง /usr/local/src ในการติดตั้งซอฟต์แวร์ NoCatAuth ในบทนี้ต้องการสร้างการพิสูจน์ตัวจริงและเกตเวย์ อยู่ในคอมพิวเตอร์เครื่องเดียวกันจึงมีขั้นตอนการติดตั้งดังนี้

ก่อนที่จะติดตั้ง NoCatAuth ควรจะต้องทำการติดตั้ง Net-Netmask-1.9004

#tar xzvf Net-Netmask-1.9004.tar.gz

#cd Net-Netmask-1.9004

#perl MakeFile.pl

#make

#make install

หลังจากนั้นเริ่มทำการติดตั้ง NoCatAuth

tar xfvz NoCatAuth-0.82.tar.gz

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

cd NoCatAuth-0.82

make PREFIX=/usr/local/nocat/gw gateway

make PREFIX=/usr/local/nocat authserv

make PREFIX=/usr/local/nocat pgpkey

cp /usr/local/nocat/trustedkeys.gpg /usr/local/nocat/pgp

cp /usr/local/nocat/trustedkeys.gpg /usr/local/nocat/gateway/pgp

chown –R apache:apache /usr/local/nocat/pgp

chown –R apache:apache /usr/local/nocat/pgp/*

chown –R apache:apache /usr/local/nocat/gw/pgp

chown –R apache:apache /usr/local/nocat/gw/pgp/*

ตรวจสอบการทำงานของ NoCatAuth ใช้คำสั่งดังนี้

cd /usr/local/nocat

vi nocat.conf

bin/gateway

[2004-01-12 17:35:13] Resetting firewall.

[2004-01-12 17:35:13] Detected InternalDevice 'eth0'

[2004-01-12 17:35:13] Detected ExternalDevice 'eth1'

[2004-01-12 17:35:13] Detected LocalNetwork '192.168.1.0/255.255.255.0'

[2004-01-12 17:35:15] Binding listener socket to 0.0.0.0

การตั้งค่าอัตโนมัติเมื่อทำการเปิดระบบปฏิบัติการลินุกซ์ NoCatAuth จะทำงานไปพร้อมกันตอนทำการเปิดระบบ

#cp /usr/local/src/ NoCatAuth-0.82/etc/nocat.rc /etc/rc.d/init.d/nocat

vi /etc/rc.d/nocat

ทำการแก้ไขไฟล์ดังนี้ NC=/usr/local/nocat/gateway แล้วทำการบันทึก

ln -s /etc/rc.d/init.d/nocat.rc /etc/rc.d/rc3.d/S99nocat

หรือ ใน Mode Graph

ln -s /etc/rc.d/init.d/nocat.rc /etc/rc.d/rc5.d/S99nocat

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ขั้นต่อไปทำการ แก้ไขไฟล์ /usr/local/nocat/nocat.conf และ /usr/local/nocat/gw/nocat.conf โดยรายละเอียดของค่าต่าง ๆ สามารถดูได้ที่ภาคผนวก รายละเอียดสามารถดูได้ที่ภาคผนวก

4.2.3 ขั้นตอนการติดตั้งฐานข้อมูล MySQL

โดยการจัดเก็บฐานข้อมูลลงบน MySQL ด้วยคำสั่ง # mysql nocat < /etc/nocat.schema ในห้องที่ทำการแตกไฟล์ต้นฉบับ NoCatAuth-0.82

4.2.4 ขั้นตอนการติดตั้ง Freeradius

การติดตั้งโปรแกรม Freeradius เพื่อที่จะใช้ในการเชื่อมต่อระหว่างระบบพิสูจน์ตัวจริงและเกตเวย์กับระบบฐานข้อมูล โดยขั้นตอนการติดตั้งมีดังนี้

#tar -xzvf freeradius.tar.gz

#cd freeradius

#./configure

#make

#make install

จากนั้น ให้ทำการแก้ไขไฟล์ดังนี้/usr/local/etc/raddb/clients.conf , /usr/local/etc/raddb/realms, /usr/local/etc/raddb/sql.conf และ /usr/local/etc/raddb/radiusd.conf (โดยละเอียดสามารถดูได้ที่ภาคผนวก)

หลังจากนั้นให้ทำการคอนฟิกให้โปรแกรม Freeradius ใช้ข้อมูลจากระบบฐานข้อมูลของโปรแกรม MySQL

#mysql

mysql>CREATE DATABASE radius;

#mysql -uroot radius < /root/freeradius/src/modules/rlm_sql/drivers/rlm_sql_mysql/db_mysql.sql

4.2.5 ขั้นตอนการติดตั้ง iptables

ใน Linux RedHat 9 นั้นมี Iptables มาให้แล้ว ใช้คำสั่งตรวจสอบ # iptables -L

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

โดยไม่ต้องกำหนดค่านี้ echo "1"> /proc/sys/net/ipv4/ip_forward เมื่อ NoCatAuth ทำงาน จะทำการกำหนด Firewall rule และ echo "1"> /proc/sys/net/ipv4/ip_forward ให้อัตโนมัติ

เมื่อได้ติดตั้งเสร็จเรียบร้อยแล้ว ทำการตรวจสอบ # iptables –L จะได้ค่าดังนี้

```
[root@authen root]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
NoCat      all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain NoCat (1 references)
target          prot opt source           destination
NoCat_Ports     all  --  anywhere         anywhere
NoCat_Inbound   all  --  anywhere         anywhere
ACCEPT          all  --  192.168.0.0/24   anywhere        MARK match 0x1
ACCEPT          all  --  192.168.0.0/24   anywhere        MARK match 0x2
ACCEPT          all  --  192.168.0.0/24   anywhere        MARK match 0x3
ACCEPT          tcp  --  192.168.0.0/24        192.168.0.1          tcp dpt:http
ACCEPT          tcp  --  192.168.0.1           192.168.0.0/24       tcp spt:http
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
ACCEPT     tcp  --  192.168.0.0/24          192.168.0.1          tcp dpt:https
ACCEPT     tcp  --  192.168.0.1            192.168.0.0/24       tcp spt:https
ACCEPT     all  --  platinum.it.kmitl.ac.th  192.168.0.0/24
ACCEPT     tcp  --  192.168.0.0/24     platinum.it.kmitl.ac.thtcp dpt:domain
ACCEPT     udp  --  192.168.0.0/24     platinum.it.kmitl.ac.thudp dpt:domain
DROP       tcp  -- !192.168.0.1        anywhere        tcp dpt:5280
DROP       all  --  anywhere           anywhere

Chain NoCat_Inbound (1 references)
target     prot opt source          destination
Chain NoCat_Ports (1 references)
target     prot opt source          destination
DROP       tcp  --  anywhere        anywhere        tcp dpt:smtp MARK match 0x3
DROP       udp  --  anywhere        anywhere        udp dpt:smtp MARK match 0x3
```

4.2.6 ขั้นตอนการติดตั้ง Apache กับ mod_ssl

apache ทำหน้าที่ให้บริการเวบเซอร์เวอร์ ส่วน mod_ssl เป็นเครื่องมือรักษาความปลอดภัยระหว่างเบราเซอร์กับเครื่องแม่ข่ายเวบ ทำการเข้ารหัสรักษาความปลอดภัย 128 บิต ส่วนใน ลีนุกซ์ RedHat 9 นั้นมี Apache กับ mod_ssl อยู่แล้ว ให้ทำการเปิดไฟล์ /etc/httpd/conf/httpd.conf ทำการเพิ่มคำสั่งนี้ Include /usr/local/nocat/httpd.conf แล้วทำการบันทึก Restart httpd ใหม่เพื่อให้ระบบทำงานด้วยคำสั่ง # /etc/rc.d/init.d/httpd restart

4.2.7 ขั้นตอนการติดตั้ง OpenVPN

สำหรับการติดตั้งโปรแกรม OpenVPN เพื่อที่จะสร้างระบบ VPN ขึ้น โดยการติดตั้งระบบ VPN จะแบ่งเป็น 2 ส่วนคือ ส่วนที่ใช้สำหรับเครื่องแม่ข่าย และส่วนที่ใช้สำหรับเครื่องลูกข่ายหรือเครื่องผู้ใช้ โดยขั้นตอนการติดตั้งมีดังนี้

```
#tar -xzvf openvpn-2.0_beta10.tar.gz
#cd openvpn-2.0_beta10
#./configure
#make
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#make install

หลังจากนั้นให้ทำการแก้ไขไฟล์ /usr/share/ssl/openssl.cnf โดยรายละเอียดสามารถดูได้ที่ภาคผนวก และทำขั้นตอนการติดตั้งต่อไป

#mkdir /etc/ssl

#mkdir /etc/ssl/private

#mkdir /etc/ssl/newcerts

#mkdir /etc/ssl/certs

#cd /etc/ssl

#touch index.txt

#echo "01" > serial

#openssl req -nodes -new -x509 -keyout ./private/my-ca.key -out my-ca.crt -days 3650

#openssl req -nodes -new -keyout server.key -out server.csr

#openssl ca -out server.crt -in server.csr

#cp /etc/ssl/server.key /etc/ssl/private

#cp /etc/ssl/my-ca.key /etc/ssl/private

#cp /etc/ssl/server.crt /etc/ssl/certs

#openssl req -nodes -new -keyout client.key -out client.csr

#openssl ca -out client.crt -in client.csr

#openssl dhparam -out dh1024.pem 1024

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

การพัฒนาระบบ

5.1 ซอฟต์แวร์ที่ใช้ในส่วนของการพัฒนาระบบ มีดังนี้

- ภาษาที่ใช้ในการพัฒนาระบบใช้ Php 4.2.2-17
- ภาษาที่ใช้ในการพัฒนาระบบใช้ Perl 5.8.0-88
- ภาษาที่ใช้ในการพัฒนาระบบใช้ Shell Scripts
- ดาต้าเบสของระบบ ใช้ MySQL 3.23.54a
- เครื่องการจัดการระบบฐานข้อมูลแบบ GUI PhpMyAdmin-2.5.7-pl
- Editor Coding Program ใช้ Edits Plus 2.1c
- โปรแกรมบราวเซอร์ ใช้ Internet Explorer 6.0

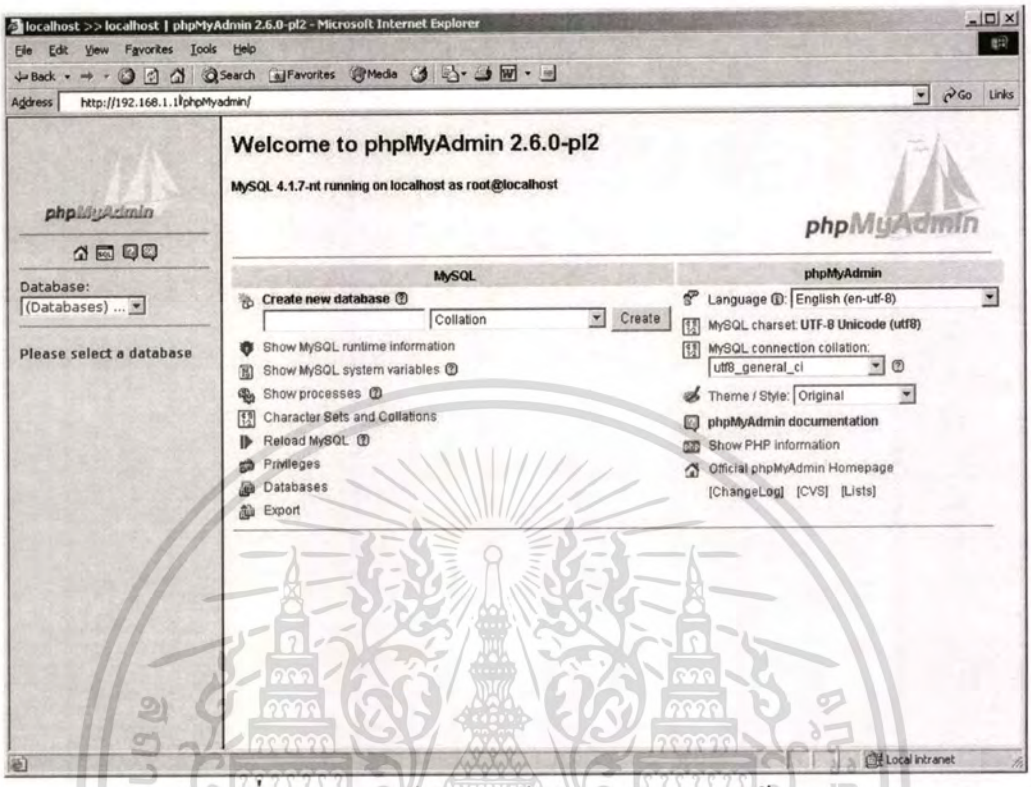
5.2 การติดตั้งซอฟต์แวร์สำหรับจัดการระบบดาต้าเบสแบบ GUI PhpMyAdmin

ทำการติดตั้ง phpMyadmin-2.5.7-pl ด้วยขั้นตอนดังนี้

- ทำการดาวน์โหลดซอฟท์แวร์ที่
- #tar -xzvf phpMyAdmin-2.5.7-pl.tar.gz
- #mv phpMyAdmin-2.5.7-pl phpMyAdmin
- #cp phpMyAdmin /var/www/html
- เปลี่ยนแปลงค่าคอนฟิกในไฟล์ phpMyAdmin ดังนี้
    - $cfgPmaAbsoluteUri='http://192.168.1.1/phpMyadmin/
    - $cfg['Servers'][$i]['auth_type'] = 'http';
    - $cfg['Servers'][$i]['user'] = '<กำหนด UserName ในการเข้าระบบ>';
    - $cfg['Servers'][$i]['password'] = '<กำหนด Password ในการเข้าระบบ>';

เมื่อระบบติดตั้งเสร็จเรียบร้อยแล้ว สามารถที่จะเข้าสู่ระบบจัดการระบบฐานข้อมูลได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



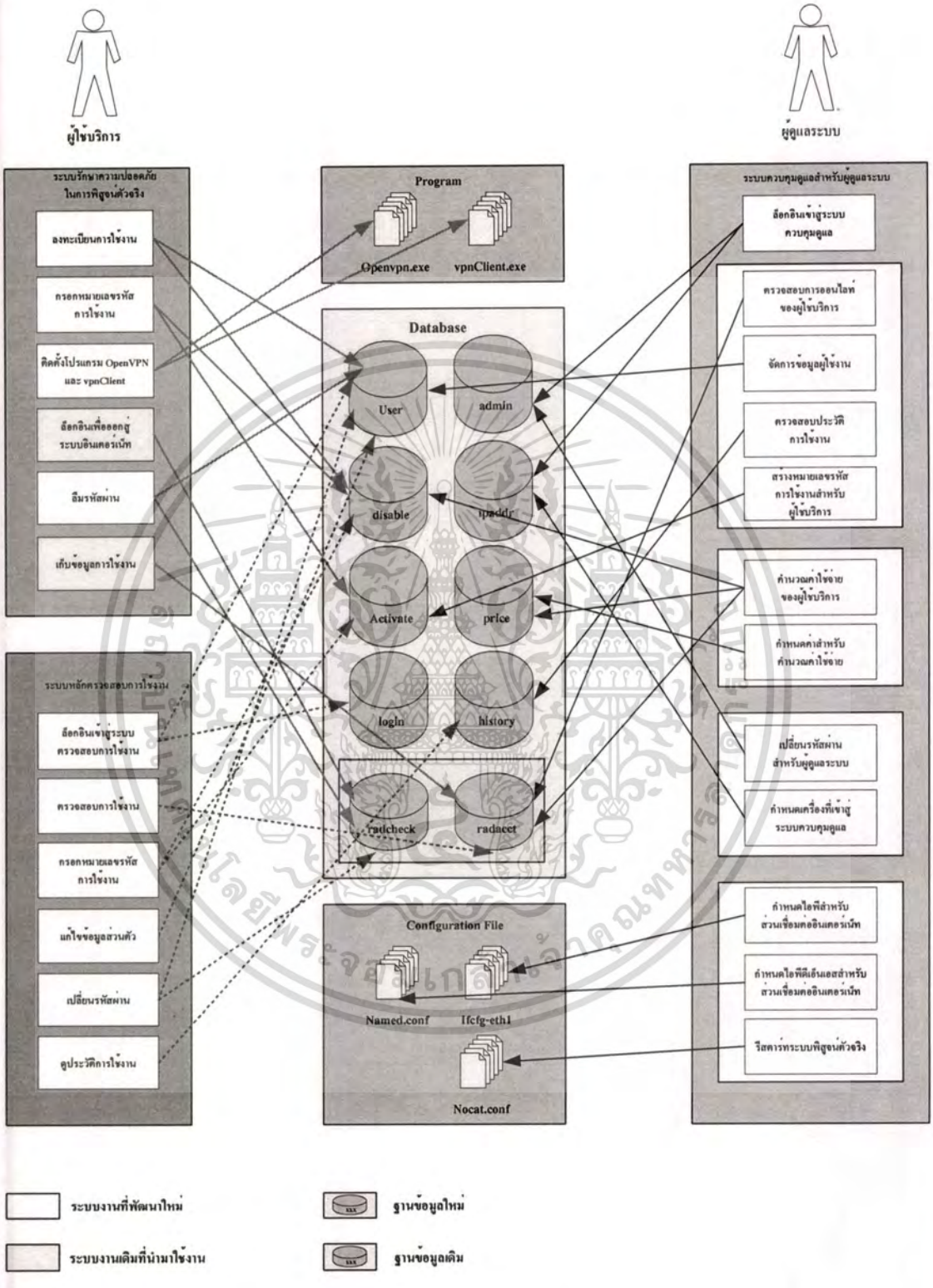
รูปที่ 5.1 แสดงหน้าจอการเข้าสู่ระบบจัดการฐานข้อมูล

หลังจากที่ดำเนินการติดตั้งติดตั้งระบบจัดการฐานข้อมูลเรียบร้อยแล้ว ก็เริ่มดำเนินการพัฒนาระบบ โดยในหัวข้อถัดไปจะเป็นโครงสร้างของระบบที่จะดำเนินการพัฒนา

5.3 โครงสร้างและการพัฒนาระบบ

โครงสร้างการทำงานของระบบทั้งหมดที่จะทำการพัฒนา สามารถดูได้จากรูปที่ 5.2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 5.2 แสดงการทำงานและการพัฒนาระบบงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากโครงสร้างของการพัฒนาระบบ จะเห็นได้ว่าในส่วนของการพัฒนาระบบจะมีการแบ่งออกเป็น 2 ส่วนคือ ส่วนที่มีการดำเนินการพัฒนาระบบขึ้นมาใหม่ กับส่วนที่นำระบบเดิมมาพัฒนา จากรูปข้างต้นในส่วนที่นำระบบเดิมมาพัฒนาจะมีอยู่ 2 ส่วนการทำงานคือการทำงานของระบบที่ใช้ในการตรวจสอบเพื่อเข้าสู่ระบบและการเก็บข้อมูลการใช้งานของระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง นอกนั้นจะเป็นส่วนที่มีการดำเนินการพัฒนาระบบใหม่ ซึ่งในส่วนที่มีการดำเนินการพัฒนาระบบขึ้นมาใหม่นั้น จะมีการใช้ภาษา PHP ซึ่งครอบคลุมการทำงานของระบบทั้ง 3 ระบบคือ ระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ และระบบควบคุมดูแลสำหรับผู้ดูแลระบบ โดยในการพัฒนาระบบนั้น ได้มีการใช้งานฐานข้อมูล 2 ส่วนคือส่วนของฐานข้อมูลของระบบเดิมคือตาราง radcheck และตาราง radacct และส่วนของฐานข้อมูลใหม่ ซึ่งมีจำนวน 8 ตาราง ตามรูปข้างต้น นอกจากนี้ยังมีส่วนของไฟล์คอนฟิกของระบบที่นำมาใช้ในการพัฒนาระบบ ซึ่งมีไฟล์หลัก คือไฟล์ named.conf สำหรับส่วนของการคอนฟิกระบบดีเอ็นเอส และไฟล์ ifcfg-eth1 สำหรับส่วนของการตั้งค่าหมายเลขไอพีของระบบนั่นเอง

ต่อไปจะมีการกล่าวถึงรายละเอียดในการพัฒนาระบบแต่ละระบบภายในโครงงานนี้

5.3.1 การพัฒนาระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

การพัฒนาระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง ได้ดำเนินการพัฒนาตามที่ได้วิเคราะห์และออกแบบไว้ในเนื้อหาของบทที่ 3 โดยการพัฒนาระบบนี้ เริ่มจากการดำเนินการติดตั้งซอฟท์แวร์ของระบบซึ่งวิธีการติดตั้งได้มีการกล่าวไปในเนื้อหาของบทที่ 4 การปรับปรุงระบบบางส่วนเพื่อให้มีประสิทธิภาพในการทำงานมากขึ้นเช่นส่วนการปรับปรุงระบบการตรวจสอบการเข้าสู่ระบบพิสูจน์ตัวจริงให้สามารถใช้งานร่วมกับการใช้โปรแกรม OpenVPN และ vpnClient ในการเข้าสู่ระบบ VPN โดยทำการเพิ่มเติมการทำงานบางส่วนเข้าไปในไฟล์ที่ใช้สำหรับตรวจสอบการเข้าใช้งานของผู้ใช้บริการ โดยส่วนที่เพิ่มเติมสามารถจะดูในภาคผนวก และส่วนที่ดำเนินการพัฒนาการทำงานขึ้นมาใหม่ โดยใช้ภาษา Php, Perl และ Shell Script ในการพัฒนา และใช้ฐานข้อมูล MySQL

5.3.2 การพัฒนาระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

การพัฒนาระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ ได้ดำเนินการพัฒนาตามที่ได้วิเคราะห์และออกแบบไว้ในบทที่ 3 ซึ่งระบบทั้งหมดถูกพัฒนาขึ้นมาใหม่ โดยใช้ภาษา Php ในการพัฒนา และใช้ฐานข้อมูล MySQL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.3.3 การพัฒนาระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

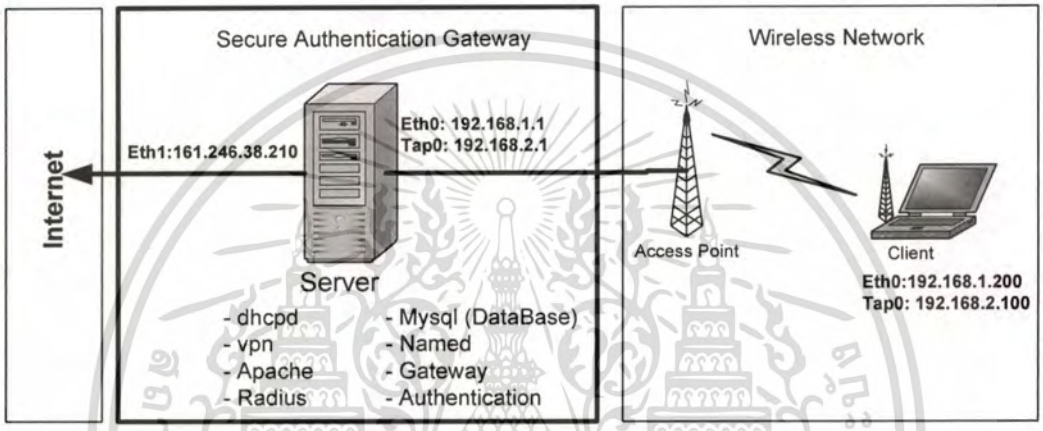
การพัฒนาระบบควบคุมดูแลสำหรับผู้ดูแลระบบ ได้ดำเนินการพัฒนาตามที่ได้วิเคราะห์และออกแบบไว้ในบทที่ 3 ซึ่งระบบทั้งหมดถูกพัฒนาขึ้นมาใหม่ โดยใช้ภาษา Php ในการพัฒนาและใช้ฐานข้อมูล MySQL นอกจากนี้ยังมีส่วนที่ต้องทำการตั้งค่าเพิ่มสำหรับส่วนของคอนฟิกกรูเรชั่นที่จะต้องทำการอ่านไฟล์ค่าคอนฟิกของระบบ โดยส่วนที่ทำการตั้งค่าเพิ่มนั้นสามารถดูรายละเอียดได้ในภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 6

ผลการทดลอง

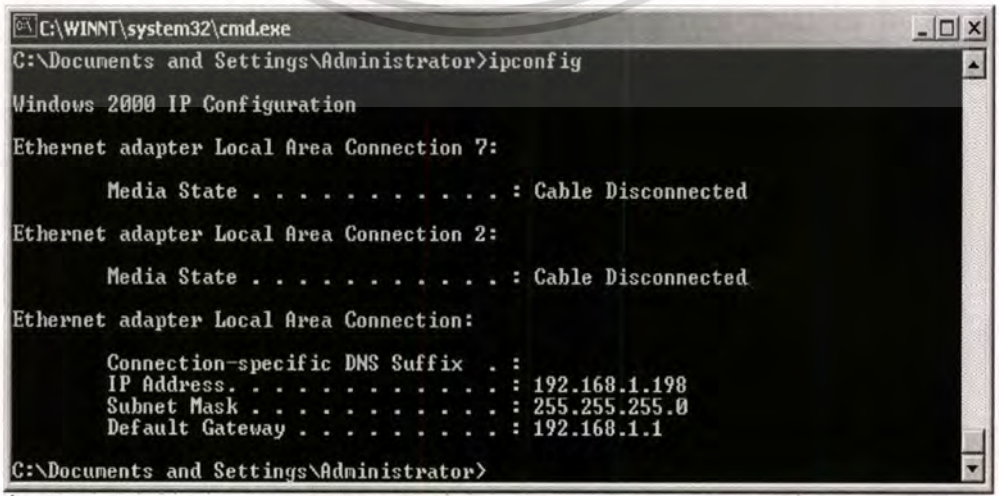
เนื้อหาในบทนี้จะกล่าวถึง การทดสอบการใช้งานโครงงานพัฒนาระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง รายละเอียดการทดสอบใช้งานนำเสนอดังนี้



รูปที่ 6.1 แสดงภาพการทดสอบโครงงานพัฒนาระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

6.1 การทดสอบการใช้งานระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

ผู้ใช้บริการเริ่มดำเนินการใช้งาน โดยการเชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่ายไวร์เลสแลนด์ เมื่อผู้ใช้บริการได้ทำการเชื่อมต่อเข้าสู่ระบบเครือข่ายไวร์เลสแลนของระบบเรียบร้อยแล้วจะได้รับหมายเลขไอพี ตามรูปที่ 6.2



รูปที่ 6.2 แสดงหน้าจอหมายเลขไอพีที่ผู้ใช้บริการได้รับเมื่อเข้าสู่เครือข่ายไวร์เลสแลนของระบบ

เอกสารนี้สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปจะเห็นได้ว่าเครื่องผู้ใช้บริการจะได้รับหมายเลขไอพีเบอร์ 192.168.1.198/24 และหมายเลขไอพีของเกต์เวย์เบอร์ 192.168.1.1 โดยหมายเลขไอพีที่ผู้ใช้บริการจะได้รับจะอยู่ในช่วงของ 192.168.1.100 – 192.168.1.200 /24

หลังจากนั้นทำการทดสอบการออกสู่ระบบอินเตอร์เน็ท หน้าจอของผู้ใช้บริการจะถูกรีไดเร็คมายังหน้าจอที่ให้ทำการดาวน์โหลดโปรแกรมเพื่อเชื่อมต่อกับระบบ VPN และให้ทำการลงทะเบียนในกรณีที่ผู้ใช้บริการได้เริ่มใช้บริการในระบบนี้เป็นครั้งแรกผ่าน HTTPS โดยจะมีหน้าจอดังรูปที่ 6.3

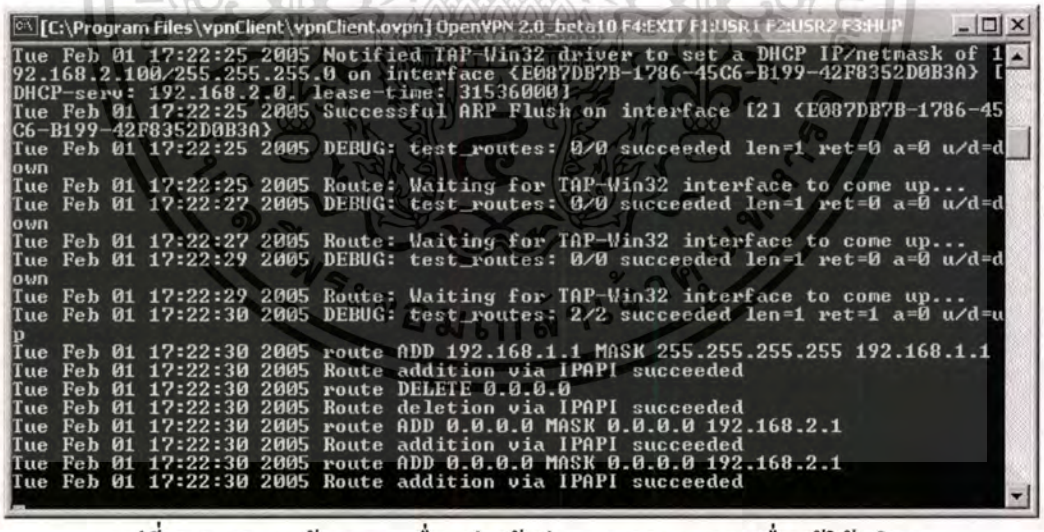
รูปที่ 6.3 แสดงหน้าจอการเข้าสู่ระบบเพื่อทำการดาวน์โหลดโปรแกรมสำหรับเชื่อมต่อระบบ VPN และการลงทะเบียน

โดยเมื่อผู้ใช้ได้ทำการดาวน์โหลดและลงทะเบียนเรียบร้อยแล้ว ผู้ใช้บริการได้ทำการขอหมายเลขรหัสการใช้งานจากผู้ดูแลระบบ และได้ทำการกรอกหมายเลขรหัสการใช้งานในหน้าจอที่ 6.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 6.4 แสดงหน้าจอระบบกรอกหมายเลขรหัสการใช้งาน

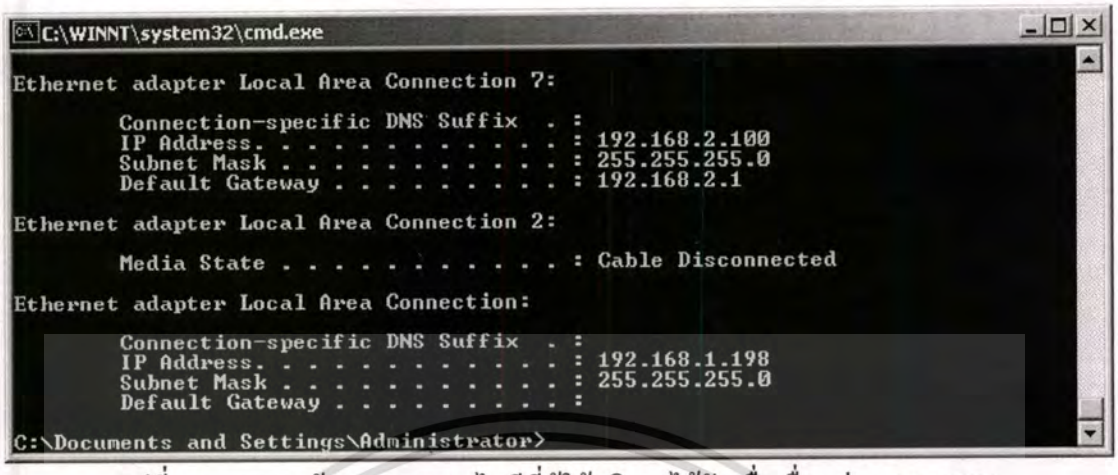
หลังจากการกรอกหมายเลขรหัสการใช้งานผ่านเรียบร้อยแล้ว ผู้ใช้บริการได้ทำการเชื่อมต่อเข้าสู่ระบบ VPN โดยจะปรากฏหน้าจอดังรูปที่ 6.5 และได้รับหมายเลขไอพีอีกชุดหนึ่ง ตามรูปที่ 6.6 หลังจากนั้นผู้ใช้บริการได้ทำการทดสอบการออกสู่อินเตอร์เน็ทอีกครั้ง ซึ่งผลที่ได้คือหน้าจอของผู้ใช้บริการจะถูกรีไดเร็กไปยังเว็บเพจที่ระบบกำหนดไว้เพื่อให้ทำการล็อกอินอีกครั้ง โดยหน้าจอของระบบจะเป็นไปตามรูปที่ 6.7



รูปที่ 6.5 แสดงหน้าจอการเชื่อมต่อเข้าสู่ระบบ VPN ของเครื่องผู้ใช้บริการ

เมื่อผู้ใช้ได้ทำการเชื่อมต่อแล้วจะได้รับหมายเลขไอพีชุดใหม่มาอีกชุด โดยเป็นหมายเลขไอพีที่ใช้ในการเชื่อมต่อเพื่อออกสู่ระบบอินเตอร์เน็ทเท่านั้น โดยจะเห็นได้จากรูที่ 6.15

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.6 แสดงหน้าจอหมายเลขไอพีที่ผู้ใช้บริการได้รับเมื่อเชื่อมต่อระบบ VPN

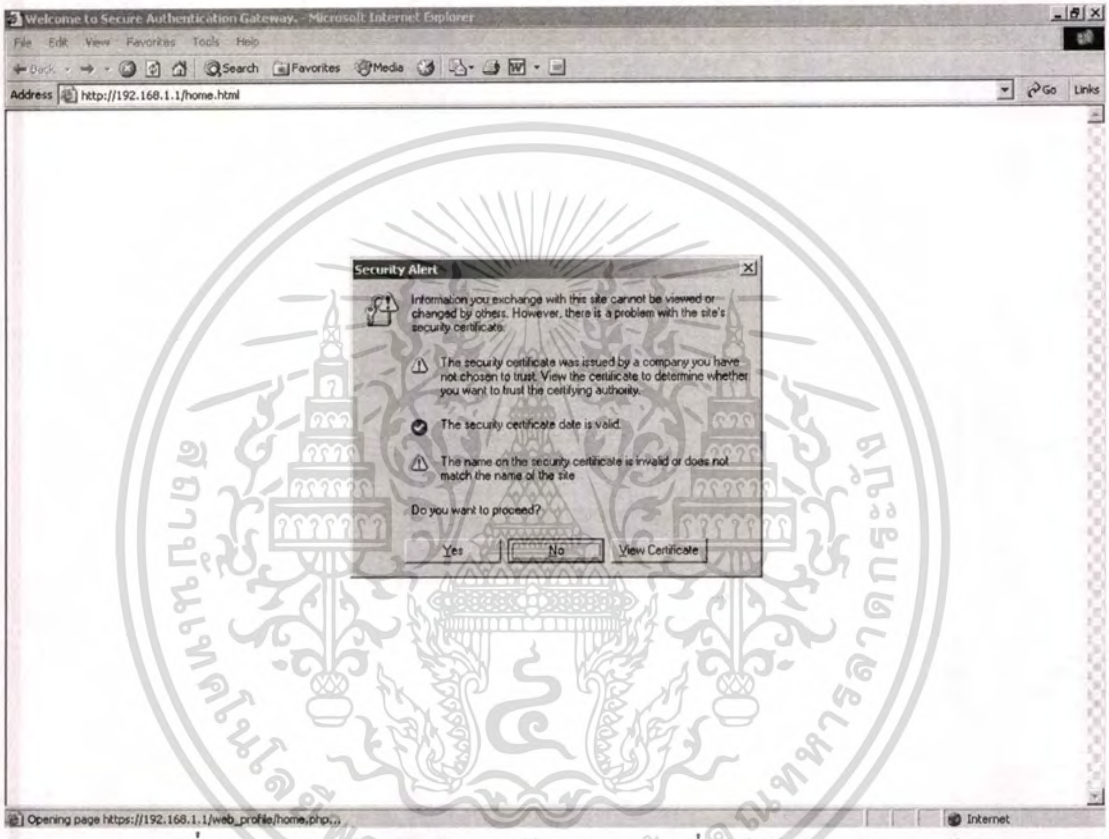
รูปที่ 6.7 แสดงหน้าจอการล็อกอินเข้าสู่ระบบ

โดยเมื่อผู้ใช้บริการได้ทำการกรอกรหัสล็อกอินและรหัสผ่านถูกต้องก็สามารถออกสู่อินเตอร์เน็ทได้อย่างสมบูรณ์ โดยข้อมูลการใช้งานของผู้ใช้จะถูกบันทึกโดยระบบ ซึ่งจะนำไปใช้ในการคำนวณค่าใช้จ่ายในการใช้งานต่อไป

เอกสารนี้ใช้เพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

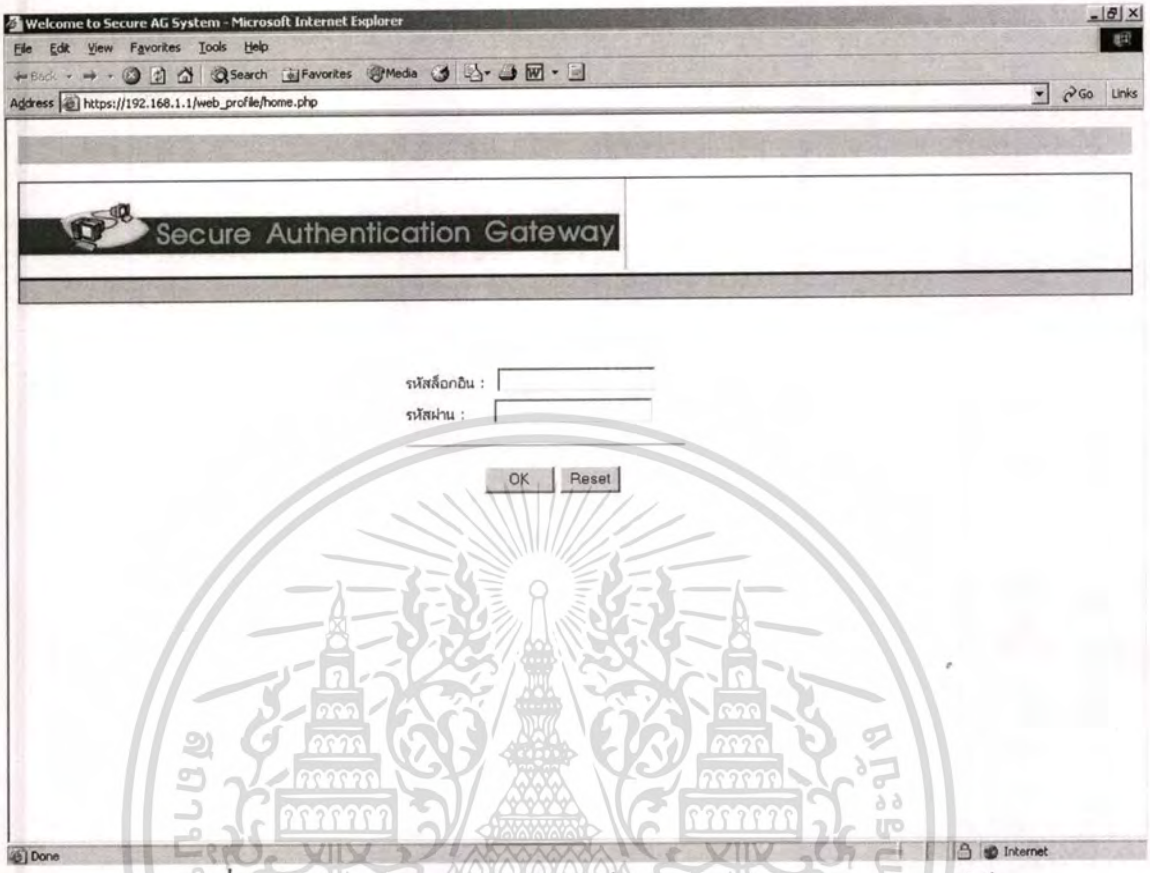
6.2 การทดสอบการใช้งานระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

สำหรับการทดสอบระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการนี้ ผู้ใช้สามารถเข้าสู่ระบบได้ที่ http://192.168.1.1/home.html โดยระบบจะรีไดเร็กไปยัง https://192.168.1.1/web_profile/home.php ซึ่งจะปรากฏหน้าจอดังรูป 6.8 และ 6.9 ตามลำดับ



รูปที่ 6.8 แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องผู้ใช้บริการในการเข้าสู่ระบบตรวจสอบการใช้งาน

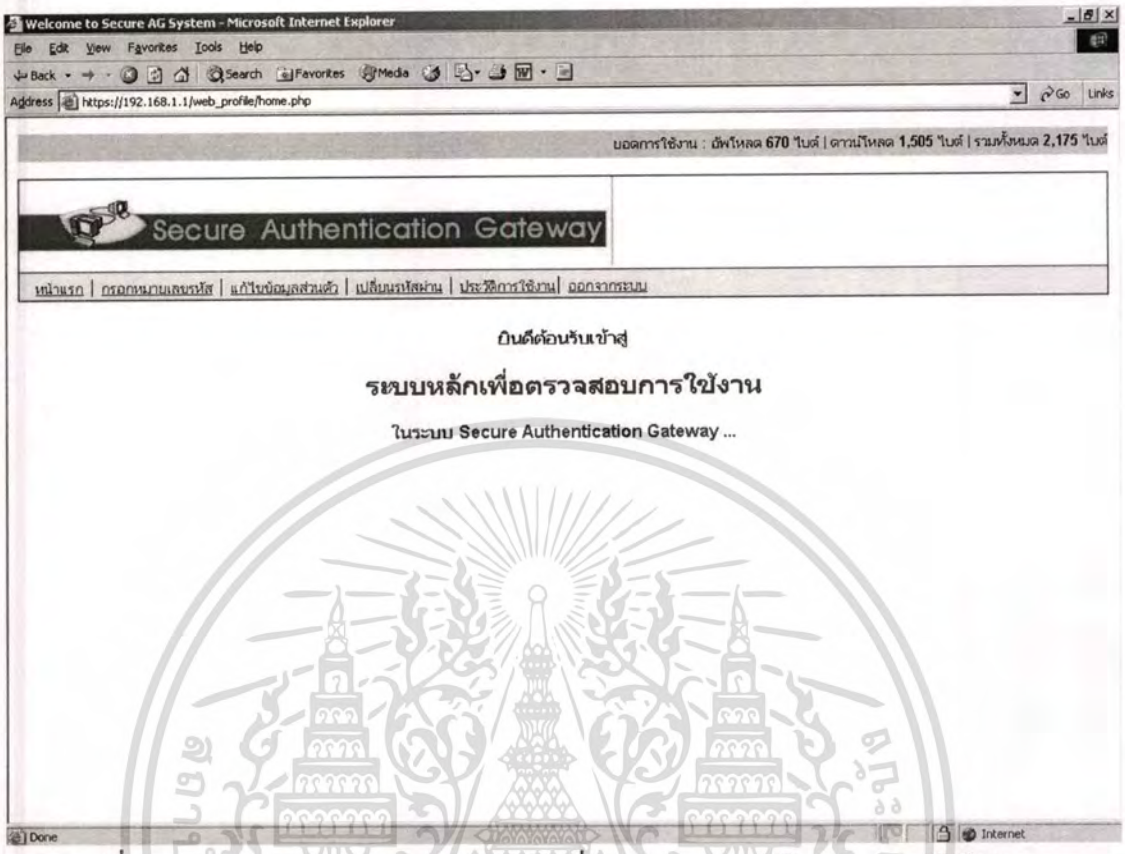
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6.9 แสดงหน้าจอการเข้าสู่ระบบล็อกอินของระบบตรวจสอบการใช้งาน

หลังจากที่ผู้ใช้บริการทำการล็อกอินเข้าสู่ระบบตรวจสอบการใช้งานได้เรียบร้อยแล้วจะปรากฏหน้าจอดังรูปที่ 6.10 ขึ้น เพื่อให้ผู้ใช้บริการสามารถที่จะทำงานภายในระบบนี้ได้ โดยการทำงานภายในระบบนี้คือ การตรวจสอบการใช้งาน โดยระบบจะมีการแสดงข้อมูลการใช้งานของผู้ใช้ ณ ขณะนั้นให้ทราบ หรือจะเป็นการแก้ไขข้อมูลส่วนตัว หรือเปลี่ยนรหัสผ่านก็สามารถทำได้อย่างสมบูรณ์ หรือจะเป็นการดูประวัติการใช้งานที่ผ่าน ๆ มาก็ทำได้อย่างสมบูรณ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



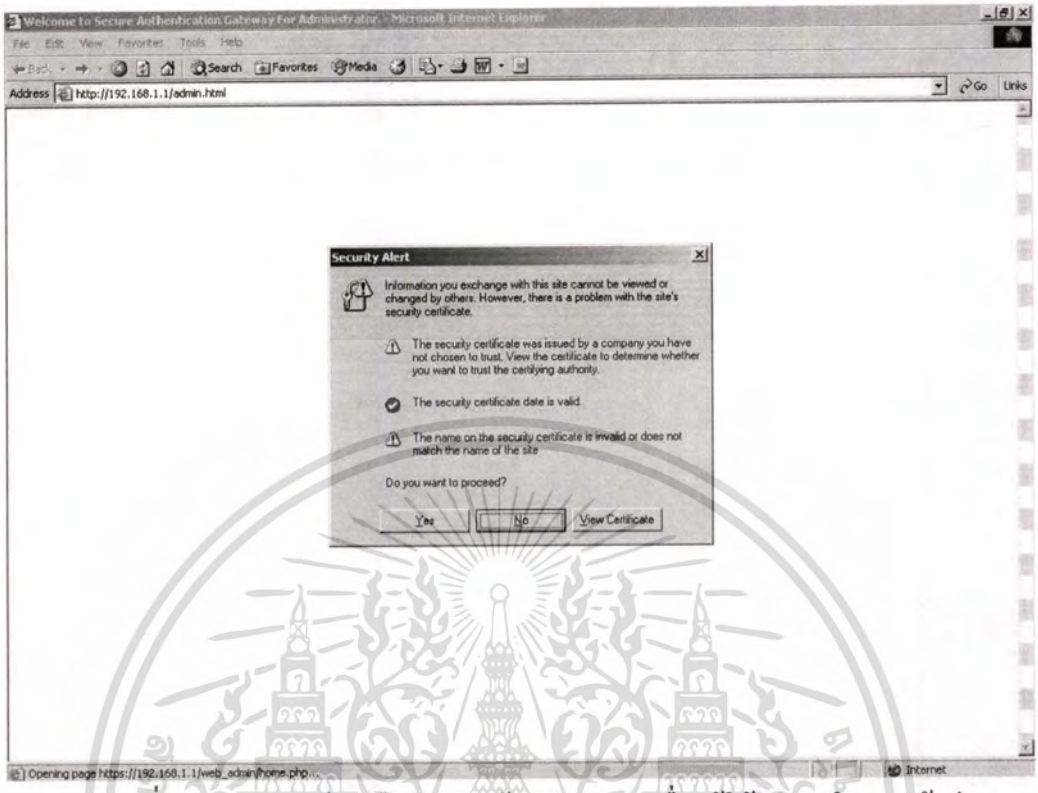
รูปที่ 6.10 แสดงหน้าจอการเข้าสู่ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

โดยเมื่อผู้ใช้บริการทำงานในระบบเรียบร้อยแล้วก็สามารถออกจากระบบได้โดยการคลิกที่เมนูออกจากระบบ

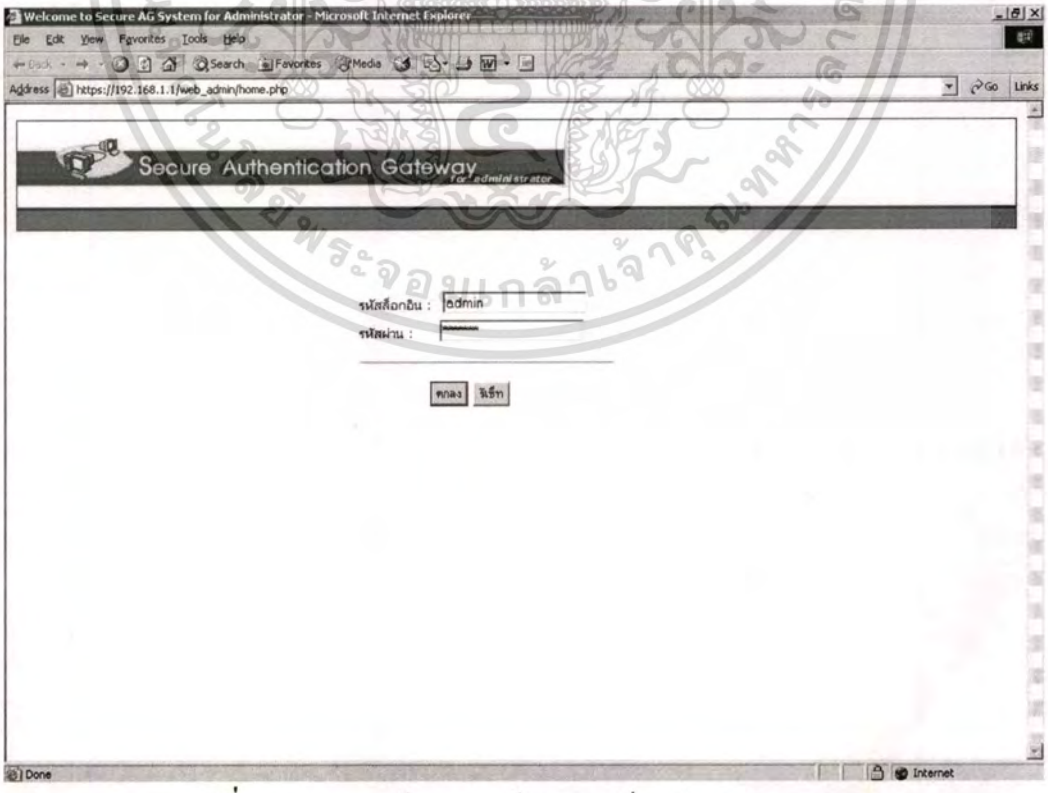
6.3 การทดสอบการใช้งานระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

สำหรับการทดสอบระบบควบคุมดูแลสำหรับผู้ดูแลระบบ ผู้ดูแลระบบสามารถเข้าสู่ระบบได้ที่ http://192.168.1.1/admin.html โดยระบบจะรีไดเร็กไปยัง https://192.168.1.1/web_admin/home.php ซึ่งจะปรากฏหน้าจอดังรูป 6.11 และ 6.12 ตามลำดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



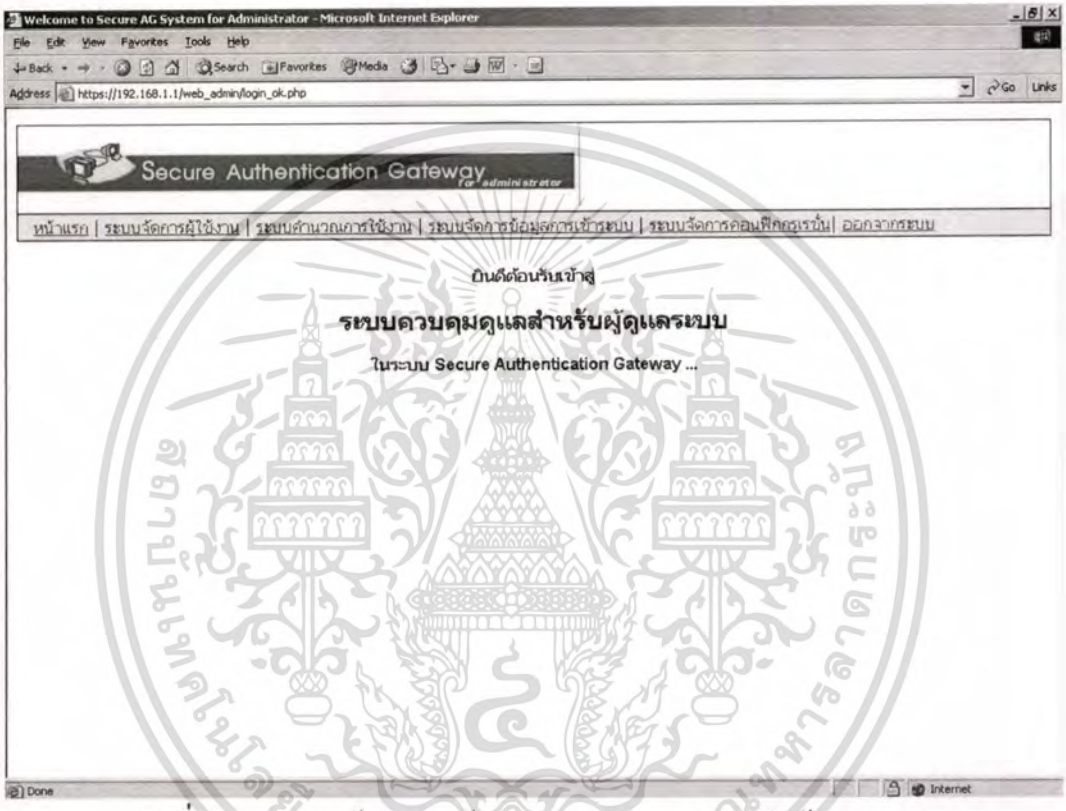
รูปที่ 6.11 แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องผู้ใช้บริการในการเข้าสู่ระบบควบคุมดูแล



รูปที่ 6.12 แสดงหน้าจอการเข้าสู่ระบบล็อกอินของระบบควบคุมดูแล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อผู้ดูแลระบบทำการกรอกรหัสล็อกอินและรหัสผ่าน ผ่านเข้าสู่ระบบได้เรียบร้อยแล้ว จะปรากฏหน้าจอดังรูปที่ 6.13 เพื่อให้ผู้ดูแลระบบสามารถเลือกที่จะทำงานได้ โดยแบ่งเป็นระบบย่อย 4 ระบบคือระบบจัดการผู้ใช้บริการ ระบบคำนวณการใช้งาน ระบบจัดการข้อมูลการเข้าสู่ระบบควบคุมดูแลและระบบจัดการคอนฟิกกรูเรชั่น



รูปที่ 6.13 แสดงหน้าจอการเข้าสู่ระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

โดยเมื่อผู้ดูแลระบบทำงานในระบบนี้เรียบร้อยแล้วก็สามารถออกจากระบบได้โดยการคลิกที่เมนูออกจากระบบ

6.4 สรุปผลการทดลองการใช้งานระบบ

จากการทดลองระบบที่ทำการพัฒนานั้น สามารถสรุปการทำงานของแต่ละระบบได้คือ

การทดลองใช้งานในระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริงนั้น มีการทำงานตามขั้นตอนที่ได้วิเคราะห์และออกแบบไว้ โดยการทำงานของระบบส่วนใหญ่จะมีการเช็คความผิดพลาดในการทำงานไว้แล้ว ทำให้การทดลองใช้งานระบบจึงไม่มีปัญหาใด ๆ โดยระบบจะมีการตรวจสอบการทำงานของผู้ใช้บริการใหม่ ให้ทำการลงทะเบียน กรอกหมายเลขรหัสการใช้งานและ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดาวน์โหลดโปรแกรมสำหรับเชื่อมต่อระบบ VPN และตรวจสอบผู้ใช้บริการเดิมให้ทำการกรอกหมายเลขรหัสการใช้งาน และทำการเชื่อมต่อเข้าสู่ระบบ VPN และให้ทำการล็อกอินก่อนออกสู่ระบบอินเตอร์เน็ท โดยผู้ใช้บริการสามารถที่จะออกจากระบบโดยการล็อกเอ้าท์ ซึ่งการทำงานของระบบทั้งหมดได้ผลดี

การทดลองใช้งานในระบบหลักเพื่อตรวจสอบการใช้งานของผู้ใช้บริการนั้น มีการทำงานตามขั้นตอนที่ได้วิเคราะห์และออกแบบไว้ โดยการทำงานของระบบส่วนใหญ่จะมีการเช็คความผิดพลาดในการทำงานไว้แล้ว ทำให้การทดลองใช้งานระบบจึงไม่มีปัญหาใด ๆ โดยระบบจะมีการตรวจสอบผู้ใช้บริการให้ทำการล็อกอินก่อนเข้าสู่ระบบ เมื่อเข้าระบบได้แล้วผู้ใช้บริการสามารถที่จะเลือกตรวจสอบการใช้งาน หรือทำงานอื่น ๆ ได้คือการกรอกหมายเลขรหัสการใช้งาน การแก้ไขข้อมูลส่วนตัว การเปลี่ยนรหัสผ่าน และการดูประวัติการใช้งาน โดยผู้ใช้บริการสามารถที่จะออกจากระบบโดยการล็อกเอ้าท์ ซึ่งการทำงานของระบบทั้งหมดได้ผลดี

การทดลองใช้งานในระบบควบคุมดูแลสำหรับผู้ดูแลระบบนั้น มีการทำงานตามขั้นตอนที่ได้วิเคราะห์และออกแบบไว้ โดยการทำงานของระบบส่วนใหญ่จะมีการเช็คความผิดพลาดในการทำงานไว้แล้ว ทำให้การทดลองใช้งานระบบจึงไม่มีปัญหาใด ๆ โดยระบบจะมีการตรวจสอบผู้ดูแลระบบให้ทำการล็อกอินก่อนเข้าสู่ระบบ และเครื่องที่ผู้ดูแลระบบใช้เข้าระบบว่ามีการกำหนดสิทธิ์ให้เข้าหรือไม่ เมื่อเข้าระบบได้แล้วผู้ดูแลระบบสามารถที่จะเลือกการทำงานภายในระบบควบคุมดูแล คือระบบจัดการผู้ใช้บริการ ที่มีสามารถทำการตรวจสอบการออนไลท์ของผู้ใช้บริการ การตรวจสอบข้อมูลของผู้ใช้บริการ การตรวจสอบประวัติการใช้งาน และการสร้างหมายเลขรหัสการใช้งาน หรือระบบคำนวณการใช้งาน ที่มีสามารถทำการคำนวณการใช้งานที่เป็นค่าใช้จ่ายของผู้ใช้บริการที่เข้าใช้งานในระบบ โดยผู้ดูแลสามารถกำหนดอัตราการคำนวณได้ หรือระบบจัดการการเข้าสู่ระบบควบคุมดูแล ที่สามารถให้ผู้ดูแลระบบทำการเปลี่ยนรหัสผ่านหรือการกำหนดเครื่องในการเข้าสู่ระบบควบคุมดูแล หรือระบบจัดการคอนฟิกกรูเรชั่น ที่สามารถให้ผู้ดูแลกำหนดหมายเลขไอพีและหมายเลขไอพีดีเอ็นเอสในส่วนเชื่อมต่อระบบอินเตอร์เน็ท รวมทั้งการรีสตาร์ทระบบในส่วนต่าง ๆ ที่เกี่ยวข้อง โดยผู้ดูแลระบบสามารถที่จะออกจากระบบ โดยการล็อกเอ้าท์ ซึ่งการทำงานของระบบทั้งหมดได้ผลดี

โดยสรุปแล้ว ภาพรวมการทำงานของระบบสามารถทำงานได้ ตามที่ผู้ศึกษาออกแบบพัฒนาระบบไว้ และคาดหวังว่าจะสามารถนำไปใช้งานได้จริง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 7
สรุปผลการพัฒนาระบบงาน และข้อเสนอแนะ

เนื้อหาในบทนี้จะสรุปผล พร้อมทั้งข้อเสนอแนะสำหรับผู้ที่สนใจนำระบบงานไปทำการพัฒนาต่อไป

7.1 สรุปผลการพัฒนาระบบงาน

สำหรับผลที่ได้จากการพัฒนาโครงงานนี้ ทำให้เกิดระบบที่สร้างความปลอดภัยในการใช้งานผ่านระบบเครือข่ายไวร์เลสแลน โดยการทำงานของตัวระบบจะแบ่งออกเป็น 2 ส่วนคือส่วนแรกใช้ป้องกันการใช้งานจากผู้ที่ไม่มีสิทธิ์ใช้งาน ด้วยการพิสูจน์ตัวจริงของผู้ใช้งาน จากรหัสผู้ใช้และรหัสผ่าน และส่วนที่สองใช้ป้องกันการรั่วไหลของข้อมูลจากผู้ที่ไม่ประสงค์ดี โดยการใช้ระบบ VPN เข้ามาช่วยในการทำงาน โดยจะทำการเชื่อมต่อระหว่างเครื่องผู้ใช้งานกับเครื่องเซอร์ฟเวอร์ที่ให้บริการ ซึ่งทำให้ผู้ใช้งานมั่นใจได้ว่าในระหว่างการใช้งานบนระบบเครือข่ายไวร์เลสแลนนั้นจะมีความปลอดภัย

นอกจากการพัฒนาตัวระบบที่ช่วยสร้างความปลอดภัยในการใช้งานบนเครือข่ายไวร์เลสแลนนี้แล้ว ผู้พัฒนายังดำเนินการพัฒนาระบบอีก 2 ระบบหลัก เพื่อที่จะช่วยให้ผู้ใช้บริการและผู้ดูแลระบบสามารถที่จะใช้งานระบบได้สะดวกขึ้นอีกด้วย โดย 2 ระบบนี้จะมีการทำงานหลักคือระบบสำหรับผู้ใช้บริการเพื่อใช้ในการตรวจสอบการใช้งานของผู้ใช้เอง และระบบสำหรับผู้ดูแลระบบเพื่อใช้ในการควบคุมดูแลการทำงานของระบบและคิดคำนวณการใช้งานของผู้ใช้บริการ

โดยโครงงานที่พัฒนาทั้งหมดมีราคาไม่แพง สามารถใช้ระบบปฏิบัติการและซอฟท์แวร์ที่ไม่เสียค่าลิขสิทธิ์ โดยตัวซอฟต์แวร์นี้มีความยืดหยุ่นต่อการพัฒนาได้ดี ซึ่งสามารถที่จะนำมาดำเนินการดัดแปลงให้สอดคล้องกับการใช้งานที่ต้องการได้ง่าย อีกทั้งตัวระบบที่พัฒนาเสร็จแล้วยังสามารถที่จะนำไปใช้งานได้จริงอีกด้วย

7.2 ข้อเสนอแนะ

ข้อเสนอแนะสำหรับผู้ที่จะนำระบบงานไปพัฒนาต่อไป ผู้พัฒนาเห็นว่าระบบที่ผู้พัฒนาได้ดำเนินการพัฒนามานั้นค่อนข้างสมบูรณ์แล้ว แต่อาจจะมีรายละเอียดปลีกย่อยบางอย่างที่ผู้ที่จะนำระบบไปพัฒนาต่อ อาจจะดำเนินการปรับปรุงเพิ่มเติม เช่นการนำระบบตรวจสอบและป้องกันการบุกรุก (IDS/IPS) สำหรับระบบเครือข่ายมาติดตั้งเพิ่ม เพื่อป้องกันการใช้งานที่พึงประสงค์ หรือการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพิ่มเติมการให้บริการโดยสามารถทำการการันตีอัตราความเร็วโดยการจัดแบ่งตามผู้ใช้บริการได้เป็นต้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

ประภาพร ช่างไม้.2543.**พื้นฐานการเขียนสคริปต์และ Web Application ด้วย Perl CGI.**กรุงเทพฯ : อินโฟเพรส.

Amsternet. 2003. **NoCatAuthOnFreeBsd.**[Online]. Available: http://wiki.samage.net/amsternet/NoCatAuthOnFreeBsd

Infopop Corp. 2002. **Installing and using phpMyAdmin.** [Online]. Available: http://ubbcentral.com/resource/PhPMyAdmin.html

James Yonan. 2002-2005. **An open Source SSL VPN Solution.** [Online]. Available: http://openvpn.net

Jean Tourrilhes. 1996-2004. **Linux & Wireless LANs.** [Online]. Available: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html

Katja and Guido Socher. 2001. **Unix Basics: Shell Programming.** [Online]. Available: http://mercury.chem.pitt.edu/~sasha/LinuxFocus/English/September2001/article216.shtml

Matt Gunter. 2003. **NoCatAuth Authentication Server Configuration.**[Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/3286631

Olivier. 2003. **Doc d'installation de Nocat .** [Online]. Available: http://www.wifi-vitry.net/imprimersans.php3?id_article=14

Schuyler Erle , Robert Flickenger. 2003. **NoCatNet.** [Online]. Available: http://nocat.net/

Scott Bartlett. 2003. **FreeRadius and MySQL.** [Online]. Available: http://www.frontios.com/freeradius.html

Stig Saether Bakken. 2003. **PHP Manual.** [Online]. Available: http://www.php.net/docs.php

Tanabutr. 2003. **Basic Linux Firewall By IPTABLES.**[Online]. Available: http://www24.brinkster.com/shadowpd/db/ossys/article/firewall.html

Toni dlF Diaz. 2003. **NoCatBOX HOWTO v1.4.**[Online]. Available: http://blyx.com/public/wireless/nocatbox/nocatbox-howto-en.pdf

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค่าต่าง ๆ ของไฟล์ /etc/dhcpd.conf

```
# /etc/dhcpd.conf
class "openvpn" {
        match if substring (hardware, 1, 2) = 00:FF;
}
authoritative;
subnet 192.168.1.0 netmask 255.255.255.0 {
        always-broadcast on;
        max-lease-time 3600;
        default-lease-time 1800;
        option subnet-mask 255.255.255.0;

        pool {
            deny members of "openvpn";
            range 192.168.1.100 192.168.1.200;
            option routers 192.168.1.1;
        }
}
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค่าต่าง ๆ ของไฟล์คอนฟิก NoCat /usr/local/nocat/gw/nocat.conf โดยละเอียด

###### gateway.conf -- NoCatAuth Gateway Configuration.	
Verbosity	10
GatewayName	Secure AG
GatewayMode	Passive
GatewayLog	/usr/local/nocat/gateway/nocat.log
LoginTimeout	10800
HomePage	http://192.168.1.1/
DocumentRoot	/usr/local/nocat/gw/htdocs
SplashForm	splash.html
StatusForm	status.html
TrustedGroups	Any
AuthServiceAddr	192.168.1.1
AuthServiceURL	https://$AuthServiceAddr/cgi-bin/login
LogoutURL	https://$AuthServiceAddr/logout.html
ExternalDevice	eth1
InternalDevice	tap+
LocalNetwork	192.168.2.0/24
DNSAddr	161.246.38.21
RouteOnly	1
ExcludePorts	25
IdleTimeout	100
ResetCmd	initialize.fw
PermitCmd	access.fw permit $MAC $IP $Class
DenyCmd	access.fw deny $MAC $IP $Class
StatsCmd	stats.fw $MAC $IP
GatewayPort	5280
AccountingMethod	RADIUS
AccountingUpdateInterval	30
RADIUS_Host	192.168.1.1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

RADIUS_Secret	radius_test
RADIUS_Timeout	5

ค่าต่าง ๆ ของไฟล์คอนฟิก NoCat /usr/local/nocat/nocat.conf โดยละเอียด

###### authserv.conf -- NoCatAuth Authentication Service Configuration.	
Verbosity	10
HomePage	http://192.168.1.1/
DocumentRoot	/usr/local/nocat/htdocs
DataSource	RADIUS
RADIUS_Secret	radius_test
RADIUS_Host	192.168.1.1
RADIUS_TimeOut	5
LocalGateway	192.168.1.1
LocalNetwork	192.168.2.0/24
RedirectTime	5
UserTable	member
UserIDField	login
UserPasswdField	pass
UserAuthField	status
UserStampField	created
GroupTable	network
GroupIDField	network
GroupAdminField	admin
MinPasswdLength	6
LocalGateway	192.168.1.1
LoginForm	login.html
LoginOKForm	login_ok.html
FatalForm	fatal.html
ExpiredForm	expired.html
RenewForm	renew.html

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

PassiveRenewForm	renew_pasv.html
RegisterForm	register.html
RegisterOKForm	register_ok.html
RegisterFields	name url description
UpdateForm	update.html
UpdateFields	url description
LoginGreeting	ยินดีต้อนรับเข้าสู่ Secure AG
LoginMissing	กรุณาป้อนข้อมูลให้ครบ !
LoginBadUser	รหัสผู้ใช้ผิด. กรุณาป้อนข้อมูลใหม่.
LoginBadPass	รหัสผ่านไม่ถูต้อง. กรุณาป้อนข้อมูลใหม่.
LoginBadStatus	Sorry, you are not a registered co-op member.
RegisterGreeting	Welcome! Please enter the following information to register.
RegisterMissing	Name, E-mail, and password fields must be filled in.
RegisterUserExists	Sorry, that e-mail address is already taken. Are you already registered?
RegisterBadUser	The e-mail address provided appears to be invalid. Did you spell it correctly?
RegisterInvalidPass	All passwords must be at least six characters long.
RegisterPassNoMatch	The passwords you provided do not match. Please try again.
RegisterSuccess	Congratulations, you have successfully registered.
UpdateGreeting	Enter your E-mail and password to update your info.
UpdateBadUser	That e-mail address is unknown. Please try again.
UpdateBadPass	That e-mail and password do not match. Please try again.
UpdateInvalidPass	New passwords must be at least six characters long.
UpdatePassNoMatch	The new passwords you provided do not match. Please try again.
UpdateSuccess	Congratulations, you have successfully updated your account.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค่าต่าง ๆ ของไฟล์คอนฟิก NoCat /usr/local/nocat/httpd.conf

```
        ScriptAlias /cgi-bin/ /usr/local/nocat/cgi-bin/
<Directory /usr/local/nocat/cgi-bin>
   SetEnv PERL5LIB /usr/local/nocat/lib
   SetEnv NOCAT    /usr/local/nocat/nocat.conf
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
 nokeepalive ssl-unclean-shutdown \
 downgrade-1.0 force-response-1.0
```

ค่าต่าง ๆ ของไฟล์คอนฟิก Apache /etc/httpd/conf/httpd.conf

```
Include /usr/local/nocat/httpd.conf
```

ค่าต่าง ๆ ของไฟล์คอนฟิก Apache /etc/httpd/conf.d/ssl.conf

```
<VirtualHost _default_:443>
DocumentRoot /usr/local/nocat/htdocs
ServerName 192168.1.1:443
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
SetEnvIf User-Agent ".*MSIE.*" \
       nokeepalive ssl-unclean-shutdown \
       downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค่าต่าง ๆ ของไฟล์คอนฟิก Freeradius /usr/local/etc/raddb/clients.conf

```
client 192.168.1.1 {
                        secret radius_test
                        shortname SecureAG
                }
```

ค่าต่าง ๆ ของไฟล์คอนฟิก Freeradius /usr/local/etc/raddb/realms

```
DEFAULT LOCAL
```

ค่าต่าง ๆ ของไฟล์คอนฟิก Freeradius /usr/local/etc/raddb/sql.conf

```
server = "localhost"
login = "root"
#password
sql_user_name = "%{Stripped-User-Name:-%{User-Name:-DEFAULT}}"
#sql_user_name = "%{User-Name}"
```

ค่าต่าง ๆ ของไฟล์คอนฟิก Freeradius /usr/local/etc/raddb/radiusd.conf

```
authorize {
                preprocess
                chap
                mschap
                #counter
                # attr_filter
                #eap
                suffix
                sql
                #files
                #etc_smbpasswd
}
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
authenticate {
        authtype PAP {
            pap
        }
        authtype CHAP {
            chap
        }
        authtype MS-CHAP {
            mschap
        }
        #pam
        #unix
        #authtype LDAP {
        #       ldap
        #}
}
preacct {
        preprocess
        suffix
        #files
}
accounting {
        acct_unique
        detail
        #counter
        unix
        sql
        radutmp
        #sradutmp
}
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
session {
                radutmp
}
```

ค่าต่าง ๆ ของไฟล์คอนฟิก OpenVPN /usr/share/ssl/openssl.cnf

```
dir         = /etc/ssl            # Where everything is kept
certs       = $dir/certs          # Where the issued certs are kept
crl_dir     = $dir/crl            # Where the issued crl are kept
database    = $dir/index.txt      # database index file.
new_certs_dir = $dir/newcerts     # default place for new certs.
certificate = $dir/my-ca.crt      # The CA certificate
serial      = $dir/serial         # The current serial number
crl         = $dir/crl.pem        # The current CRL
private_key = $dir/private/my-ca.key # The private key
RANDFILE    = $dir/private/.rand  # private random number file
```

โปรแกรมสคริปต์ OpenVPN create-vpn-link.sh

```
#!/bin/sh

        device=eth0
        local_ip=192.168.1.1
        netmask=255.255.255.0
        prefix_ip=192.168.2.
        first_tap_id=0
        first_tap_ip=10
        last_tap_ip=19
        first_vpn_ip=100
        first_port=15000
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
tap_ip=$first_tap_ip
vpn_ip=$first_vpn_ip
port=$first_port
tap_id=$first_tap_id

while [ $tap_ip -le $last_tap_ip ] ; do
        output_prefix=vpn-link-port-$port

        cat > $output_prefix.conf <<EOF

        local $local_ip
        dev tap
proto tcp-server
      port $port
ifconfig $prefix_ip$tap_ip $netmask
      route $prefix_ip$vpn_ip 255.255.255.255 $prefix_ip$tap_ip
      tls-server
dh /etc/ssl/dh1024.pem
      ca /etc/ssl/my-ca.crt
      cert /etc/ssl/certs/server.crt
key /etc/ssl/private/server.key
      verb 3

      mode server
ifconfig-pool $prefix_ip$vpn_ip $prefix_ip$vpn_ip
      ping 15
ping-restart 45

      push "ping 15"
push "ping-restart 45"
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
        #comp-lzo
EOF


            tap_id=`expr $tap_id + 1`
            tap_ip=`expr $tap_ip + 1`
            vpn_ip=`expr $vpn_ip + 1`
            port=`expr $port + 1`
done
```

โปรแกรมสคริปต์ OpenVPN vpn-client.sh

```
#!/bin/sh

number_vpn=10
vpn_link=1
port=15000
ip_vpn_serv=10

while [ $vpn_link -le $number_vpn ] ; do
output_prefix=vpn-client-port-$port

    # Create Temp Directory
    mkdir /$output_prefix

# Copy CA and Client Key to each directory
cp /var/www/html/download/my-ca.crt /$output_prefix
cp /var/www/html/download/client.crt /$output_prefix
    cp /var/www/html/download/client.key /$output_prefix

    cat > /$output_prefix/$output_prefix.ovpn <<EOF
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
remote 192.168.1.1
dev tap
        proto tcp-client
port $port

        tls-client
ca my-ca.crt
        cert client.crt
key client.key

        pull
#comp-lzo
        verb 3

        route-gateway 192.168.2.$ip_vpn_serv
#redirect-gateway
        route 0.0.0.0 0.0.0.0
EOF

        # Zip file
tar -czf /usr/local/nocat/htdocs/vpn/download/$output_prefix.tar.gz /$output_prefix

        # Remove Temporary Directory
            rm -rf /$output_prefix

        port=`expr $port + 1`
vpn_link=`expr $vpn_link + 1`
        ip_vpn_serv=`expr $ip_vpn_serv + 1`
done
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โปรแกรมสคริปต์ OpenVPN run-vpn.sh

```
#!/bin/sh

killall openvpn

number_vpn=10
vpn_link=1
port=15000

while [ $vpn_link -le $number_vpn ] ; do
        #run openvpn
        /usr/local/sbin/openvpn --config /etc/openvpn/vpn-link-port-$port.conf &

        port=`expr $port + 1`
        vpn_link=`expr $vpn_link + 1`
done
```

การแก้ไขปัญหา Perl ให้แสดงภาษาไทย

การแก้ไขปัญหา Perl แสดงภาษาไทยไม่อัตโนมัติ เข้าไปแก้ที่ /usr/lib/perl5/5.8.0/CGI.pm ทำการแก้เป็น $self->charset('tis-620');

การแก้ไขเพิ่มเติมไฟล์ initialize.fw

1. ส่วนที่ 1

```
net_novpn="192.168.1.0/24"
```

2. ส่วนที่ 2

```
for iface in $InternalDevice; do
if [ "$AuthServiceAddr" -o "$AllowedWebHosts" ]; then
        for host in $AuthServiceAddr $AllowedWebHosts; do
    for port in 80 443; do
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
                $nat      -s $net_novpn -d $host -p tcp --dport $port -j MASQUERADE
            $redirect -s $net_novpn -d $host -p tcp --dport $port -j RETURN
                $fwd -s $net_novpn -d $host -p tcp --dport $port -j ACCEPT
            $fwd -d $net_novpn -s $host -p tcp --sport $port -j ACCEPT
            done
          done
    fi
      if [ "$DNSAddr" ]; then
    for dns in $DNSAddr; do
        $fwd -d $net_novpn -s $dns -j ACCEPT
        for prot in tcp udp; do
      $fwd -s $net_novpn -d $dns -p $prot --dport 53 -j ACCEPT
        $nat -p $prot -s $net_novpn -d $dns --dport 53 -j MASQUERADE
        done
    done
      fi
done
```

3. ส่วนที่ 3

```
iptables  -t nat -A NoCat_Capture -s $net_novpn -p tcp --dport 80 -j REDIRECT --to-port 80
iptables  -t nat -A NoCat_Capture -s $net_novpn -p tcp --dport 443 -j REDIRECT --to-port 80
```

การแก้ไขเพิ่มเติมค่าคอนฟิกกรูเรชั่นของระบบ

1. สร้าง link file

```
#ln -s /etc /usr/local/nocat/htdocs/web_admin/dir_dns
#ln -s /etc/sysconfig/network-scripts /usr/local/nocat/htdocs/web_admin/dir_ip
```

2. ทำการเปลี่ยนสิทธิ์การเข้าถึงไฟล์

```
#chown apache:apache /usr/local/nocat/htdocs/web_admin
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

#chown apache:apache /usr/local/nocat/htdocs/web_admin/

#chown apache:root /usr/local/nocat/htdocs/web_admin/dir_dns

#chown apache:root /usr/local/nocat/htdocs/web_admin/dir_dns/

#chown apache:root /usr/local/nocat/htdocs/web_admin/dir_dns/named.conf

#chown apache:root /usr/local/nocat/htdocs/web_admin/dir_ip

#chown apache:root /usr/local/nocat/htdocs/web_admin/dir_ip/

#chown apache:root /usr/local/nocat/htdocs/web_admin/dir_ip/ifcfg-eth0

3. เพิ่มเติมการใช้งานไฟล์คอนฟิก

#chmod 600 /etc/sudoers

#vi /etc/sudoers

apache ALL=(root) NOPASSWD: /sbin/service named restart ,/sbin/service network restart , /usr/bin/killall gateway, /usr/local/nocat/gw/bin/gateway

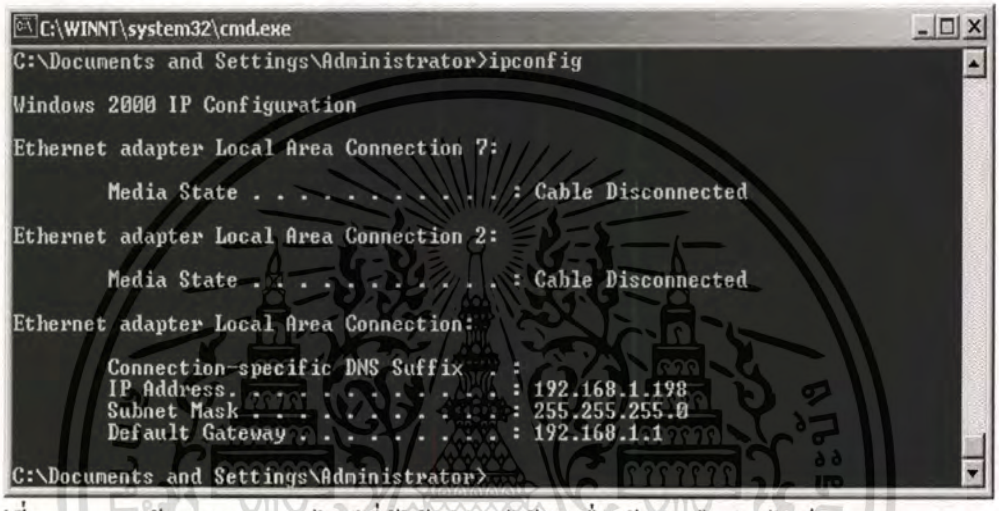
#chmod 440 /etc/sudoers

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คู่มือการใช้งาน

1. ระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง

ผู้ใช้บริการเริ่มดำเนินการใช้งาน โดยการเชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่ระบบเครือข่ายไวร์เลสแลนด์ เมื่อผู้ใช้บริการได้ทำการเชื่อมต่อเข้าสู่ระบบเครือข่ายไวร์เลสแลนของระบบเรียบร้อยแล้วจะได้รับหมายเลขไอพี ตามรูปที่ 1



รูปที่ 1 แสดงหน้าจอหมายเลขไอพีที่ผู้ใช้บริการได้รับเมื่อเข้าสู่เครือข่ายไวร์เลสแลนของระบบ

จากรูปจะเห็นได้ว่าเครื่องผู้ใช้บริการจะได้รับหมายเลขไอพีเบอร์ 192.168.1.198/24 และหมายเลขไอพีของเกต์เวย์เบอร์ 192.168.1.1 โดยหมายเลขไอพีที่ผู้ใช้บริการจะได้รับจะอยู่ในช่วงของ 192.168.1.100 – 192.168.1.200 /24

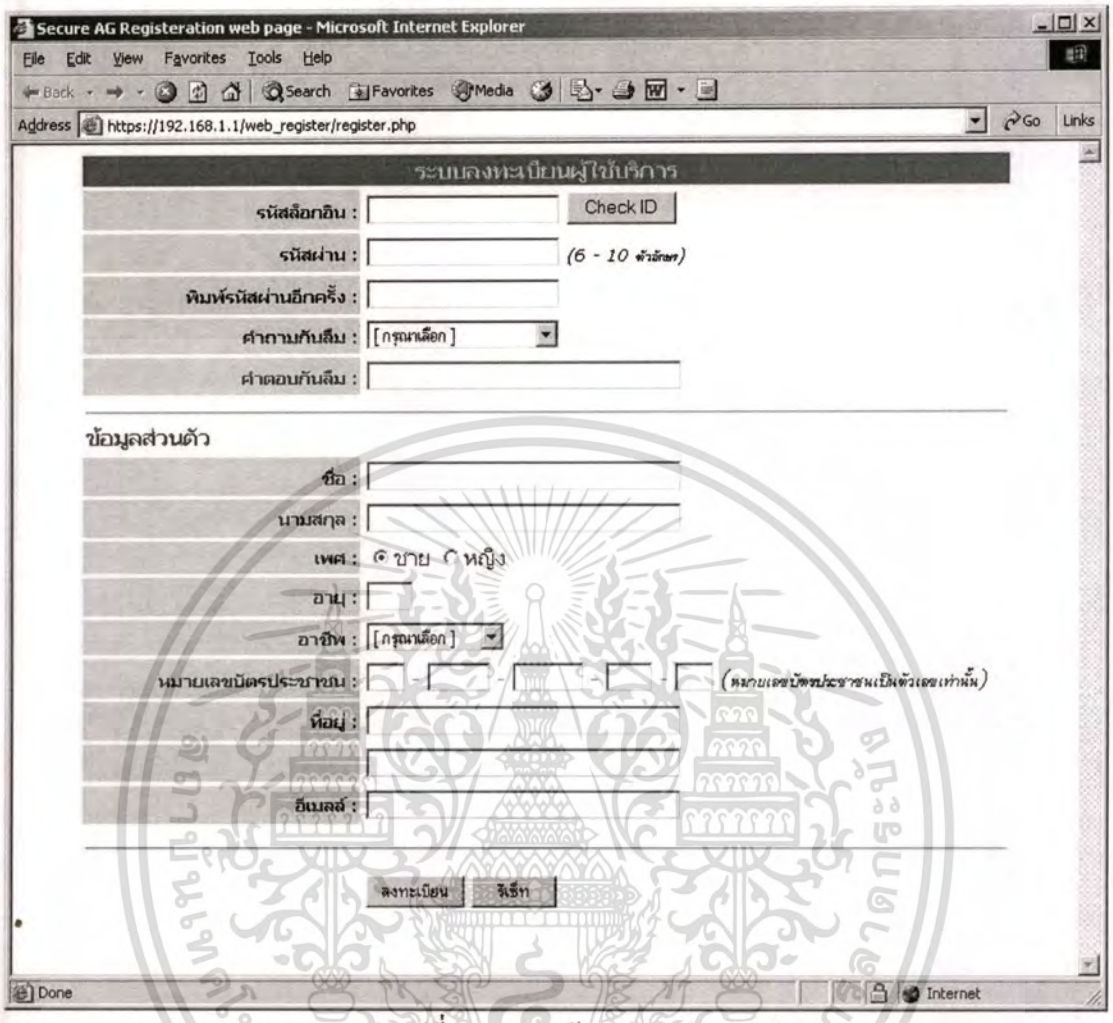
สำหรับผู้ใช้บริการใหม่ต้องการที่ใช้เข้าใช้บริการของระบบ จะต้องมีการดำเนินการลงทะเบียน และดาวน์โหลดโปรมแกรมเพื่อเชื่อมต่อกับระบบ VPN ของระบบก่อน โดยการดำเนินการนั้น ผู้ใช้สามารถเข้าสู่ระบบได้โดยการเปิดเว็บเบราเซอร์และเรียกเว็บโดยตรงคือ http://192.168.1.1/index.html หรือการเปิดเว็บเบราเซอร์แล้วทำการใส่เว็บไซต์ใด ๆ ก็ได้ โดยตัวระบบจะทำการรีไดเร็กมาที่เว็บของระบบ ซึ่งหน้าจอของระบบจะเป็นไปตามรูปที่ 2 โดยข้อมูลที่มีการรับ-ส่งระหว่างเครื่องผู้ใช้บริการกับเครื่องให้บริการจะทำงานอยู่บนระบบ SSL

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปที่ 2 แสดงหน้าจอการเข้าสู่ระบบเพื่อทำการดาวน์โหลดโปรแกรมสำหรับเชื่อมต่อระบบ VPN และการลงทะเบียน

จากรูป 2 ผู้ใช้บริการสามารถที่จะทำการดาวน์โหลดโปรแกรมสำหรับเชื่อมต่อระบบ VPN ได้ที่ลิงค์หมายเลข 1 และ 2 คือโปรแกรม OpenVPN และ vpnClient ตามลำดับ ซึ่งผู้ใช้สามารถจะดูวิธีการติดตั้งและทำงานของโปรแกรมทั้ง 2 ได้จากลิงค์หมายเลข 3 และ 4 ตามลำดับ นอกจากลิงค์ที่ให้ผู้ใช้บริการทำการโปรแกรมสำหรับเชื่อมต่อระบบ VPN แล้ว ยังมีลิงค์หมายเลข 5 ที่เชื่อมต่อไปยังระบบลงทะเบียน โดยเมื่อผู้ใช้ทำการเลือกคลิกที่ลิงค์นี้ จะมีการเรียกไปยังระบบลงทะเบียนซึ่งมีหน้าจอ ตามรูปที่ 3

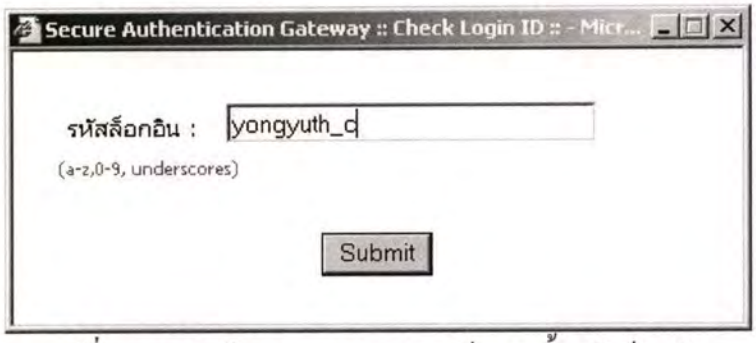
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3 แสดงหน้าจอระบบลงทะเบียน

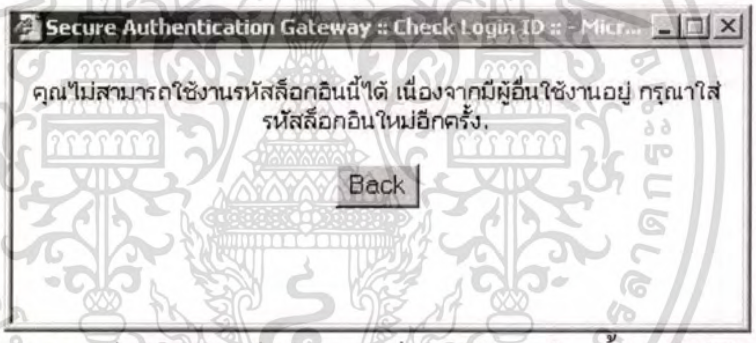
จากรูปข้างต้นเป็นหน้าจอของระบบลงทะเบียน โดยจะมีส่วนที่ให้ผู้ใช้ทำการกรอกข้อมูลอยู่ 2 ส่วนคือส่วนของข้อมูลที่ใช้ในระบบรักษาความปลอดภัยในการพิสูจน์ตัวจริง และส่วนของข้อมูลส่วนตัว โดยข้อมูลที่เป็นรหัสล็อกอินและรหัสผ่านในการเข้าสู่ระบบ จะให้ผู้ใช้สามารถทำการตั้งเองได้เพื่อความสะดวกในการจำ แต่ตัวระบบจะมีการตรวจสอบข้อมูลเหล่านั้นไว้ โดยส่วนของรหัสล็อกอิน ผู้ใช้จะต้องการตรวจสอบการตั้งโดยการกดที่ปุ่ม CheckID ซึ่งจะปรากฏหน้าจอตามรูปที่ 4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



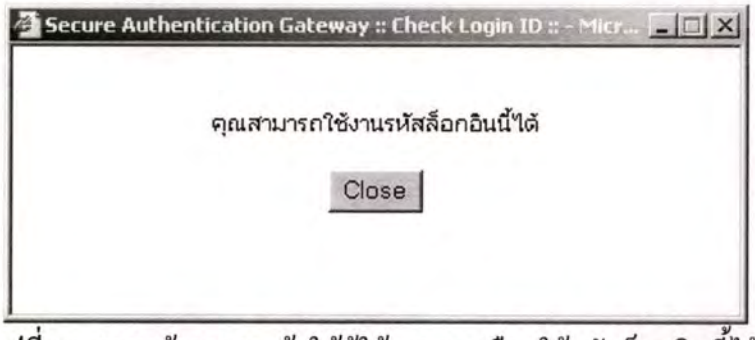
รูปที่ 4 แสดงหน้าจอระบบการตรวจเช็คการตั้งรหัสล็อกอิน

ตัวระบบตรวจเช็คการตั้งรหัสล็อกอินนี้จะมีการตรวจสอบรหัสล็อกอินที่ผู้ใช้เลือก โดยถ้ารหัสล็อกอินนั้น ๆ มีผู้อื่นที่ใช้อยู่แล้วระบบจะแจ้งเตือนมา เพื่อให้ผู้ใช้ทำการเปลี่ยนไปใช้รหัสล็อกอินอื่นแทน โดยตัวอย่างหน้าจอรูปที่ 5 จะเป็นระบบแจ้งเตือนเมื่อรหัสล็อกอินนั้น ๆ ซ้ำกับผู้อื่น



รูปที่ 5 แสดงหน้าจอระบบแจ้งเตือนรหัสล็อกอินมีการเลือกซ้ำกับผู้ใช้บริการอื่น

แต่ถ้ารหัสล็อกอินที่ผู้ใช้ทำการเลือกแล้วนั้นไม่ได้ถูกเลือกใช้จากผู้ใช้บริการอื่น ระบบก็จะทำการแจ้งให้ผู้ใช้สามารถเลือกใช้รหัสล็อกอินนี้ได้ โดยจะมีหน้าจอแสดงตามรูปที่ 6



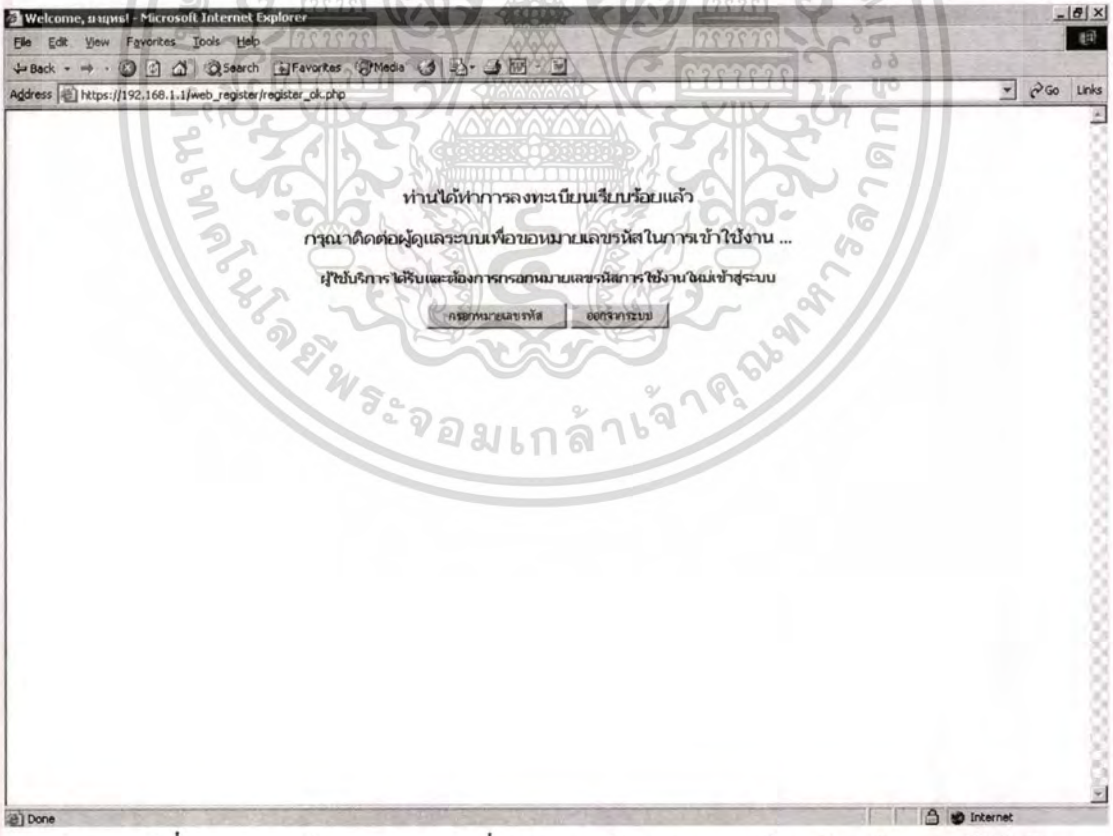
รูปที่ 6 แสดงหน้าจอการแจ้งให้ผู้ใช้สามารถเลือกใช้รหัสล็อกอินนี้ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในระบบลงทะเบียนผู้ใช้จะต้องดำเนินการกรอกข้อมูลทั้งหมดให้ถูกต้อง ครบถ้วน เนื่องจากระบบจะมีการเช็คความผิดพลาดของข้อมูลในการลงทะเบียน โดยมีตัวอย่างของหน้าจอที่เช็คความผิดพลาดในการกรอกข้อมูลของรหัสผ่านที่กรอกเกินจำนวน10 ตัวอักษร จะแสดงตามรูปที่ 7

รูปที่ 7 แสดงหน้าจอตัวอย่างการแจ้งเตือนการใส่ข้อมูลรหัสผ่านไม่ถูกต้อง

หลังจากที่ผู้ใช้บริการกรอกข้อมูลในระบบลงทะเบียนได้ถูกต้อง ครบถ้วนแล้ว ระบบจะมีการแสดงหน้าจอตอบรับ ดังรูปที่ 8



รูปที่ 8 แสดงหน้าจอของระบบที่มีการตอบรับการลงทะเบียนเรียบร้อยของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

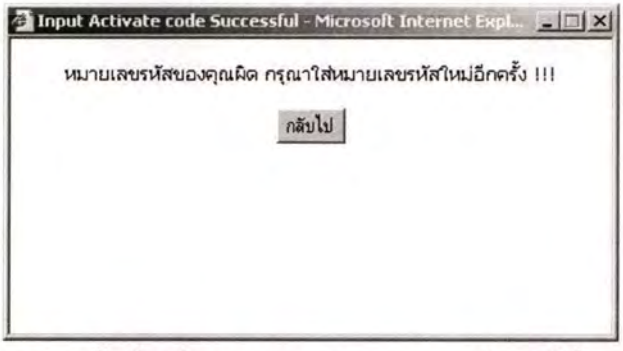
จากหน้าจอในรูปที่ 8 เป็นการแสดงหน้าจอการแจ้งการบันทึกข้อมูลในระบบลงทะเบียนเรียบร้อยแล้ว และมีการแจ้งผู้ใช้บริการดำเนินการติดต่อเพื่อขอหมายเลขรหัสการใช้งาน (Activate code) จากผู้ดูแลระบบ เพื่อทำการกรอกข้อมูลในการขอเข้าใช้บริการ

เมื่อผู้ใช้ได้รับหมายเลขรหัสการเข้าใช้งาน (Activate Code) จะสามารถทำการกรอกข้อมูลได้ โดยจะมีการแสดงหน้าจอดังรูปที่ 9

รูปที่ 9 แสดงหน้าจอระบบกรอกหมายเลขรหัสการใช้งาน

ในระบบกรอกหมายเลขรหัสการเข้าใช้งานนี้ ได้มีการตรวจสอบการทำงาน โดยถ้าผู้ใช้บริการมีการกรอกข้อมูลไม่ครบถ้วนและถูกต้อง ระบบจะมีการแจ้งเตือนดังเช่นรูปที่ 10 และ 11

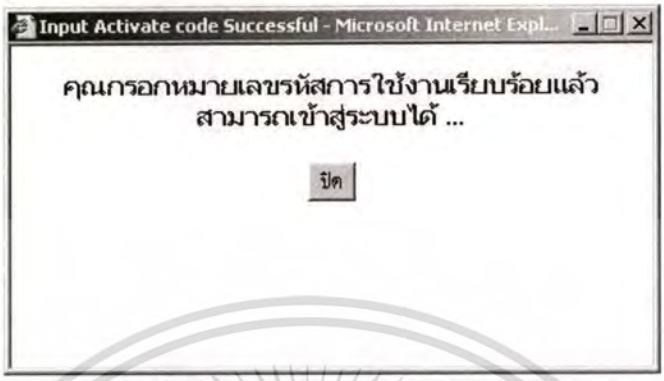
รูปที่ 10 แสดงหน้าจอการแจ้งเตือนในระบบกรอกหมายเลขรหัสการใช้งานเมื่อใส่ข้อมูลไม่ครบ



รูปที่ 11 แสดงหน้าจอการแจ้งเตือนในระบบกรอกหมายเลขรหัสการใช้งานเมื่อใส่ข้อมูลไม่ถูก

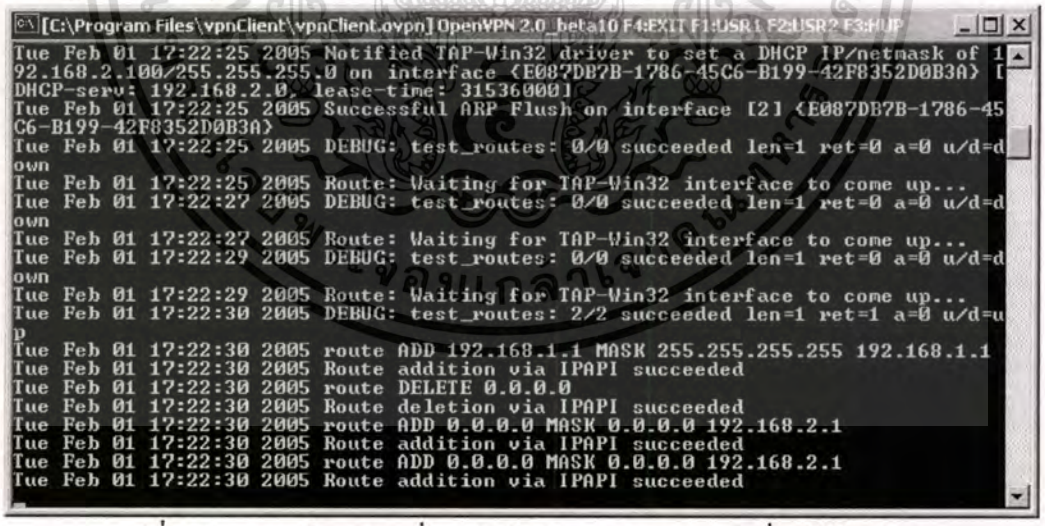
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แต่ถ้าผู้ใช้มีการกรอกหมายเลขรหัสได้ถูกต้องและครบถ้วน ระบบจะทำการแจ้งให้ทราบว่าผู้ใช้ทำการกรอกข้อมูลเรียบร้อยแล้ว ตามรูปที่ 12



รูปที่ 12 แสดงหน้าจอการบันทึกข้อมูลเรียบร้อยแล้วของระบบกรอกหมายเลขรหัสการใช้งาน

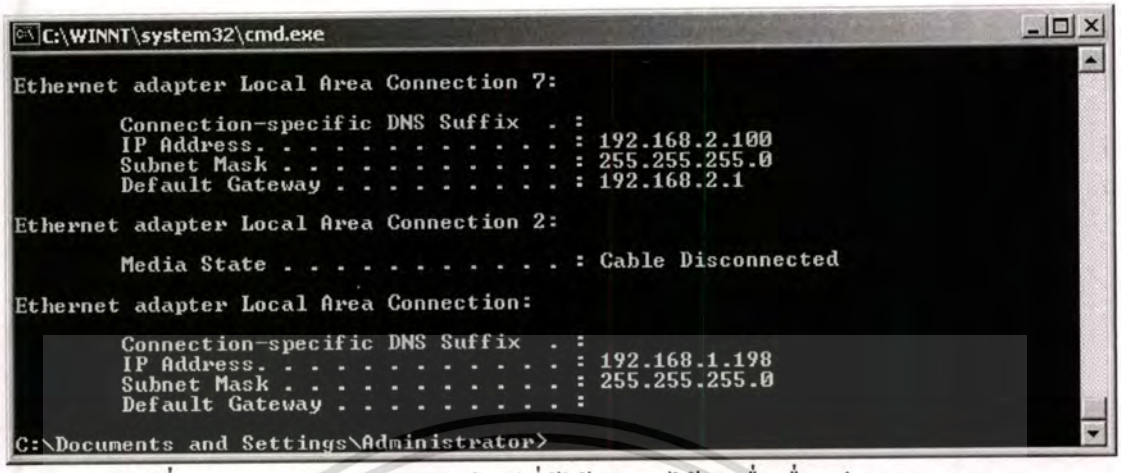
หลังจากที่ผู้ใช้มีการลงทะเบียน กรอกหมายเลขรหัสการเข้าใช้งาน และติดตั้งโปรแกรมสำหรับเชื่อมต่อระบบ VPN เรียบร้อยแล้ว ต่อไปจะเป็น การเข้าใช้บริการเพื่อออกสู่ระบบอินเตอร์เน็ท โดยผู้ใช้บริการจะต้องดำเนินการเชื่อมต่อระบบ VPN ก่อน โดยการคลิกสตาร์ทที่ไอคอนตัวระบบเชื่อมต่อ VPN ของโปรแกรม vpnClient ที่มีการติดตั้งไปแล้ว โดยเมื่อทำการเชื่อมต่อจะปรากฏหน้าจอ ดังรูปที่ 6.14



รูปที่ 13 แสดงหน้าจอการเชื่อมต่อเข้าสู่ระบบ VPN ของเครื่องผู้ใช้บริการ

เมื่อผู้ใช้ได้ทำการเชื่อมต่อแล้วจะได้รับหมายเลขไอพีชุดใหม่มาอีกชุด โดยเป็นหมายเลขไอพีที่ใช้ในการเชื่อมต่อเพื่อออกสู่ระบบอินเตอร์เน็ทเท่านั้น โดยจะเห็นได้จากรูที่ 14

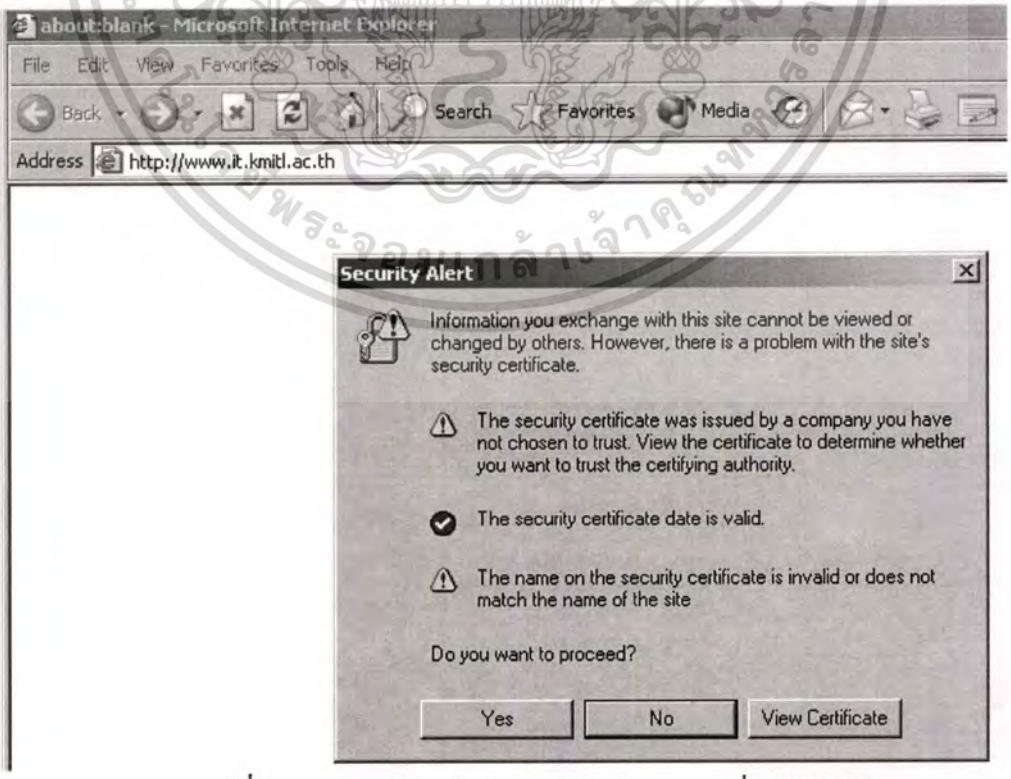
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 14 แสดงหน้าจอหมายเลขไอพีที่ผู้ใช้บริการได้รับเมื่อเชื่อมต่อระบบ VPN

จากรูปที่ 14 จะเห็นได้ว่าผู้ใช้จะได้รับหมายเลขไอพีใหม่มาอีกชุดคือเบอร์ 192.168.2.100/24 และหมายเลขไอพีของเกต์เวย์คือ 192.168.2.1 นั่นเอง โดยหมายเลขไอพีที่ผู้ใช้บริการจะได้รับนั้นจะอยู่ในช่วงของ 192.168.2.100–200/24

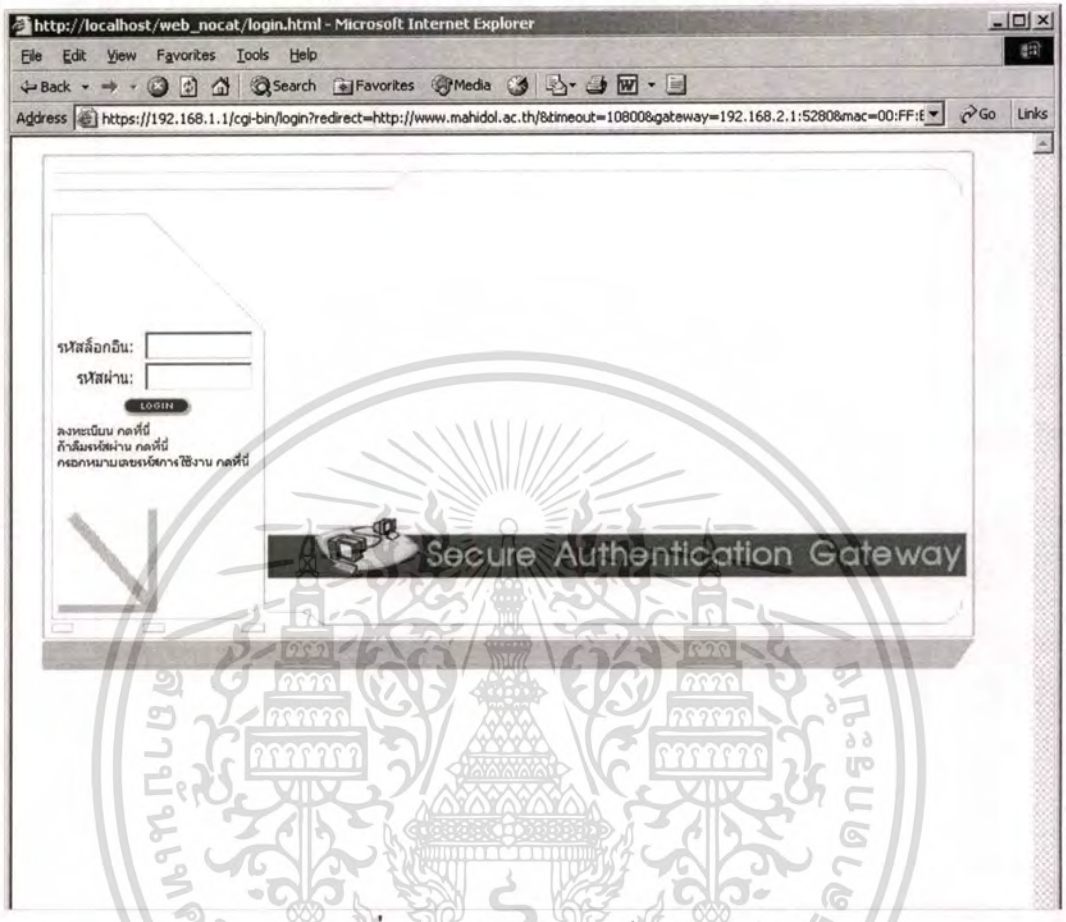
ต่อไปจะเป็นการเข้าสู่ระบบพิสูจน์ตัวจริงของผู้ใช้บริการผ่าน SSL โดยใช้เวบเบราเซอร์พิมพ์ยูอาร์แอลเวบไซต์ที่ต้องการ ดังรูปที่ 15



รูปที่ 15 แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อทำการตอบยืนกดปุ่ม Yes แล้วระบบจะทำการขึ้นหน้าจอให้ลอกอินขึ้นมาโดยอัตโนมัติ



รูปที่ 16 แสดงหน้าจอการล็อกอินเข้าสู่ระบบ

ภายในหน้าจอล็อกอินนี้ นอกจากจะมีส่วนที่ใช้สำหรับการล็อกอินเข้าสู่ระบบแล้ว ยังมีส่วนการทำงานอื่นอีก คือส่วนของระบบตรวจสอบรหัสผ่านในกรณีลืม ส่วนของระบบกรอกหมายเลขรหัสการใช้งาน และส่วนของระบบลงทะเบียน ซึ่ง 2 ระบบหลังนี้ได้มีการกล่าวถึงการใช้งานไปแล้วในข้างต้น

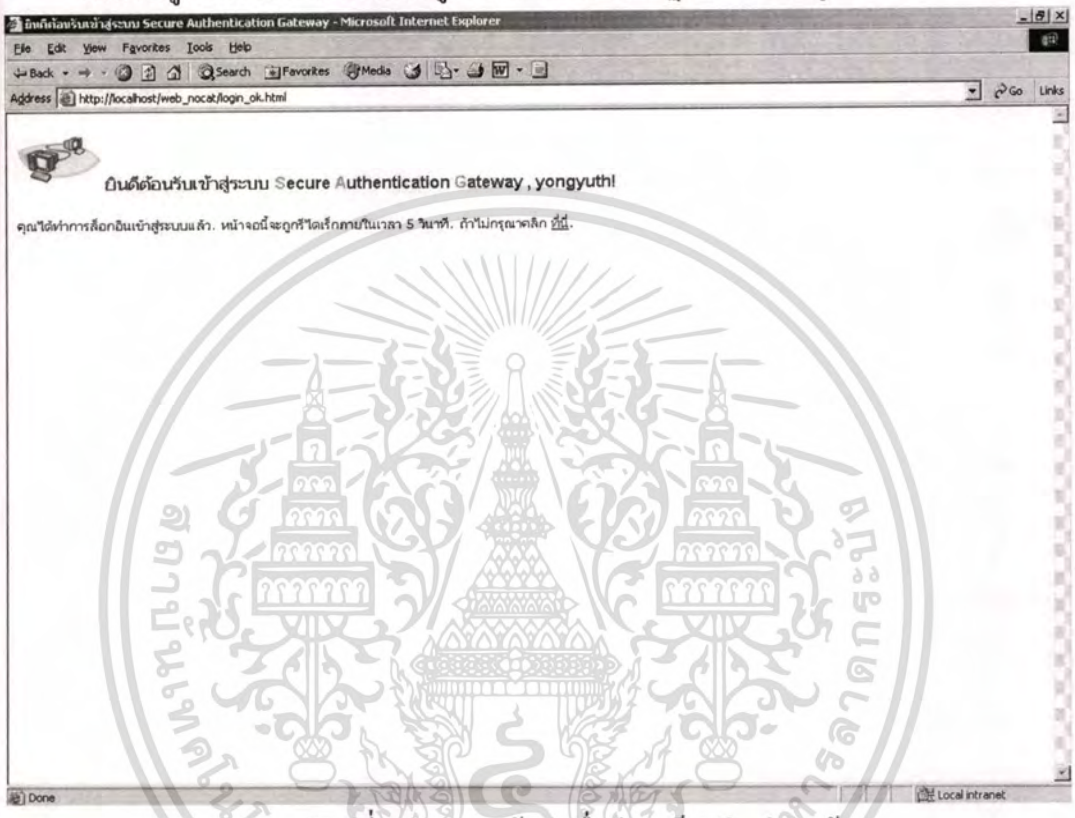
สำหรับส่วนของระบบตรวจสอบรหัสผ่านในกรณีลืมนี้ จะมีหน้าจอดังรูปที่ 17

รูปที่ 17 แสดงหน้าจอระบบตรวจสอบรหัสผ่านในกรณีลืม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยเมื่อผู้ใช้บริการทำการกรอกข้อมูลสำหรับใช้ตรวจสอบเรียบร้อยแล้ว ระบบจะแจ้งรหัสผ่านกลับมา

สำหรับผู้ใช้ที่ทำการล็อกอินเข้าสู่ระบบแล้ว จะปรากฏหน้าจอตามรูปที่ 18



รูปที่ 18 แสดงหน้าจอเมื่อมีการล็อกอินผ่านแล้ว

เมื่อทำการล็อกอินผ่านแล้วระบบจะทำการส่งค่าที่ผู้ใช้เคยทำการพิมพ์ยูอาร์แอลไว้แต่ต้นให้อัตโนมัติ โดยในระหว่างการใช้งานของผู้ใช้จะมีเว็บเพจสำหรับตรวจสอบสถานะการทำงาน (Agent Page) ดังรูป 19

รูปที่ 19 แสดงหน้าจอระบบตรวจสอบสถานการณ์ใช้งาน

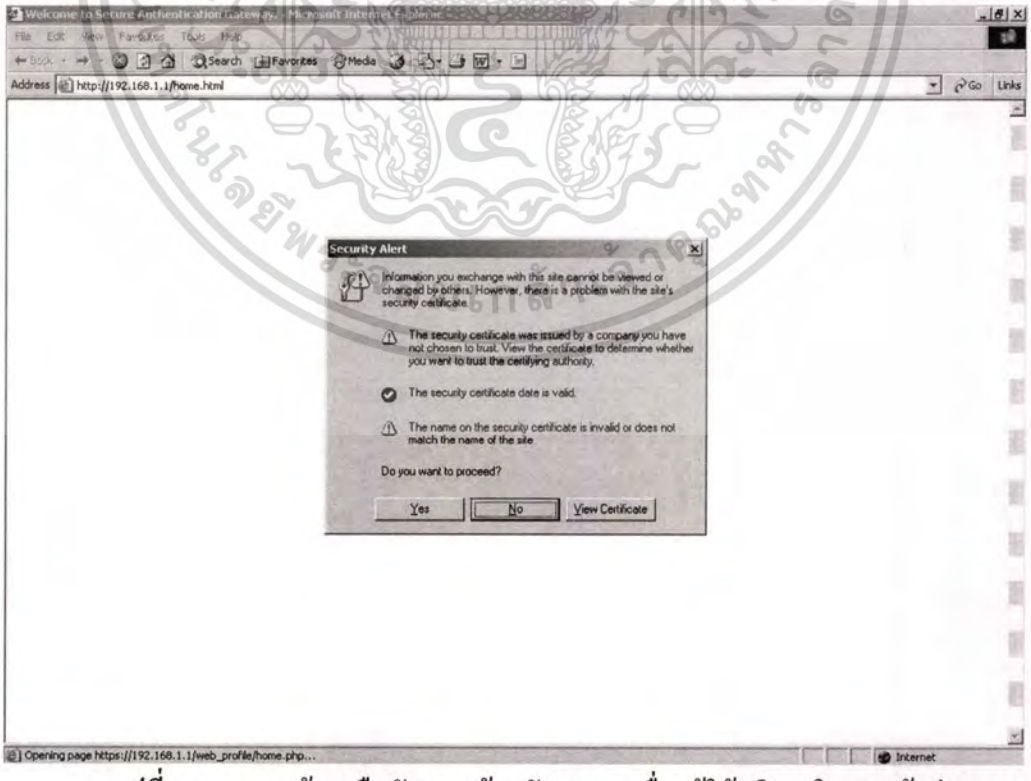
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และเมื่อผู้ใช้ต้องการที่จะต้องจากระบบสามารถทำการล็อกเอ้าท์ ได้จาเว็บตรวจสอบสถานการณ์ใช้งาน โดยเมื่อทำการล็อกเอ้าท์เรียบร้อยแล้วจะปรากฏ ดังรูป 20 ซึ่งเป็นการสิ้นสุดการใช้งานของระบบ

รูปที่ 20 แสดงหน้าจอของระบบที่ผู้ใช้ทำการล็อกเอ้าท์ออกเรียบร้อยแล้ว

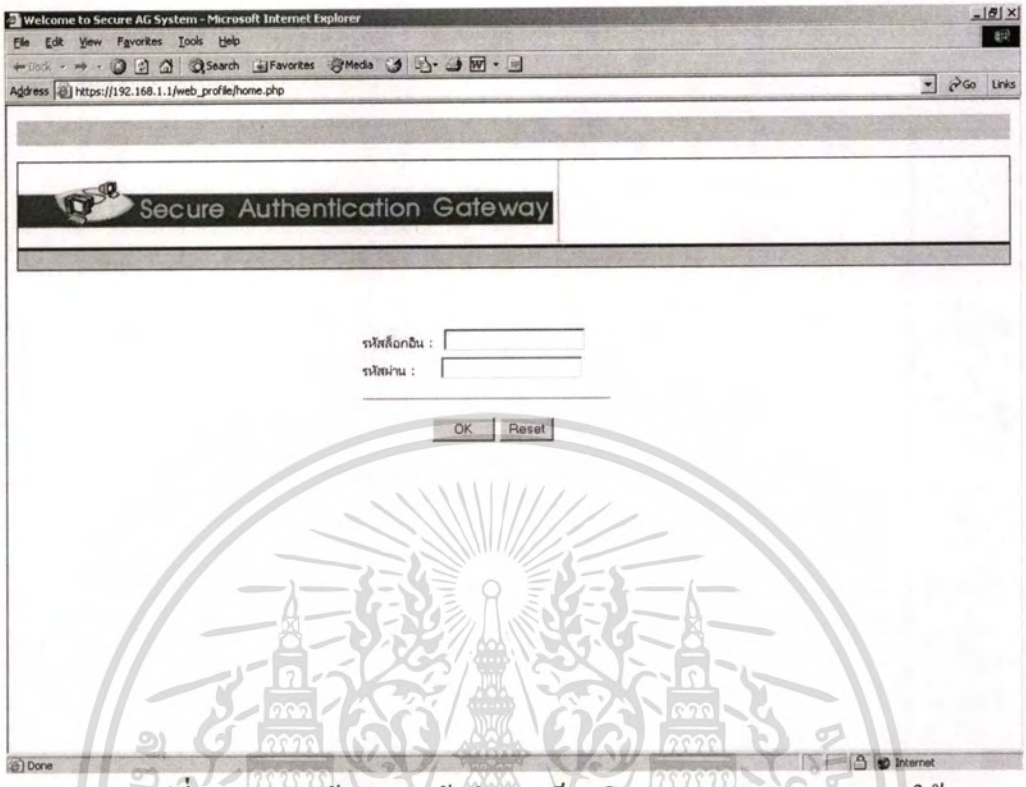
2. ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

สำหรับการทดสอบระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการนี้ ผู้ใช้สามารถเข้าสู่ระบบได้ที่ http://192.168.1.1/home.html โดยระบบจะรีไดเร็กไปยัง https://192.168.1.1/web_profile/home.php ซึ่งจะปรากฏหน้าจอดังรูป 21 และ 22 ตามลำดับ



รูปที่ 21 แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องผู้ใช้บริการในการเข้าสู่ระบบตรวจสอบการใช้งาน

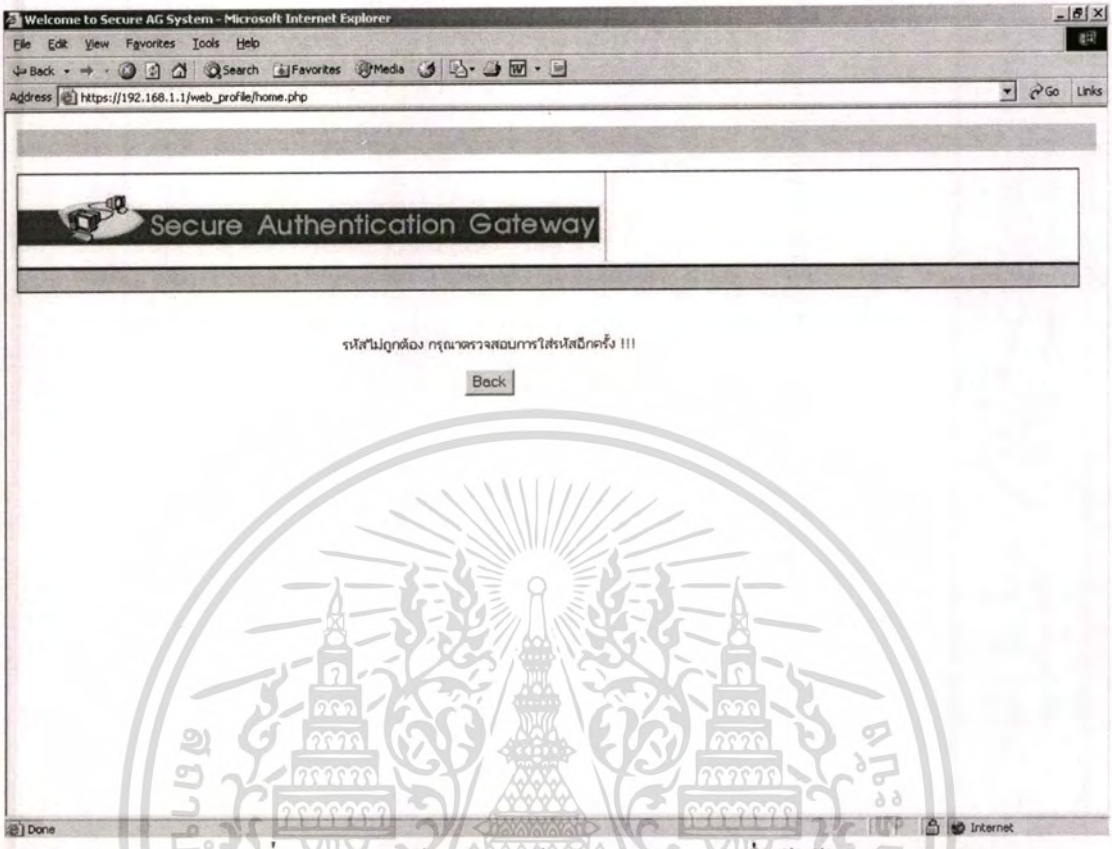
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 22 แสดงหน้าจอการเข้าสู่ระบบล็อกอินของระบบตรวจสอบการใช้งาน

ภายในระบบล็อกอินเพื่อเข้าสู่ระบบตรวจสอบการใช้งานนี้ จะมีการตรวจสอบข้อมูล โดยถ้าผู้ใช้มีการกรอกรหัสผ่านผิด ระบบจะมีการแจ้งเตือน ดังรูปที่ 23

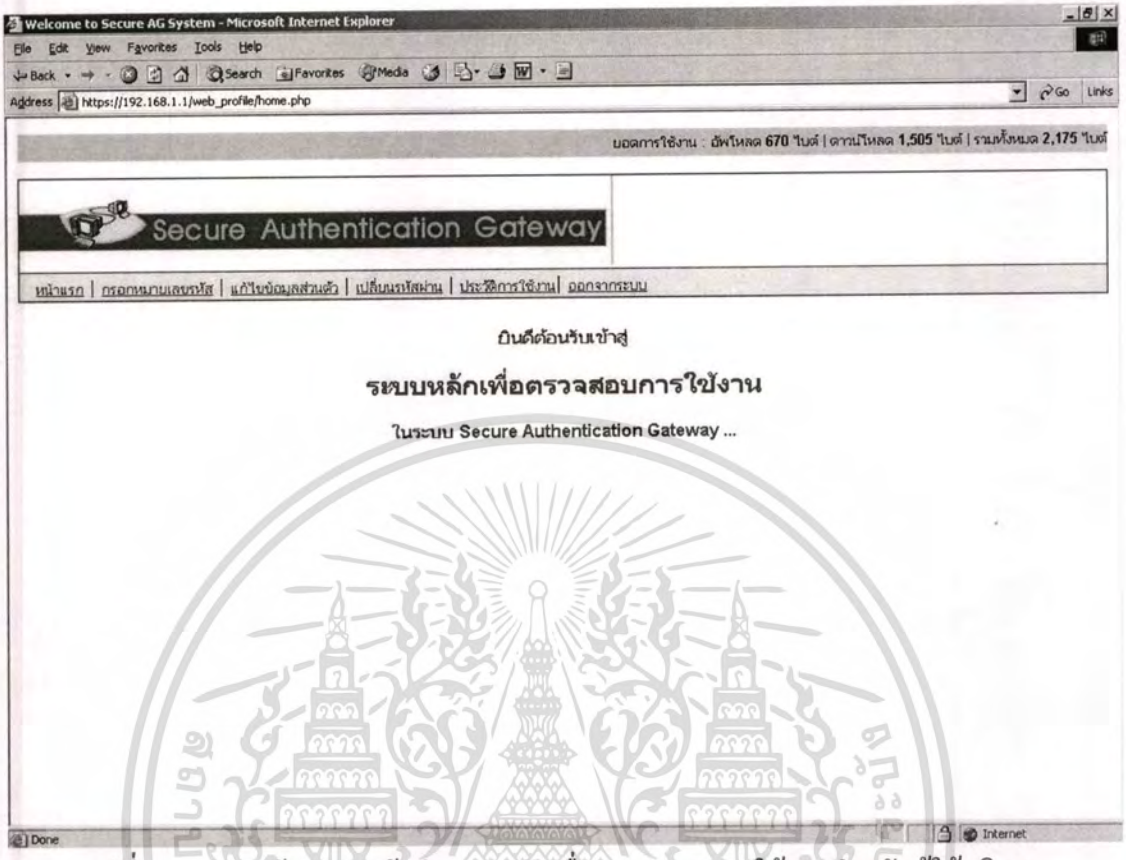
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 23 แสดงหน้าจอการแจ้งเตือนของระบบเมื่อผู้ใช้ใส่รหัสผ่านผิด

และเมื่อผู้ใช้ทำการล็อกอินผ่านแล้ว จะสามารถเข้าสู่ระบบหลักเพื่อตรวจสอบการใช้งานได้ โดยจะปรากฏหน้าจอดังรูป 6.24

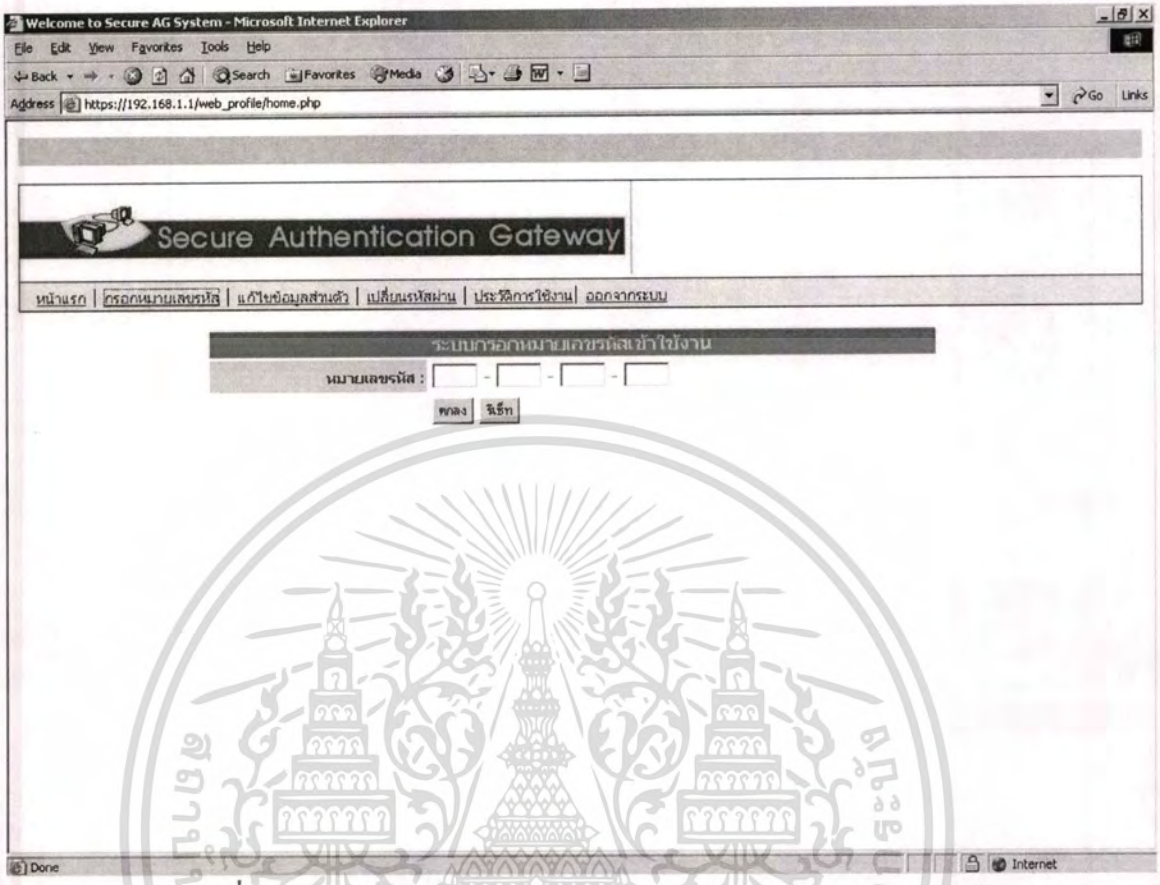
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 24 แสดงหน้าจอการเข้าสู่ระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการ

ภายในระบบหลักเพื่อตรวจสอบการใช้งานสำหรับผู้ใช้บริการนั้น จะมีการทำงานอื่น ๆ ที่นอกเหนือจากการแสดงจำนวนการใช้งานของผู้ใช้เอง คือ ผู้ใช้สามารถที่จะดำเนินการกรอกหมายเลขรหัสการใช้งานได้จากระบบนี้ โดยจะปรากฏหน้าจอดังรูป 25

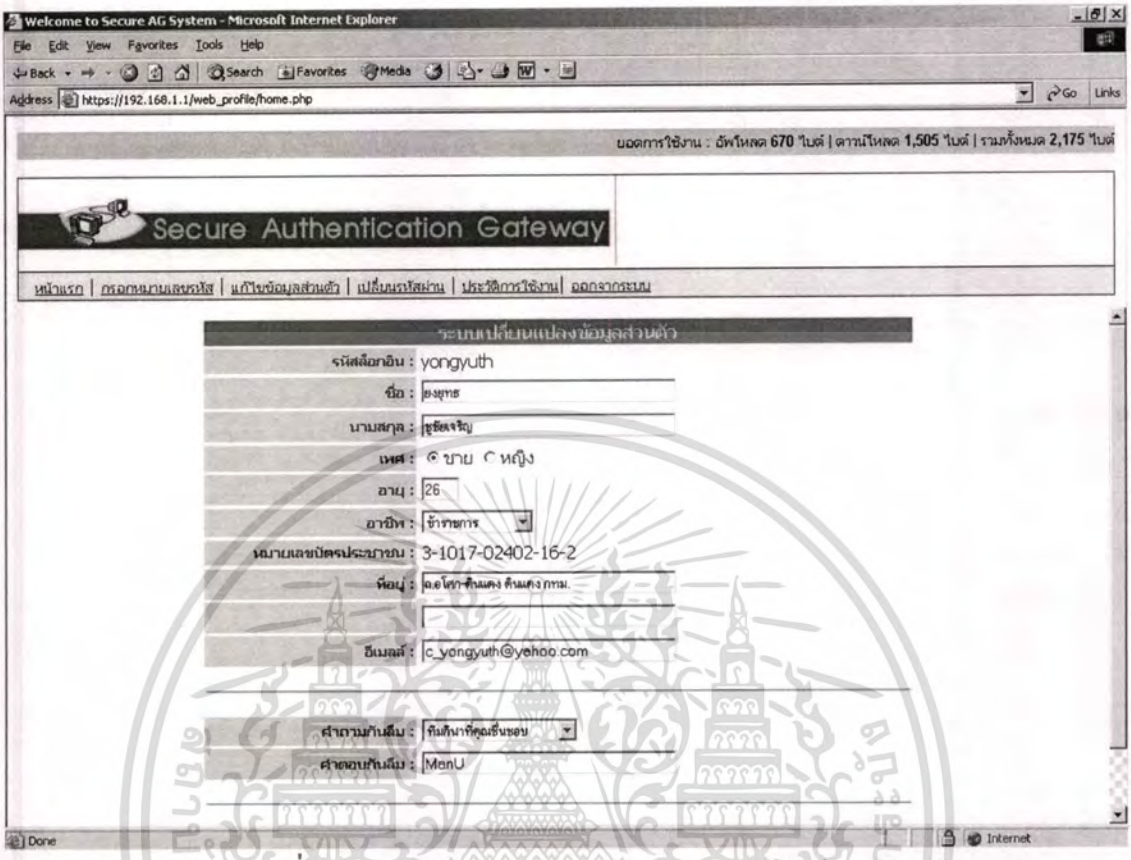
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 25 แสดงหน้าจอการทำงานสำหรับการกรอกหมายเลขรหัสการใช้งาน

ถ้าผู้ใช้เลือกแก้ไขข้อมูลส่วนตัวสามารถเลือกคลิกที่เมนู ซึ่งจะปรากฏหน้าจอดังรูป 26

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



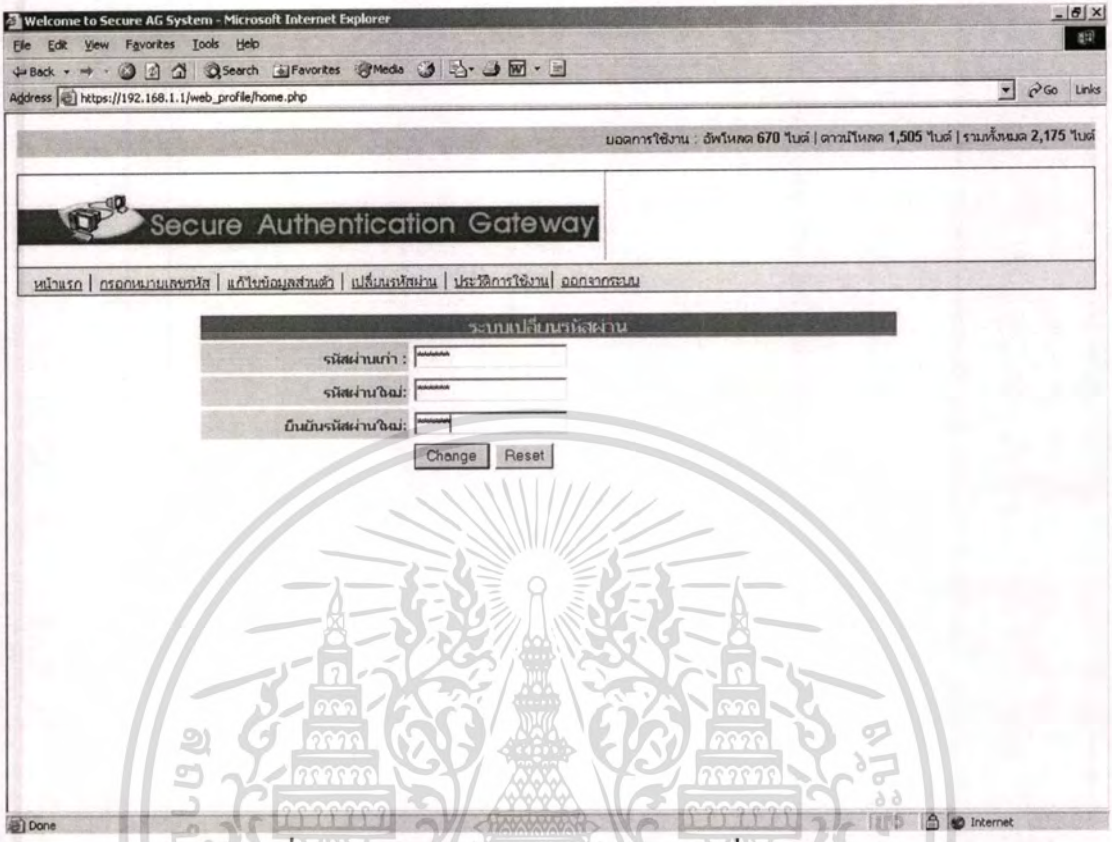
รูปที่ 26 แสดงหน้าจอการทำงานสำหรับการแก้ไขข้อมูลส่วนตัว

โดยในการแก้ไขข้อมูลส่วนตัวของผู้ใช้นั้น ระบบจะมีการตรวจสอบข้อมูลต่าง ๆ ก่อนจะทำการบันทึกว่าถูกต้อง ครบถ้วนหรือไม่ โดยถ้าข้อมูลเหล่านี้ไม่ถูกต้อง ครบถ้วนก็จะดำเนินการแจ้งเตือนเพื่อให้ผู้ใช้ดำเนินการแก้ไข ซึ่งมีตัวอย่างการแก้ไขข้อมูลไม่ถูกต้อง ครบถ้วน ดังรูป 27

รูปที่ 27 แสดงตัวอย่างหน้าจอของระบบแจ้งเตือนในการแก้ไขข้อมูลส่วนตัวไม่ถูกต้อง

ถ้าผู้ใช้เลือกทำการเปลี่ยนรหัสผ่าน สามารถคลิกได้ที่เมนู โดยจะปรากฏหน้าจอดังรูป 28

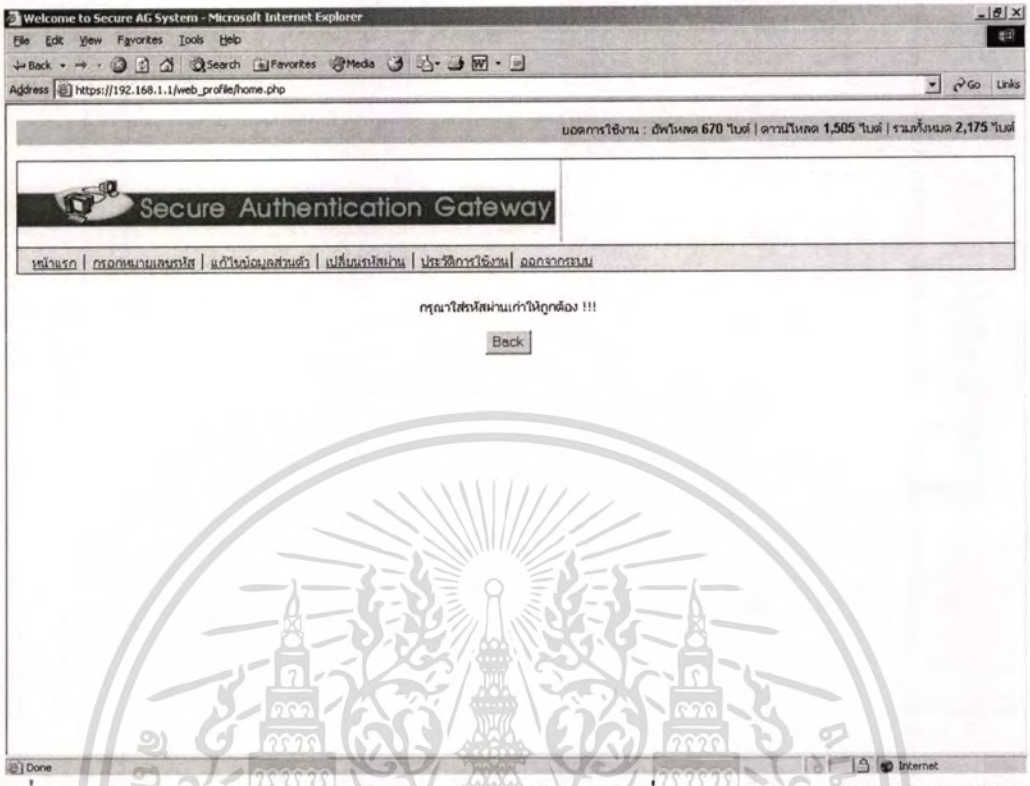
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 28 แสดงหน้าจอการทำงานของการเปลี่ยนรหัสผ่าน

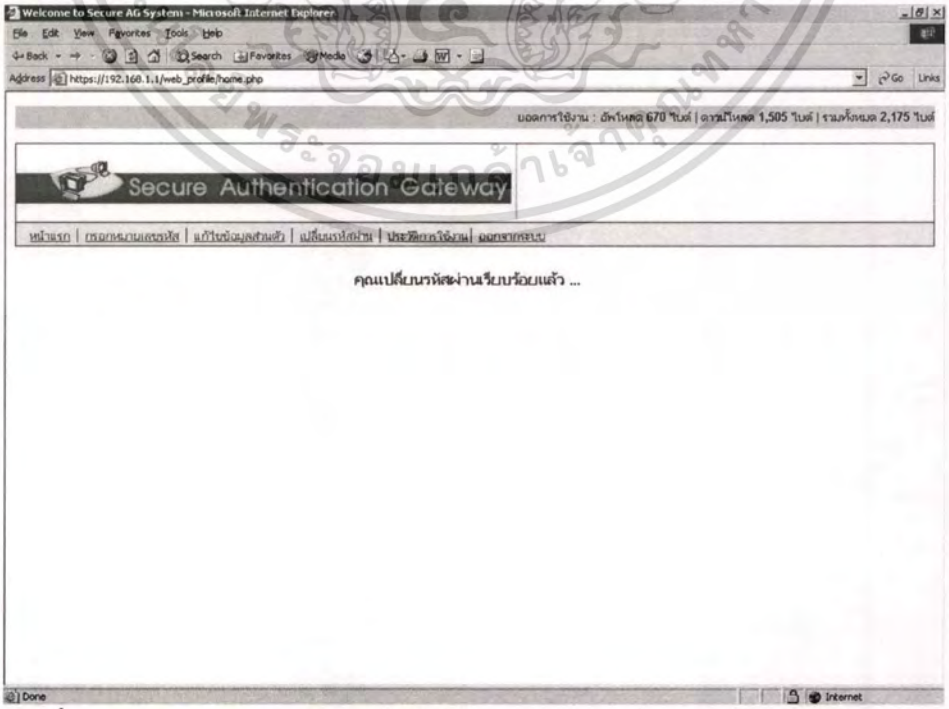
ในการเปลี่ยนรหัสผ่านนี้ ระบบจะมีการตรวจสอบรหัสผ่านเดิมก่อนด้วย ซึ่งถ้าหากผู้ใช้ใส่รหัสผ่านเดิมผิด ระบบก็จะมีการแจ้งเตือนให้ผู้ใช้ได้ทำการใส่รหัสผ่านเดิมอีกครั้ง ตามที่ปรากฏในหน้าจอ ของรูปที่ 29

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 29 แสดงตัวอย่างหน้าจอของระบบแจ้งเตือนในการเปลี่ยนรหัสผ่านโดยใส่รหัสผ่านเดิมผิด

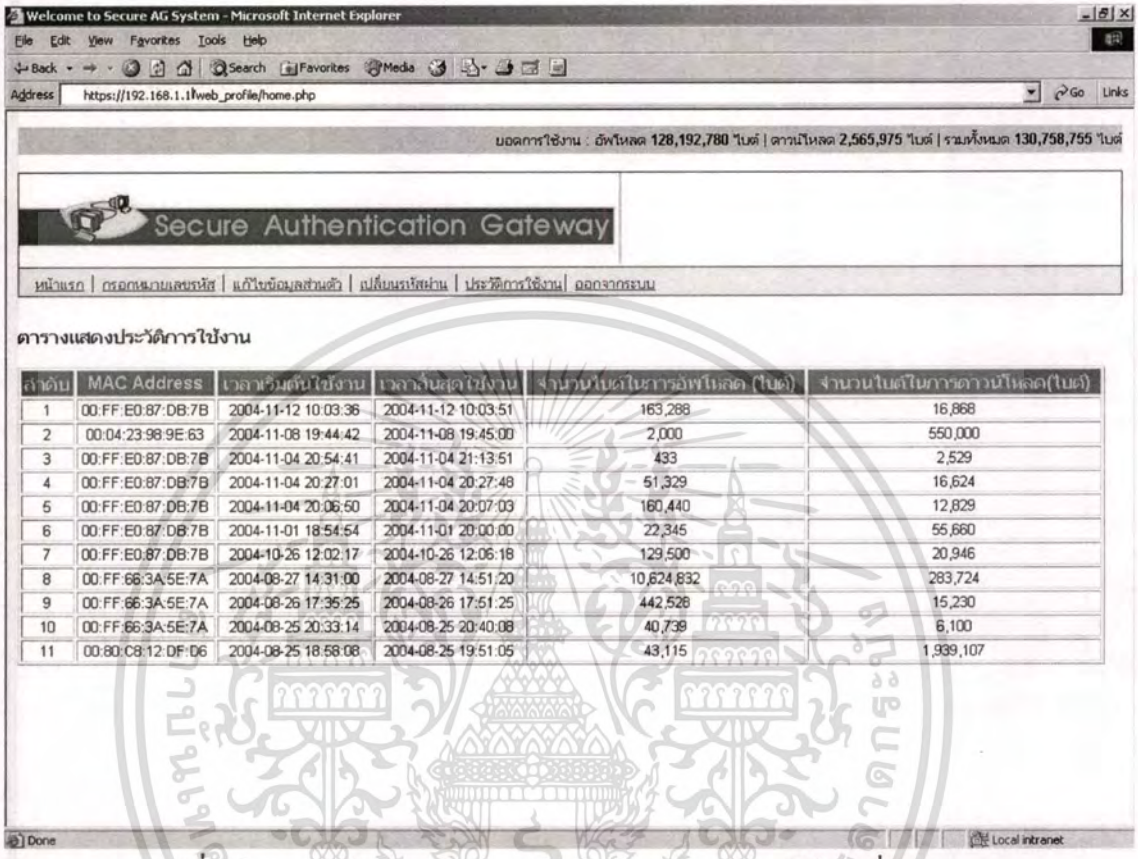
แต่ถ้าผู้ใช้ใส่รหัสผ่านเดิมถูกต้องระบบก็จะทำการเปลี่ยนรหัสผ่านใหม่ ให้โดยจะมีการแสดงหน้าจอให้ผู้ใช้ได้ทราบ ดังรูปที่ 30



รูปที่ 30 แสดงหน้าจอของระบบที่แจ้งให้ทราบว่าการเปลี่ยนรหัสผ่านเรียบร้อยแล้ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

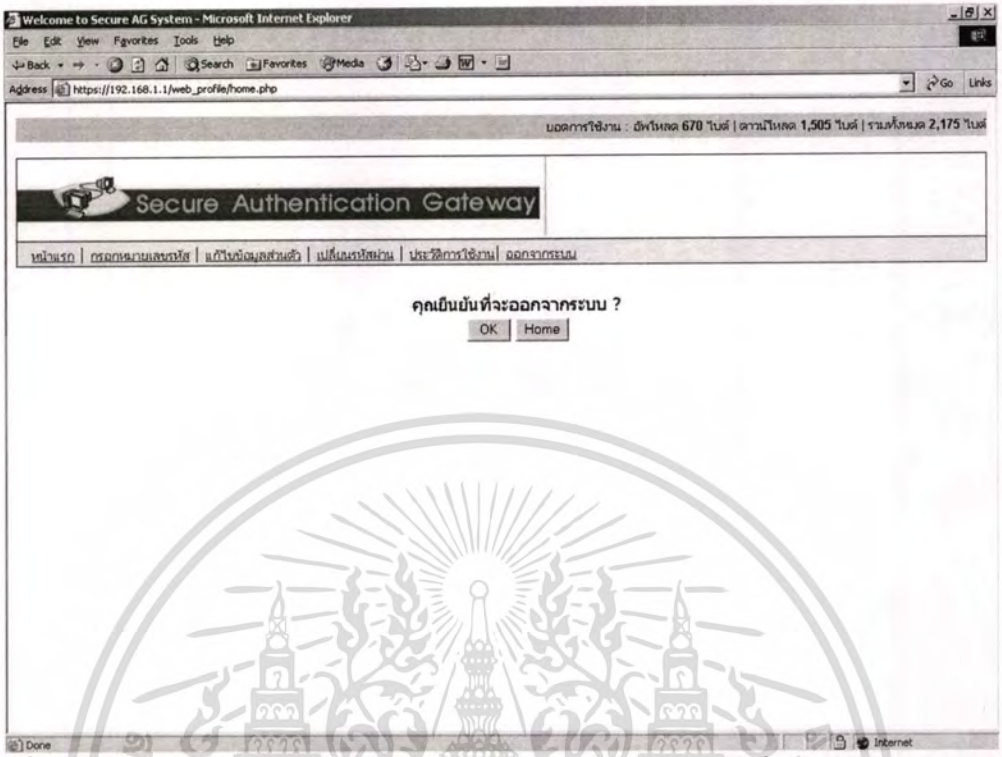
ถ้าผู้ใช้เลือกทำการดูประวัติการใช้งาน สามารถคลิกได้ที่เมนู โดยจะปรากฏหน้าจอดังรูป 31



รูปที่ 31 แสดงหน้าจอการทำงานสำหรับการดูประวัติการใช้งานที่ผ่านมา

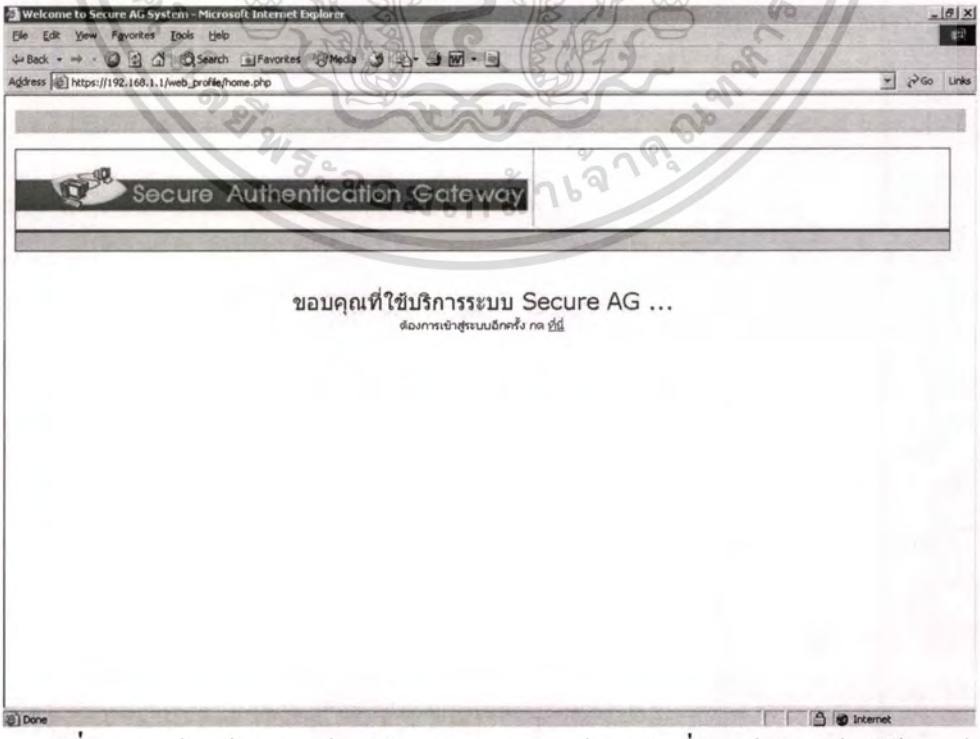
ถ้าผู้ใช้เลือกทำการล็อกเอ้าท์เพื่อออกจากระบบ ก็สามารถคลิกได้ที่เมนู โดยจะปรากฏหน้าจอดังรูป 32

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 32 แสดงหน้าจอการทำงานสำหรับการล็อกเอ้าท์ออกจากระบบเพื่อตรวจสอบการใช้งาน

โดยถ้าผู้ใช้ทำการยืนยันการออกจากระบบ ระบบก็จะทำการตอบรับการออกจากระบบ โดยปรากฏหน้าจอ ดังรูป 33 ซึ่งเป็นการสิ้นสุดการทำงานของระบบเพื่อตรวจสอบการใช้งาน

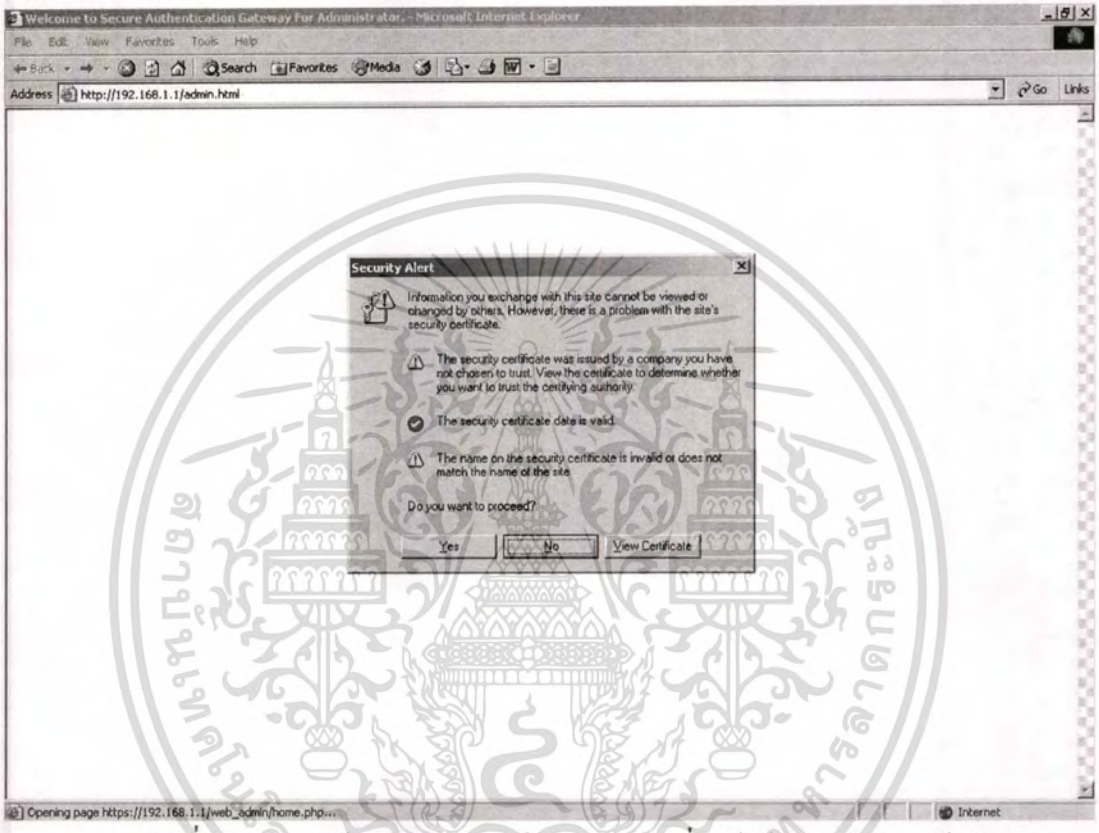


รูปที่ 33 แสดงหน้าจอการตอบรับการออกจากระบบหลักเพื่อตรวจสอบการใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

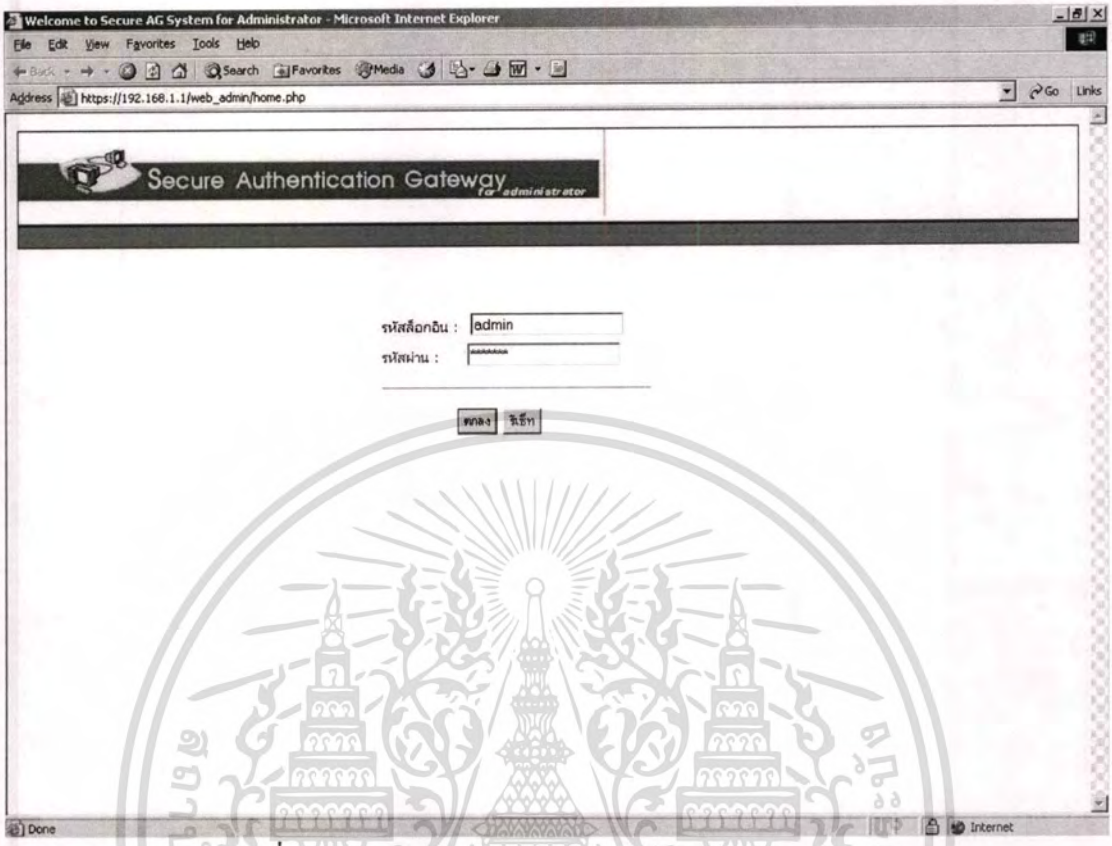
3. ระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

สำหรับการทดสอบระบบควบคุมดูแลสำหรับผู้ดูแลระบบ ผู้ดูแลระบบสามารถเข้าสู่ระบบได้ที่ http://192.168.1.1/admin.html โดยระบบจะรีไดเร็กไปยัง https://192.168.1.1/web_admin/home.php ซึ่งจะปรากฏหน้าจอดังรูป 34 และ 35 ตามลำดับ



รูปที่ 34 แสดงหน้าจอยืนยันการเข้ารหัส SSL เครื่องผู้ใช้บริการในการเข้าสู่ระบบควบคุมดูแล

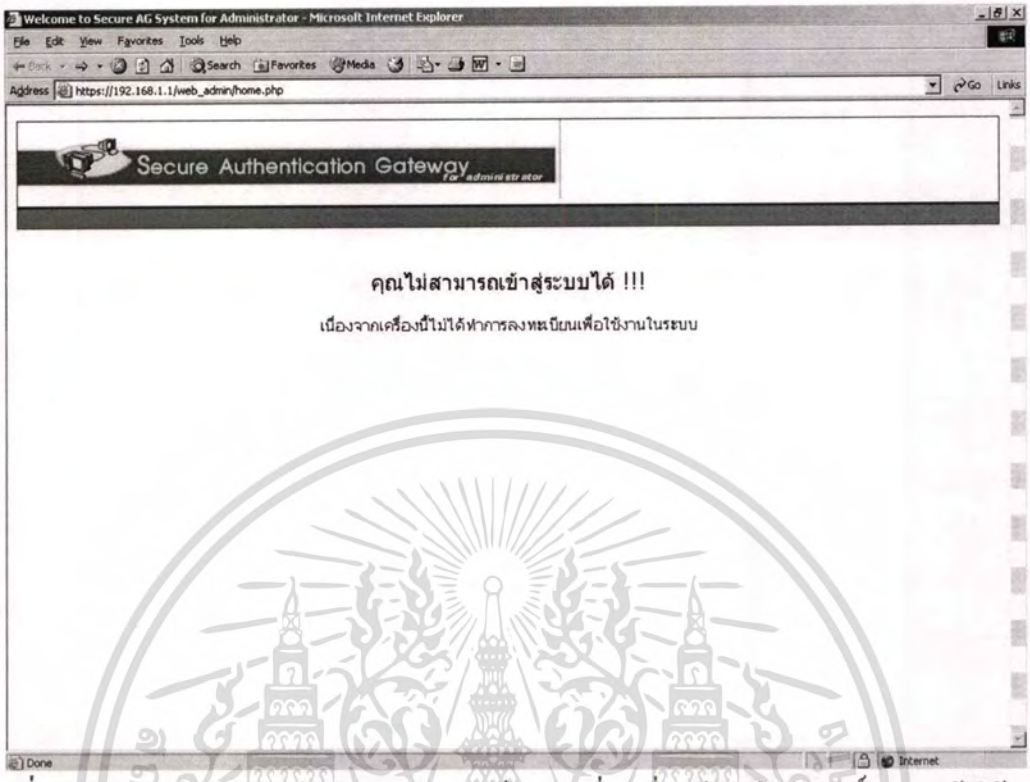
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 35 แสดงหน้าจอการเข้าสู่ระบบล็อกอินของระบบควบคุมดูแล

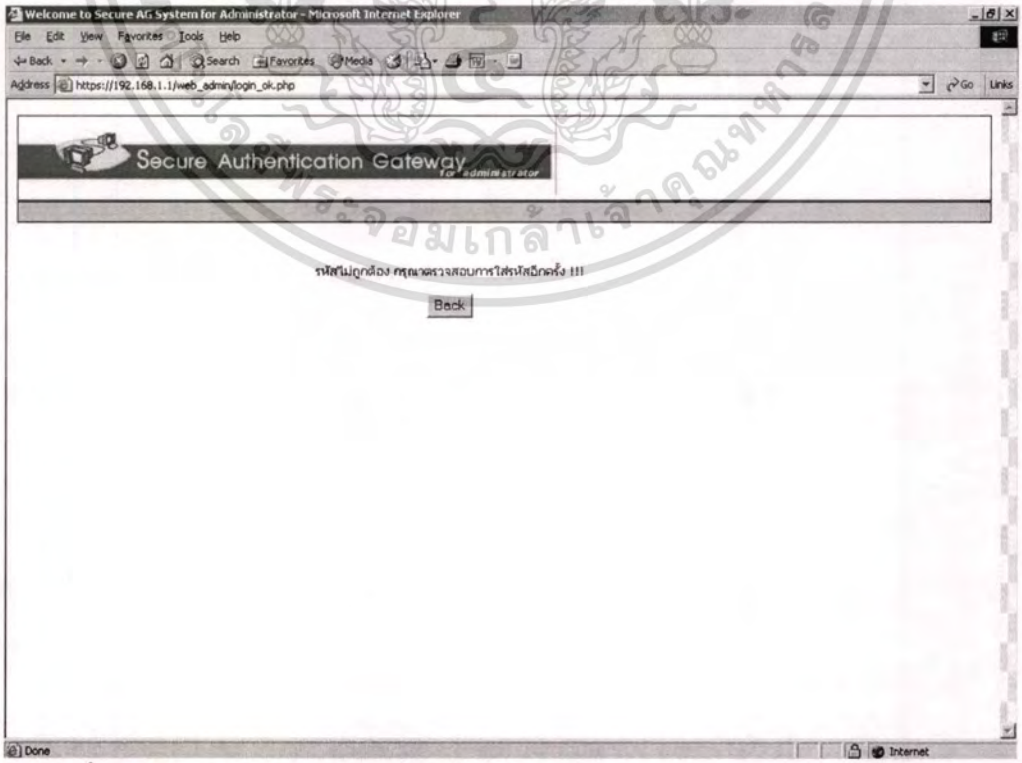
ในส่วนของการล็อกอินเข้าสู่ระบบควบคุมดูแลนี้ จะมีการตรวจเช็คหมายเลขไอพีของเครื่องที่จะเข้าทำการใช้งานระบบด้วย โดยถ้าเครื่องของผู้ดูแลไม่มีสิทธิ์เข้าใช้งานในระบบ ระบบจะทำการแจ้งเตือนให้ทราบ โดยปรากฏหน้าจอตามรูปที่ 36

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 36 แสดงหน้าจอการแจ้งเตือนของระบบล็อกอินเมื่อเครื่องผู้ดูแลไม่มีสิทธิ์ในการเข้าใช้งาน

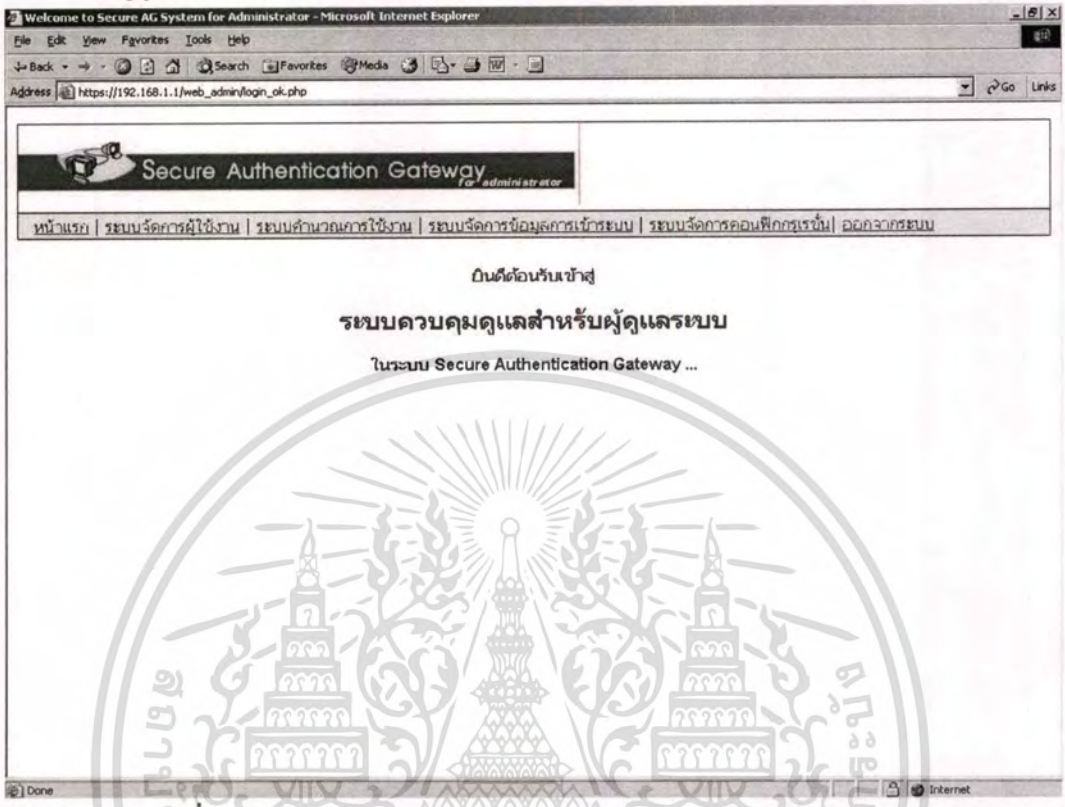
นอกจากนี้ถ้าผู้ดูแลระบบใส่รหัสผ่านผิด ระบบก็จะทำการแจ้งเตือน ดังรูปที่ 37



รูปที่ 37 แสดงหน้าจอการแจ้งเตือนเมื่อผู้ดูแลระบบใส่รหัสผ่านผิดในการเข้าสู่ระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

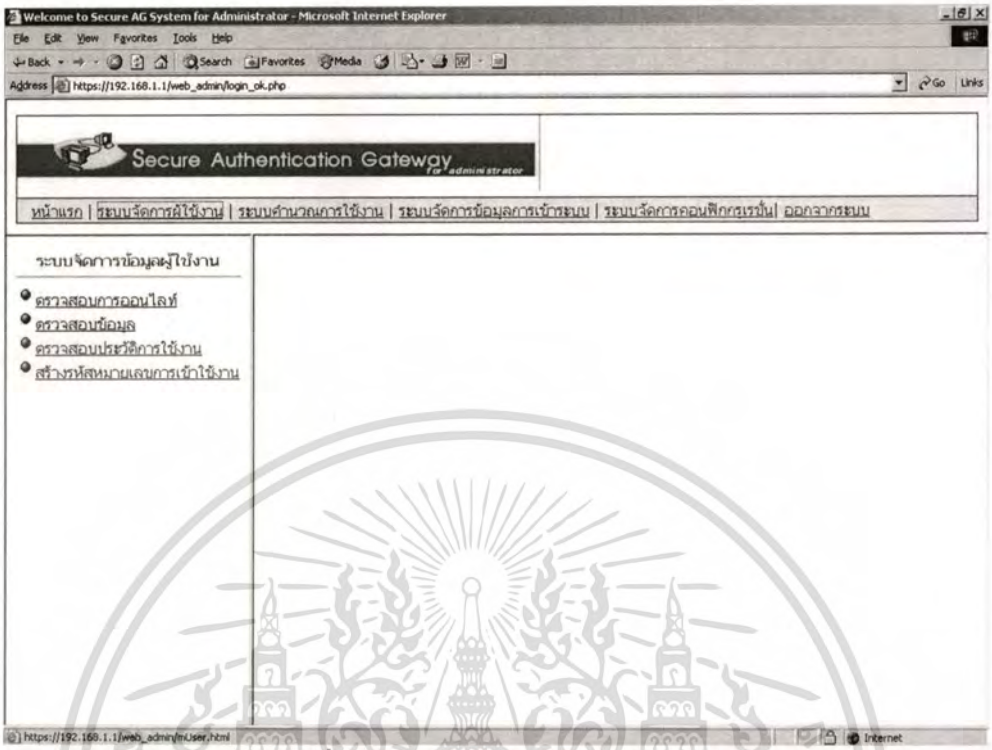
เมื่อผู้ดูแลระบบทำการล็อกอินเข้าสู่ระบบควบคุมดูแลได้แล้ว จะปรากฏหน้าจอดังรูป 38



รูปที่ 38 แสดงหน้าจอการเข้าสู่ระบบควบคุมดูแลสำหรับผู้ดูแลระบบ

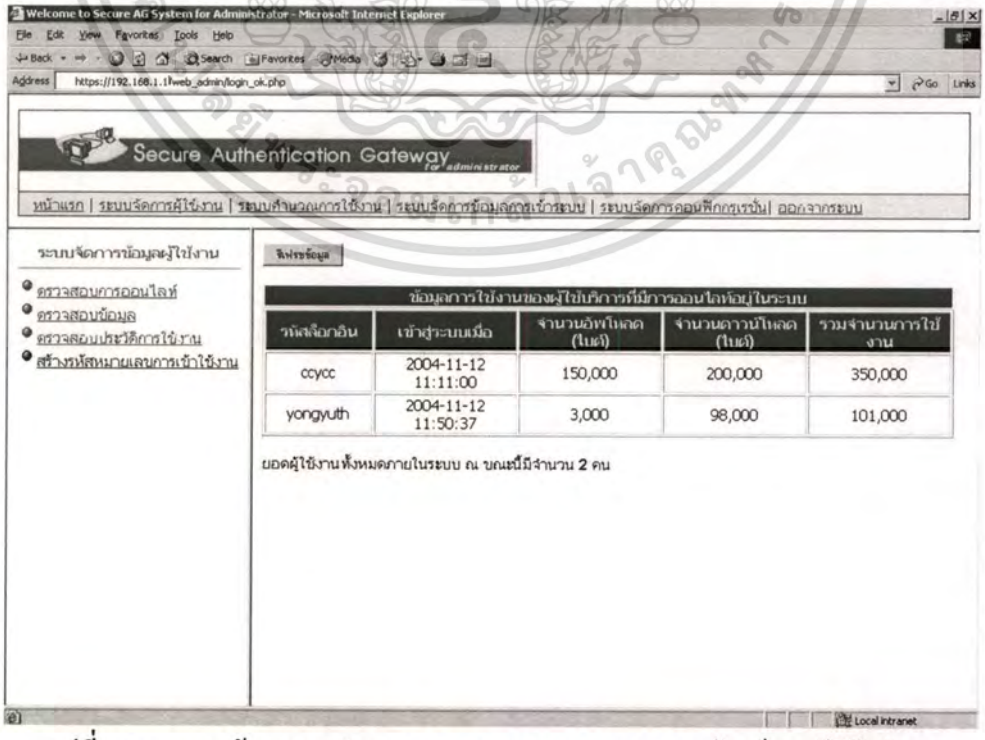
โดยการทำงานภายในระบบควบคุมดูแลนี้ ผู้ดูแลสามารถที่จะเลือกทำงานได้จากการคลิกเลือกที่เมนู ซึ่งแต่ละการทำงานของระบบ จะมีการทำงานย่อย ๆ ให้ผู้ดูแลระบบได้เลือกอีก ถ้าผู้ดูแลระบบเลือกที่จะทำงานเกี่ยวกับผู้ใช้บริการ ก็ทำการคลิกเลือกที่ระบบจัดการผู้ใช้ โดยจะปรากฏหน้าจอดังรูป 39

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 39 แสดงหน้าจอของระบบจัดการผู้ใช้งาน

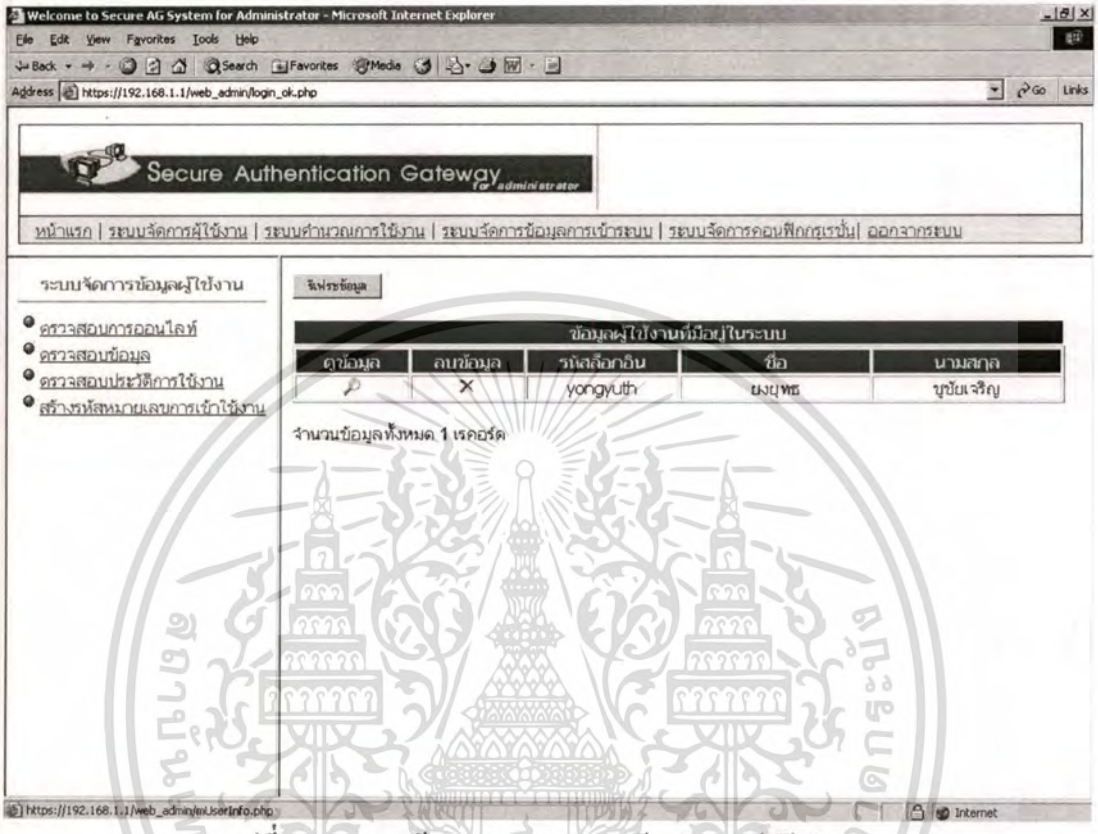
ผู้ดูแลระบบทำการเลือกทำการตรวจสอบการออนไลท์ของผู้ใช้บริการ จะปรากฏหน้าจอดัง รูปที่ 40



รูปที่ 40 แสดงหน้าจอการทำงานของการตรวจสอบการออนไลท์ของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผู้ดูแลระบบเลือกที่จะทำการตรวจสอบข้อมูลของผู้ใช้บริการ สามารถเลือกคลิกได้ที่เมนู โดยจะปรากฏหน้าจอ ดังรูปที่ 41



รูปที่ 41 แสดงหน้าจอการตรวจสอบข้อมูลของผู้ใช้บริการ

สำหรับการตรวจสอบข้อมูลของผู้ใช้บริการนั้น ผู้ดูแลระบบสามารถเลือกที่จะทำการดูข้อมูลของผู้ใช้บริการหรือลบข้อมูลของผู้ใช้บริการได้ โดยถ้าผู้ดูแลระบบเลือกที่จะทำการดูข้อมูลก็ให้ทำการเลือกที่ไอคอนรูปแว่นขยาย จะปรากฏหน้าจอ ตามรูปที่ 6.42

รูปที่ 42 แสดงตัวอย่างหน้าจอการแสดงข้อมูลของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แต่ถ้าผู้ดูแลระบบต้องการที่จะทำการลบข้อมูล ระบบจะมีการแสดงหน้าจอเพื่อยืนยันการลบข้อมูล ดังรูปที่ 43

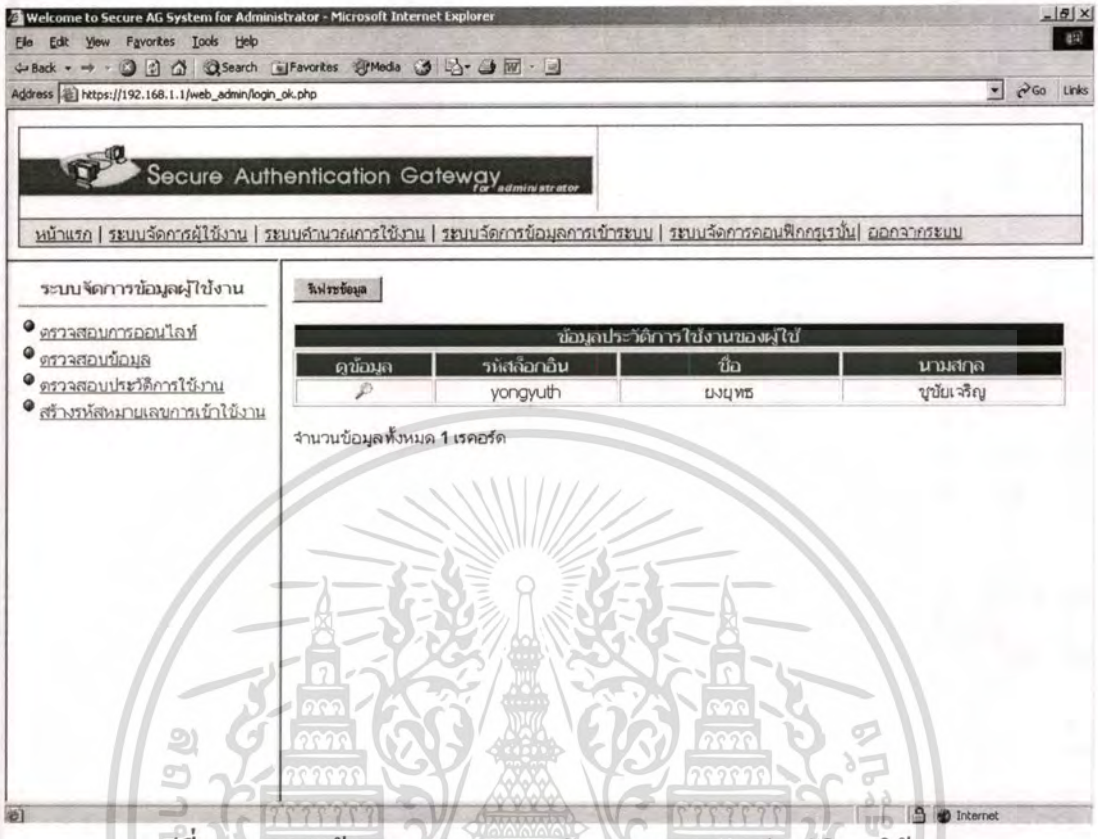
รูปที่ 43 แสดงหน้าจอยืนยันการลบข้อมูลของผู้ใช้บริการออกจากระบบ

หลังจากผู้ดูแลระบบยืนยันการลบข้อมูลระบบแล้ว ระบบจะทำการลบข้อมูลออกจากระบบ และทำการแสดงการลบข้อมูลเรียบร้อย ตามรูปที่ 44

รูปที่ 44 แสดงหน้าจอการลบข้อมูลของผู้ใช้บริการเรียบร้อยแล้ว

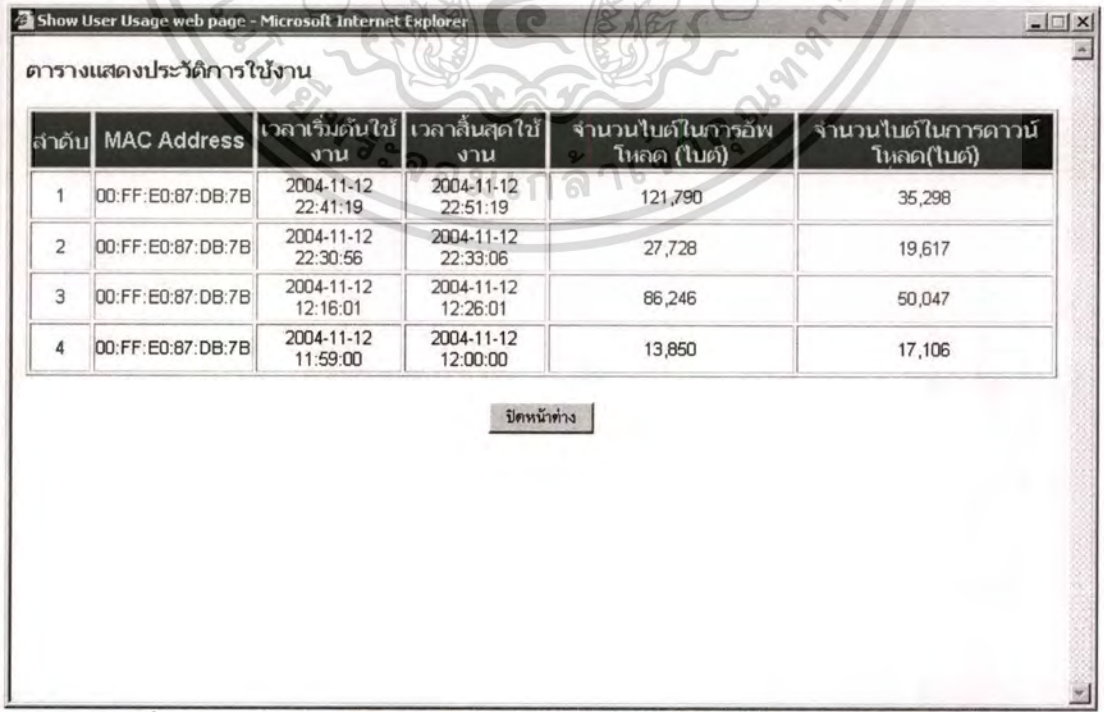
ถ้าผู้ดูแลระบบเลือกที่ทำการตรวจสอบประวัติการใช้งานของผู้ใช้ สามารถเลือกคลิกทำงานได้ที่เมนู โดยจะปรากฏหน้าจอดังรูป 45

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 45 แสดงหน้าจอการทำงานสำหรับการตรวจสอบประวัติการใช้งาน

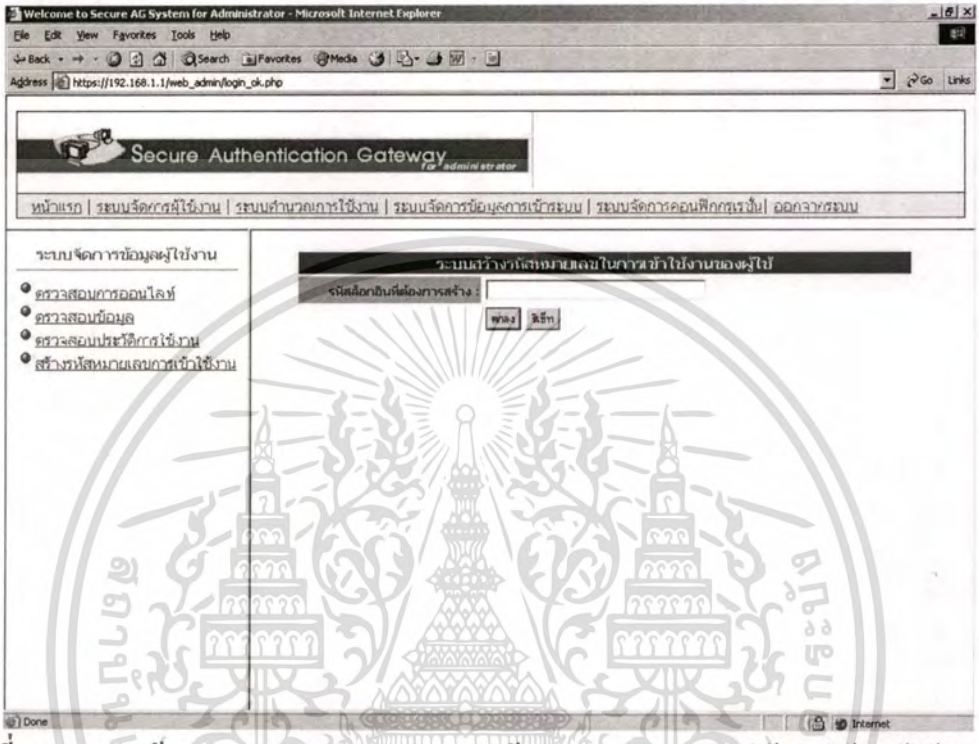
หลังจากที่ผู้ดูแลระบบทำการเลือกผู้ใช้บริการเพื่อดูประวัติการใช้งาน จะปรากฏหน้าจอดังรูป 46



รูปที่ 46 แสดงหน้าจอข้อมูลประวัติการใช้งานที่ผู้ดูแลระบบเลือกที่จะตรวจสอบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

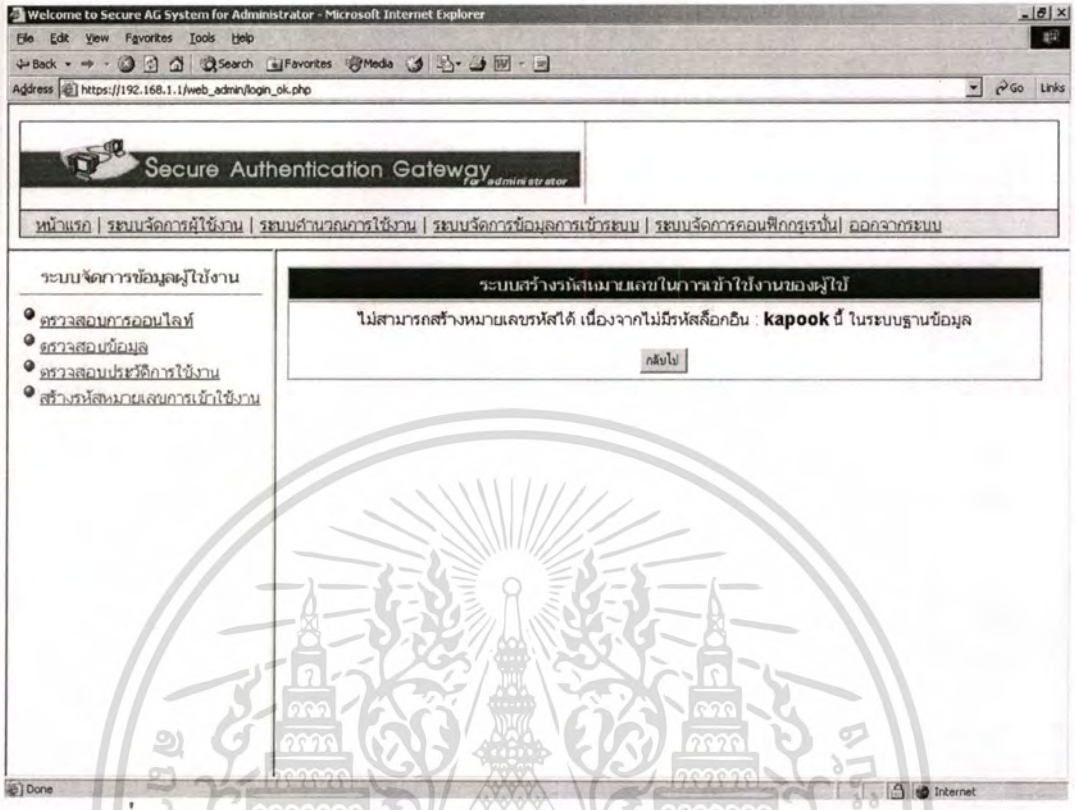
ถ้าผู้ดูแลระบบเลือกที่จะทำการสร้างหมายเลขรหัสการใช้งานให้กับผู้ใช้บริการที่เข้ามาขอ จะปรากฏหน้าจอ ดังรูปที่ 47



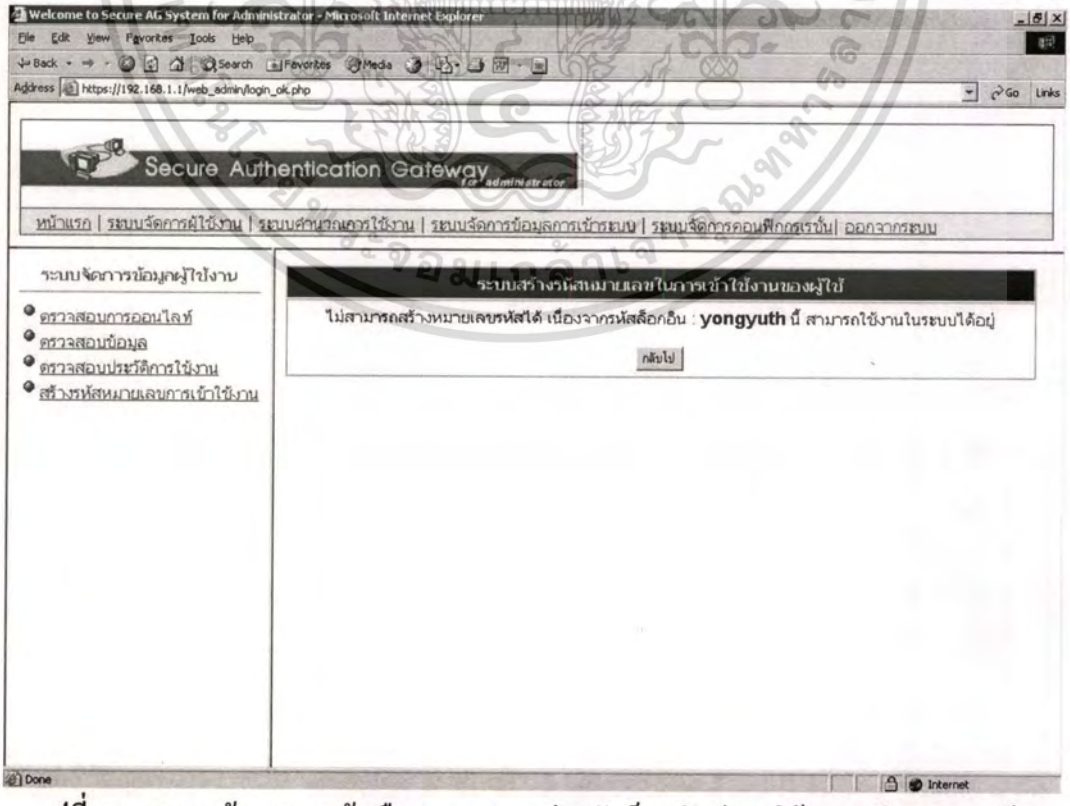
รูปที่ 47 แสดงหน้าจอการทำงานของระบบการสร้างหมายเลขรหัสการใช้งานให้กับผู้ใช้บริการ

โดยภายในระบบการสร้างหมายเลขรหัสการใช้งานนั้น จะมีการตรวจสอบข้อมูลของรหัสล็อกอินที่กรอกว่ามีอยู่ในระบบฐานข้อมูลหรือไม่ โดยถ้ารหัสล็อกอินนั้นไม่มีอยู่ในระบบจะแจ้งเตือนให้ผู้ดูแลระบบได้ทราบ ตามรูปที่ 48 และถ้ารหัสล็อกอินนี้มีการใช้งานอยู่ในระบบอยู่แล้ว ระบบก็จะแจ้งเตือนเช่นกัน ตามรูปที่ 49

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



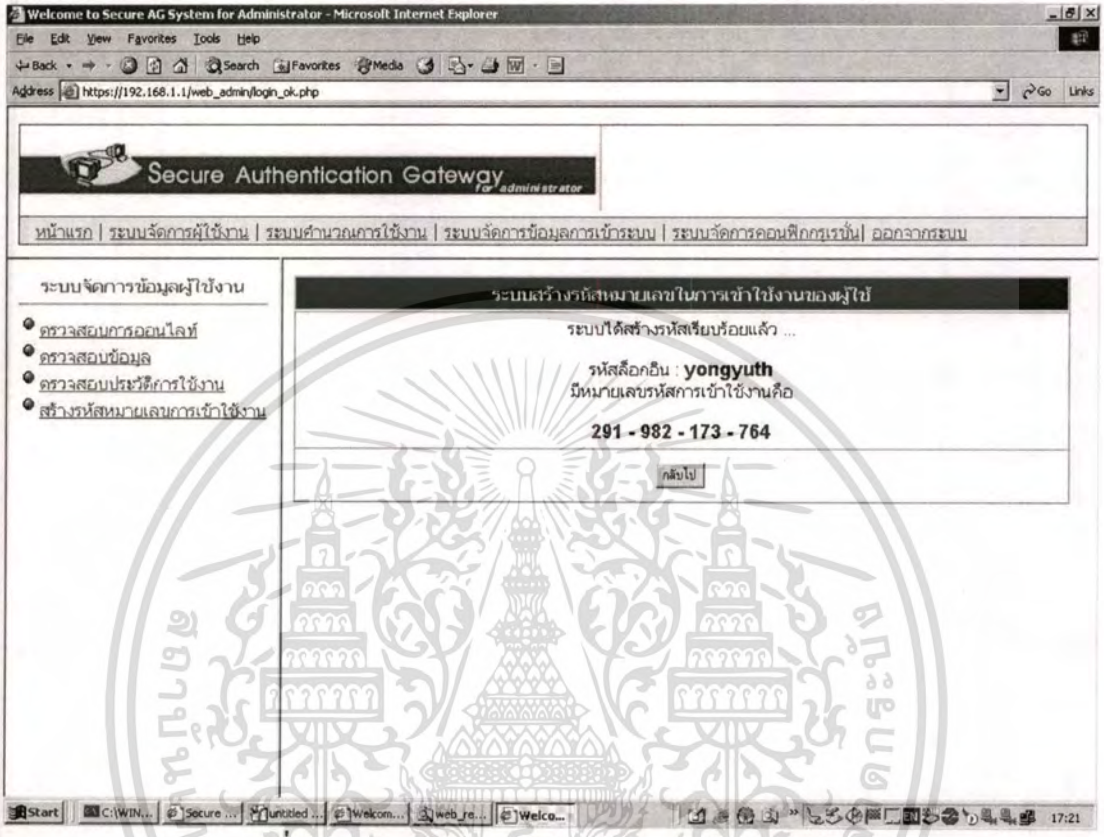
รูปที่ 48 แสดงหน้าจอการแจ้งเตือนของระบบว่ารหัสล็อกอินไม่มีอยู่ในฐานข้อมูล



รูปที่ 49 แสดงหน้าจอการแจ้งเตือนของระบบว่ารหัสล็อกอินมีการใช้งานอยู่ในระบบแล้ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ ดัดแปลง เผยแพร่ หรือจำหน่ายในเชิงการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

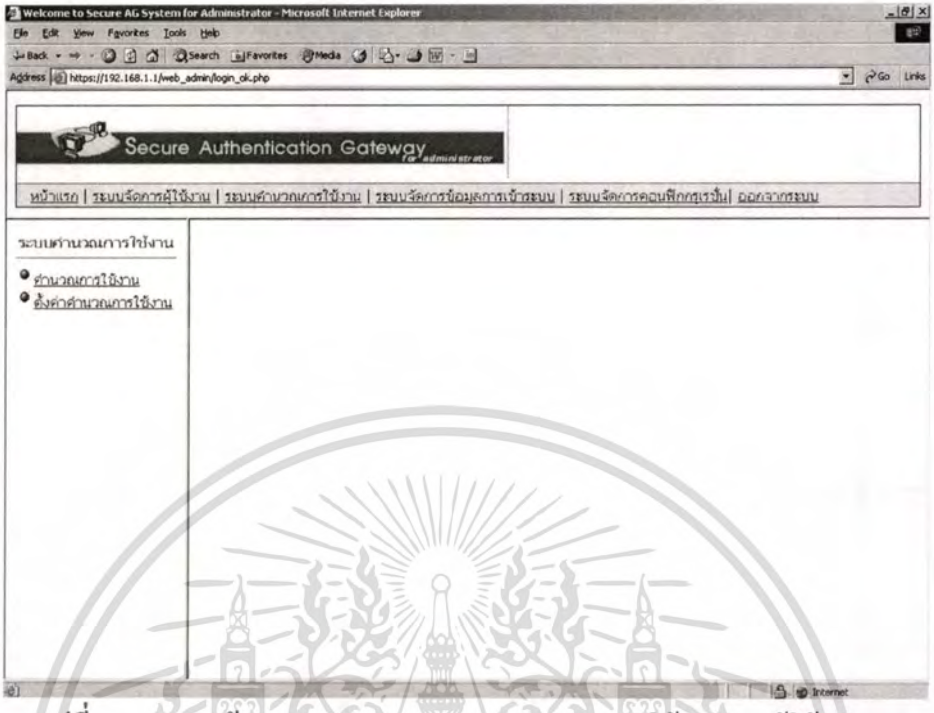
แต่ถ้าระบบตรวจสอบความถูกต้องต่าง ๆ ผ่านแล้ว ระบบจะทำการสร้างหมายเลขรหัสการใช้งานให้กับผู้ใช้บริการรายนั้น ๆ ตามหน้าจอที่ 50



รูปที่ 50 แสดงหน้าจอการสร้างหมายเลขรหัสการใช้งาน

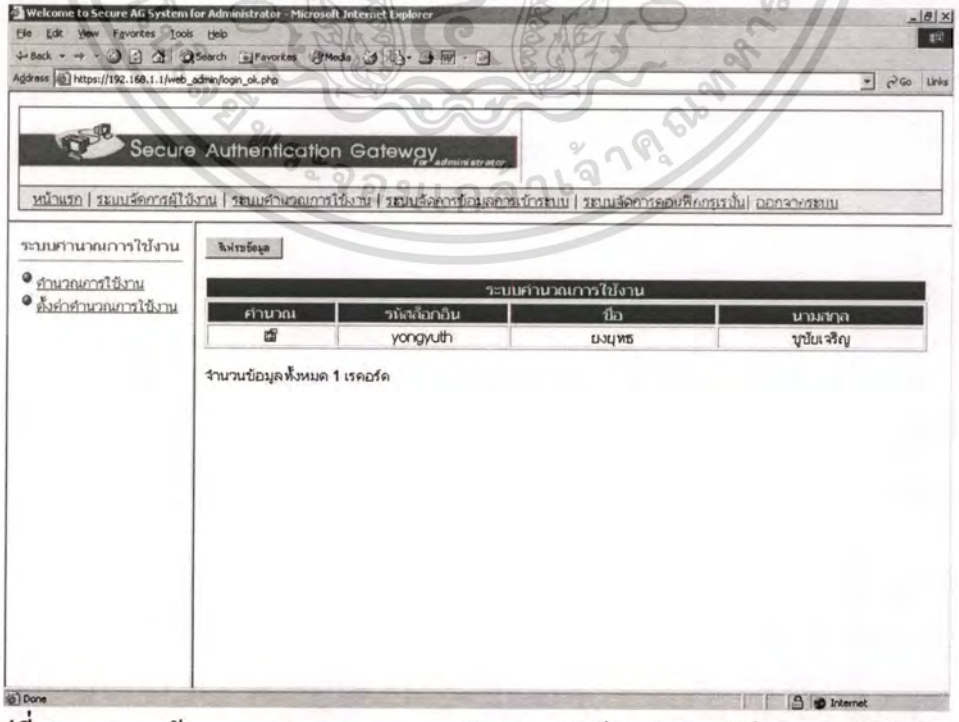
ถ้าผู้ดูแลระบบต้องการที่จะทำงานในระบบคำนวณการใช้งานของผู้ใช้บริการ สามารถเลือกคลิกที่เมนู โดยจะปรากฏหน้าจอดังรูป 51

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 51 แสดงหน้าจอการทำงานของระบบคำนวณการใช้งานของผู้ใช้บริการ

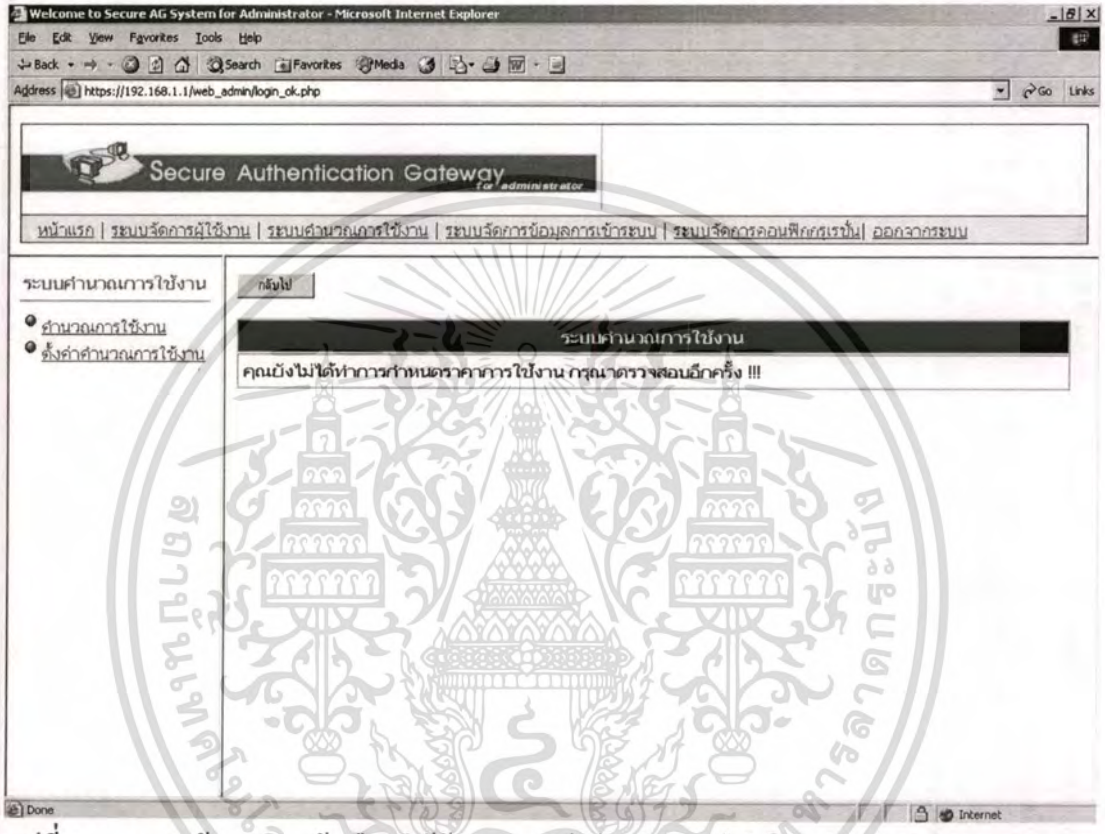
ภายในระบบคำนวณการใช้งานของผู้ใช้บริการ จะมีการทำงานที่ให้ผู้ดูแลระบบเลือกทำคือ การคำนวณค่าใช้จ่ายในการใช้งานและการกำหนดค่าคำนวณการใช้งาน โดยถ้าผู้ดูแลระบบเลือกที่จะทำการคำนวณค่าใช้จ่ายในการใช้งานของผู้ใช้บริการ จะปรากฏหน้าจอดังรูปที่ 6.52



รูปที่ 52 แสดงหน้าจอการทำงานของระบบคำนวณค่าใช้จ่ายในการใช้งานของผู้ใช้บริการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

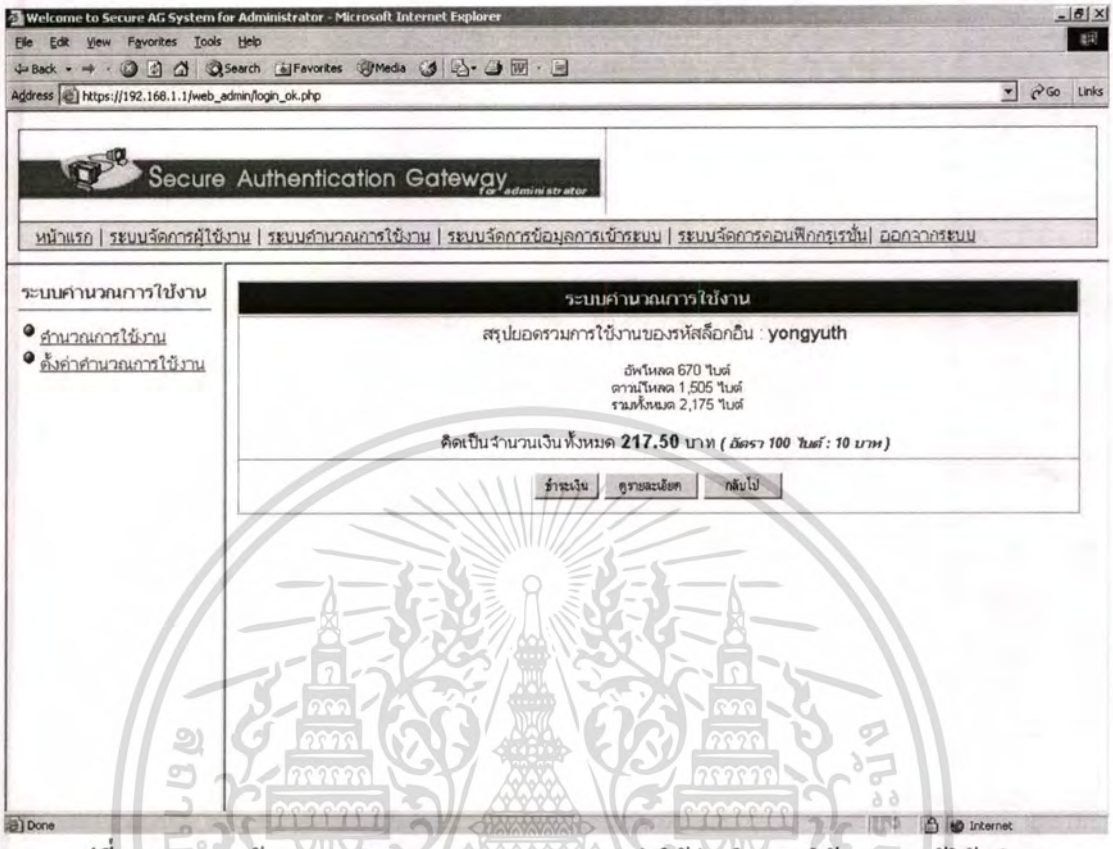
ภายในตัวระบบการคำนวณค่าใช้จ่ายในการใช้งานนี้ จะมีการตรวจเช็คค่าต่าง ๆ ที่ใช้ในการคำนวณ โดยถ้าระบบไม่มีค่าในการคำนวณจะมีการแจ้งให้ผู้ดูแลระบบได้ทราบ เพื่อให้ผู้ดูแลระบบกำหนดค่าที่ใช้ในการคำนวณค่าใช้จ่ายในการใช้งาน โดยหน้าจอการแจ้งเตือนจะเป็นไปตามรูปที่ 53



รูปที่ 53 แสดงหน้าจอการแจ้งเตือนให้ผู้ดูแลระบบได้ทราบว่ายังไม่มีการกำหนดค่าในการคำนวณการใช้งาน

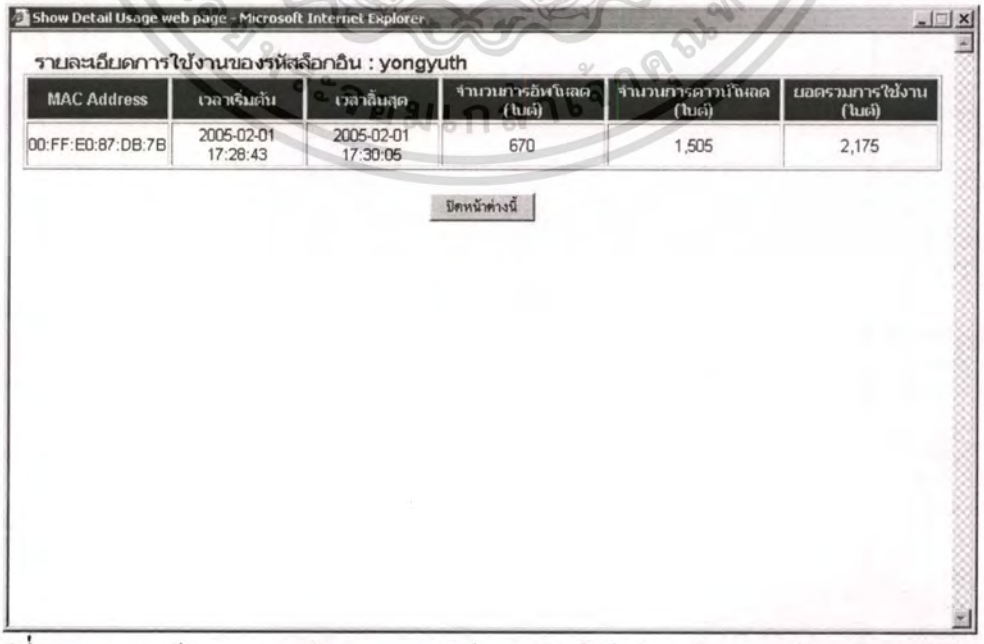
แต่ถ้าระบบมีค่าการคำนวณอยู่แล้ว ผู้ดูแลสามารถที่จะเลือกคำนวณค่าใช้จ่ายในการใช้งานของผู้ใช้บริการได้ โดยจะปรากฏหน้าจอดังรูป 54 โดยจะมีการแสดงจำนวนการใช้งานและค่าใช้จ่ายที่ผู้ใช้บริการต้องจ่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 54 แสดงหน้าจอการทำงานของระบบคำนวณค่าใช้จ่ายในการใช้งานของผู้ใช้บริการ

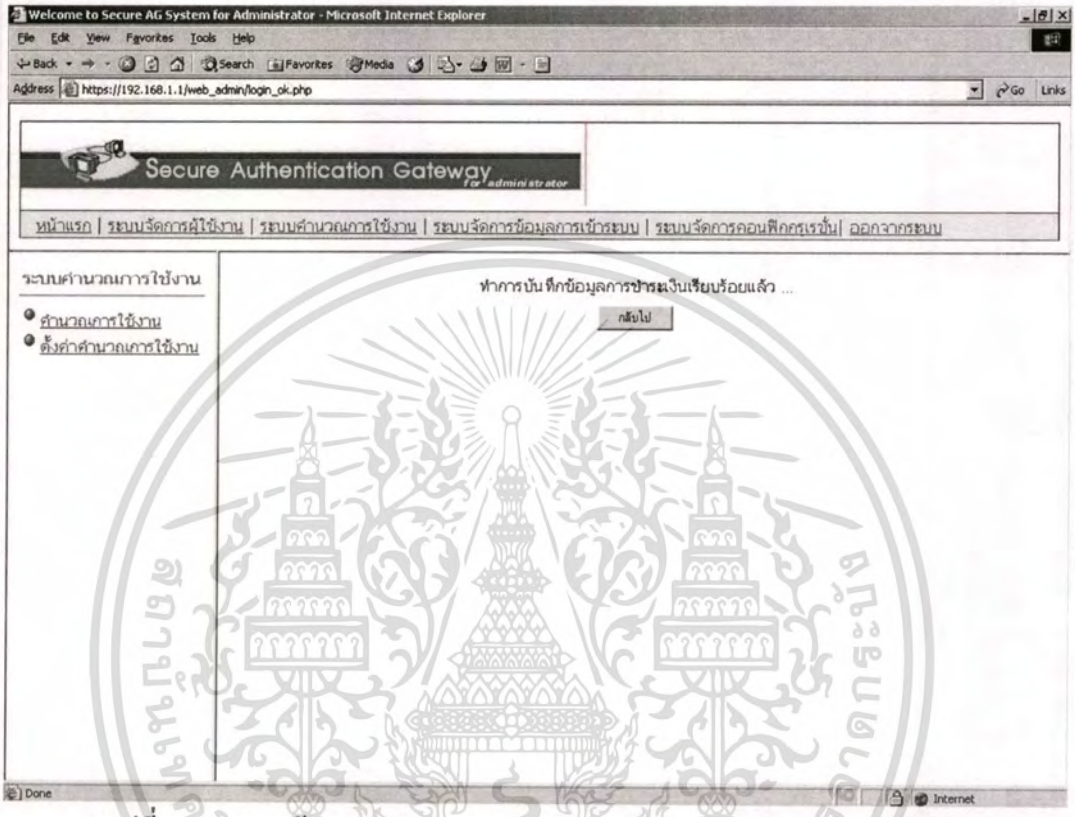
ในการแสดงค่าใช้จ่ายในการใช้งานของระบบนั้น จะมีปุ่มที่ให้ผู้ดูแลตรวจสอบดูรายละเอียดของการใช้งานได้ โดยกดที่ปุ่ม ดูรายละเอียด ซึ่งจะปรากฏหน้าจอดังรูปที่ 55



รูปที่ 55 แสดงหน้าจอรายละเอียดของการใช้งานของผู้ใช้บริการในระบบคำนวณการใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

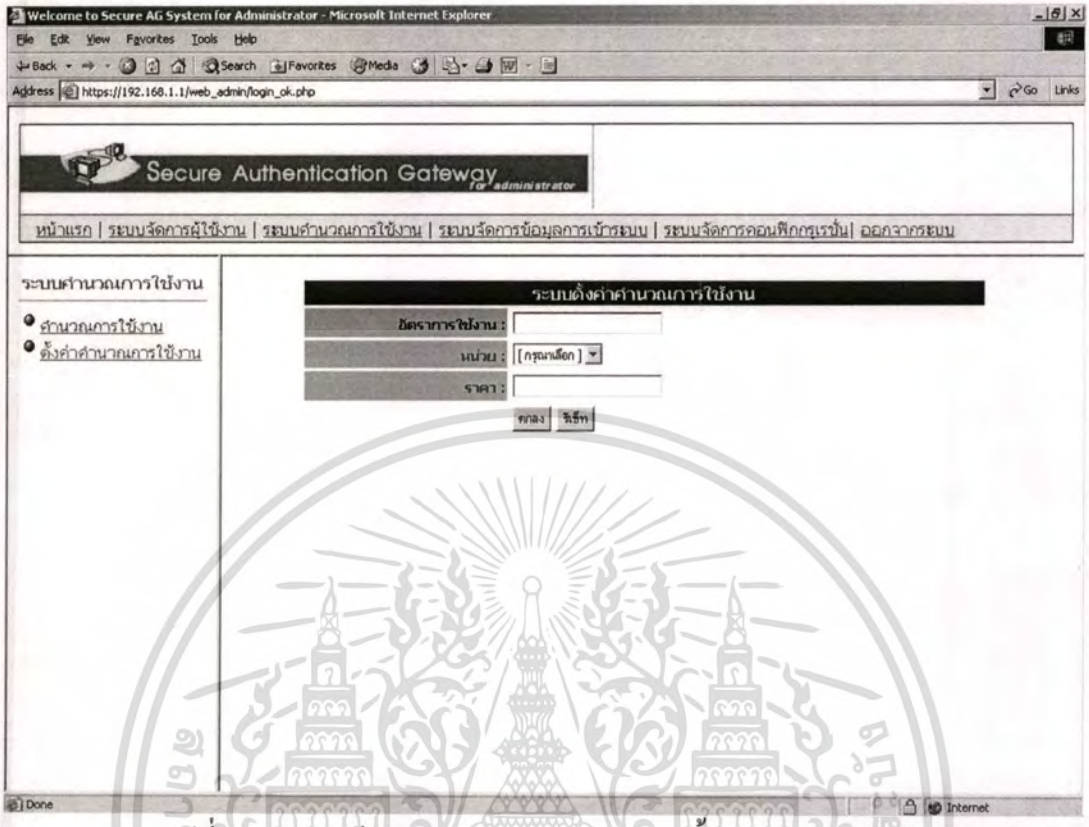
เมื่อผู้ใช้บริการได้ทำการชำระเงินเรียบร้อยแล้ว ผู้ดูแลระบบจะทำการกดที่ปุ่ม ชำระเงิน เพื่อให้ระบบตัดยอดการคำนวณค่าใช้จ่ายของผู้ใช้บริการรายนั้น ๆ ออกไป โดยจะปรากฏหน้าจอดังรูปที่ 56



รูปที่ 56 แสดงหน้าจอการทำงานของการชำระเงินในระบบคำนวณการใช้งาน

ผู้ดูแลระบบสามารถจะเลือกตั้งค่าคำนวณการใช้งานได้ จากการเลือกกดที่เมนู ซึ่งจะปรากฏหน้าจอดังรูป 57

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



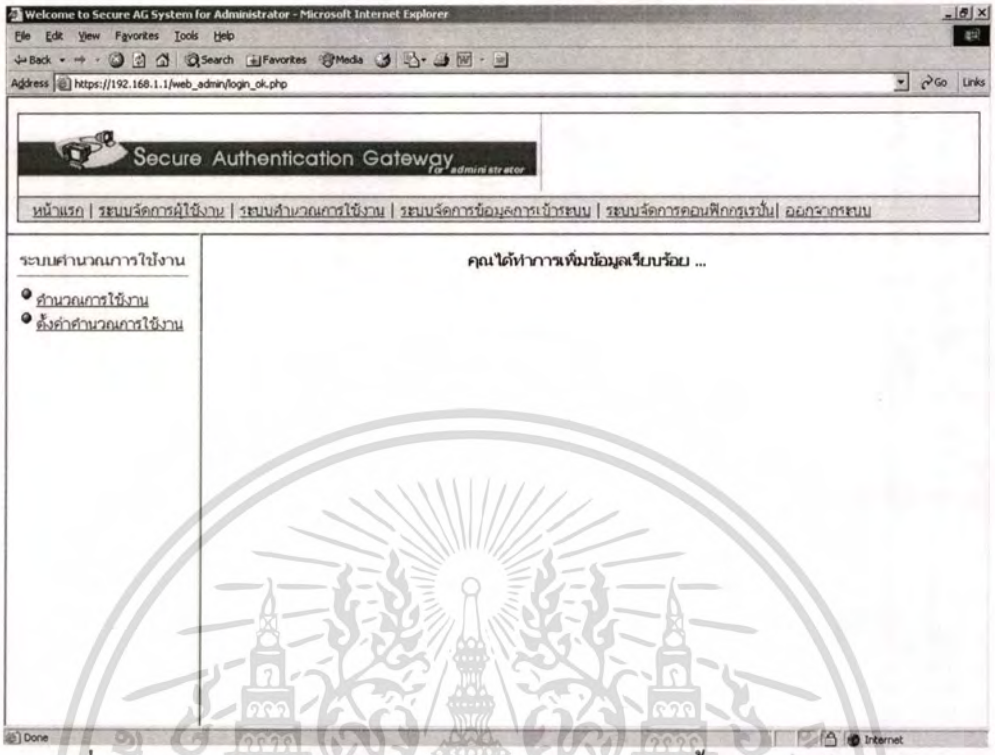
รูปที่ 57 แสดงหน้าจอการทำงานของระบบการตั้งค่าคำนวณการใช้งาน

ในระบบการตั้งค่าคำนวณการใช้งานนั้น จะมีการตรวจเช็คข้อมูลว่ามีการกรอกได้ครบถ้วนถูกต้องหรือไม่ โดยถ้าระบบมีการเช็คว่าข้อมูลไม่ครบถ้วน ถูกต้องจะมีการแจ้งเตือนให้ผู้ดูแลระบบได้ทราบ โดยจะมีตัวอย่างหน้าจอตามรูปที่ 58

รูปที่ 58 แสดงตัวอย่างหน้าจอการแจ้งเตือนของระบบตั้งค่าคำนวณการใช้งานเมื่อพบว่าข้อมูลไม่ถูกต้อง ครบถ้วน

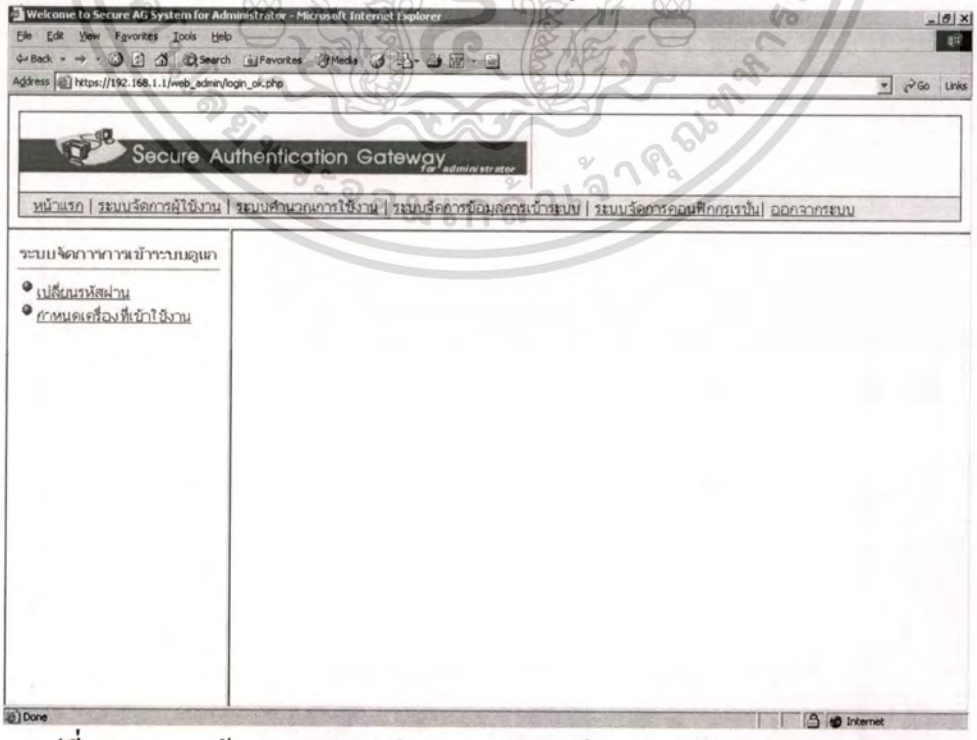
แต่ถ้าข้อมูลที่ผู้ดูแลระบบกรอกครบถ้วน ถูกต้องระบบจะแสดงข้อความการบันทึกข้อมูลเข้าสู่ระบบฐานข้อมูลเรียบร้อย ตามรูป 59

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 59 แสดงหน้าจอข้อความการบันทึกข้อมูลของระบบตั้งค่าคำนวณการใช้งาน

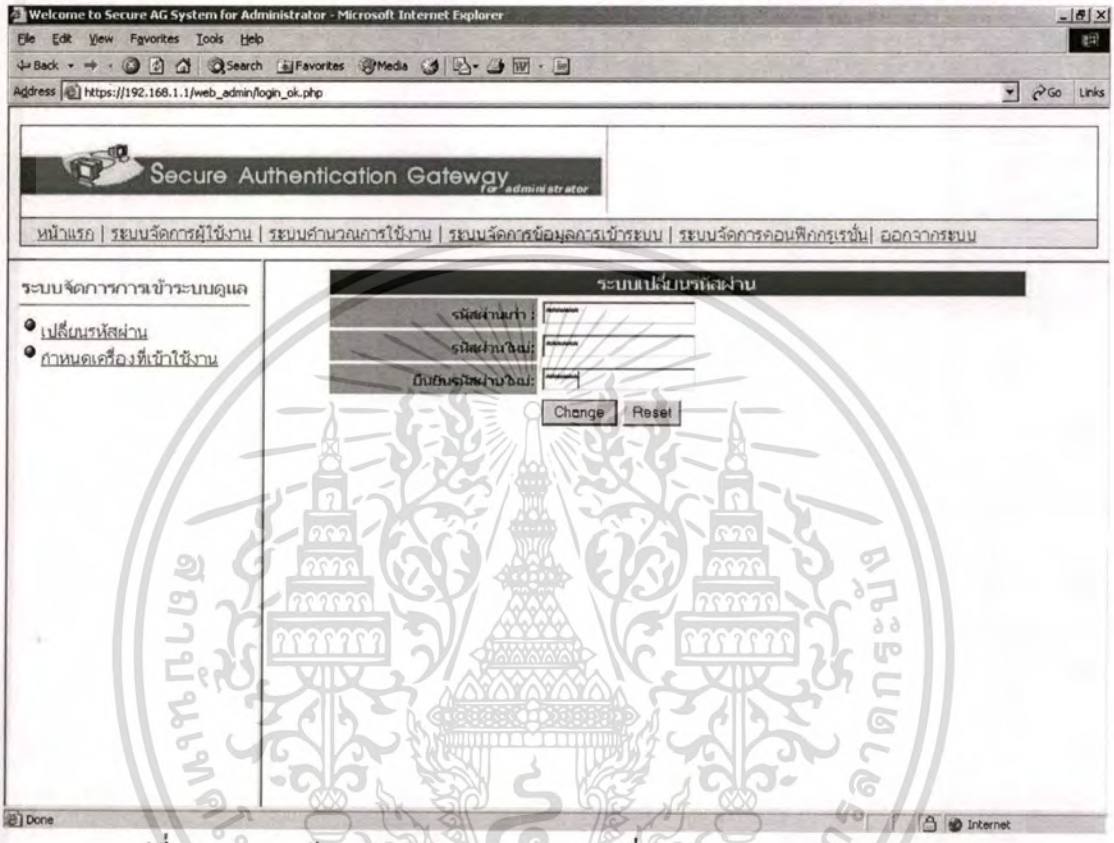
ถ้าผู้ดูแลระบบต้องการทำงานในระบบจัดการข้อมูลการเข้าสู่ระบบควบคุมดูแล ผู้ดูแลสามารถที่จะเลือกคลิกได้ที่เมนู โดยจะปรากฏหน้าจอดังรูป 60



รูปที่ 60 แสดงหน้าจอการทำงานในระบบจัดการข้อมูลการเข้าสู่ระบบควบคุมดูแล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภายในระบบจัดการข้อมูลการเข้าสู่ระบบควบคุมดูแลนี้ จะมีการทำงานอยู่ 2 ระบบย่อยคือ ระบบเปลี่ยนรหัสผ่านสำหรับผู้ดูแลระบบ และระบบกำหนดเครื่องในการเข้าใช้งานในระบบ โดย ถ้าผู้ดูแลระบบเลือกที่จะทำการเปลี่ยนรหัสผ่าน สามารถคลิกที่เมนู จะปรากฏหน้าจอดังรูป 61



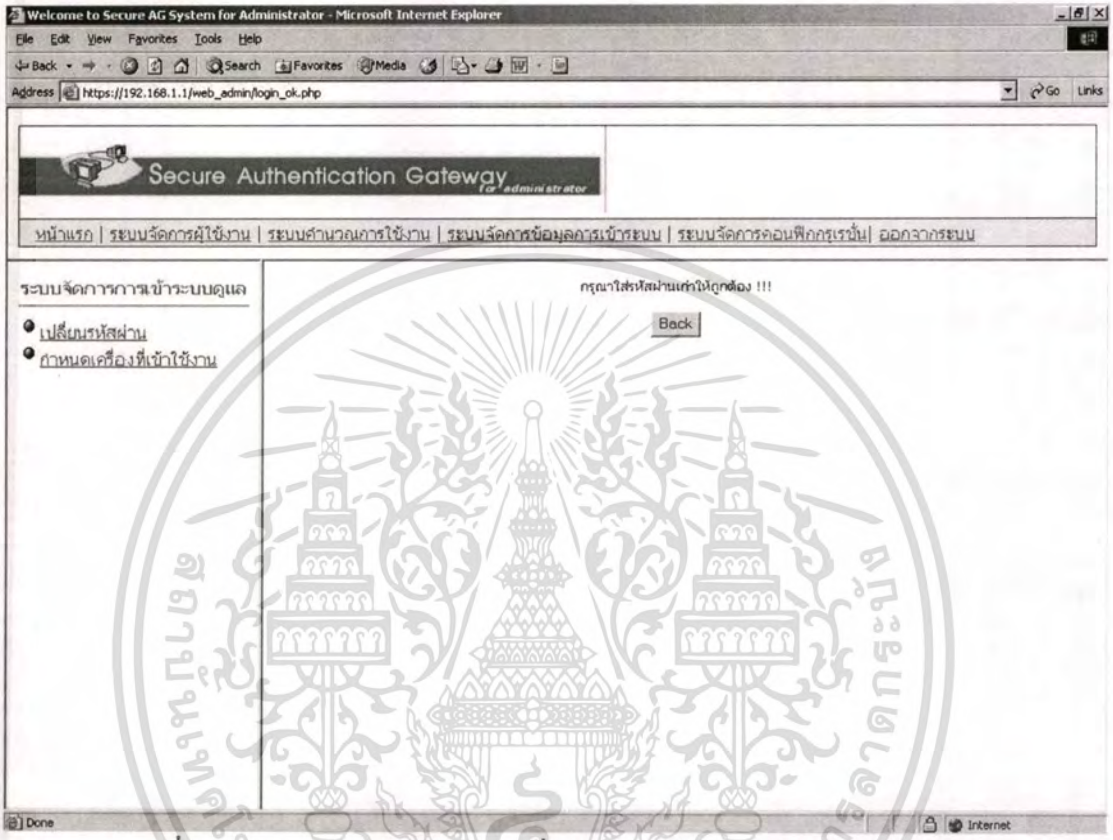
รูปที่ 61 แสดงหน้าจอการทำงานของระบบเปลี่ยนรหัสผ่านสำหรับผู้ดูแลระบบ

โดยภายในตัวระบบเปลี่ยนรหัสผ่านนี้จะมีการตรวจสอบข้อมูลที่ผู้ดูแลระบบได้ทำการกรอกว่าครบถ้วนหรือไม่ ถ้าหากว่าผู้ดูแลระบบกรอกข้อมูลไม่ครบถ้วน ระบบจะมีการแจ้งเตือน โดยจะปรากฏหน้าจอตัวอย่าง ตามรูปที่ 62

รูปที่ 62 แสดงหน้าจอการแจ้งเตือนเมื่อผู้ดูแลระบบใส่ข้อมูลไม่ครบในระบบเปลี่ยนรหัสผ่าน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

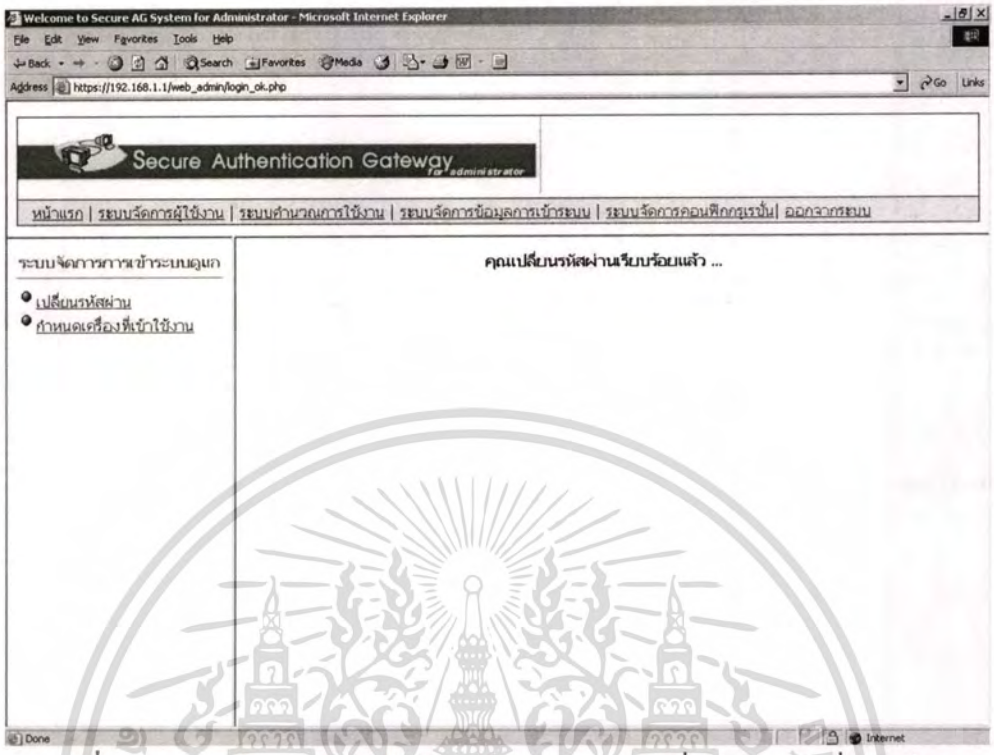
นอกจากนี้ ภายในตัวระบบเปลี่ยนรหัสผ่าน ยังมีการตรวจสอบข้อมูลของรหัสผ่านเดิม โดยถ้าผู้ดูแลระบบมีการใส่รหัสผ่านเดิมผิด ระบบจะมีการแจ้งเตือนให้ทำการใส่รหัสผ่านเดิมใหม่ โดยจะมีหน้าจอดังรูป 63



รูปที่ 63 แสดงหน้าจอการแจ้งเตือนเมื่อผู้ดูแลระบบทำการใส่รหัสผ่านเดิมผิด

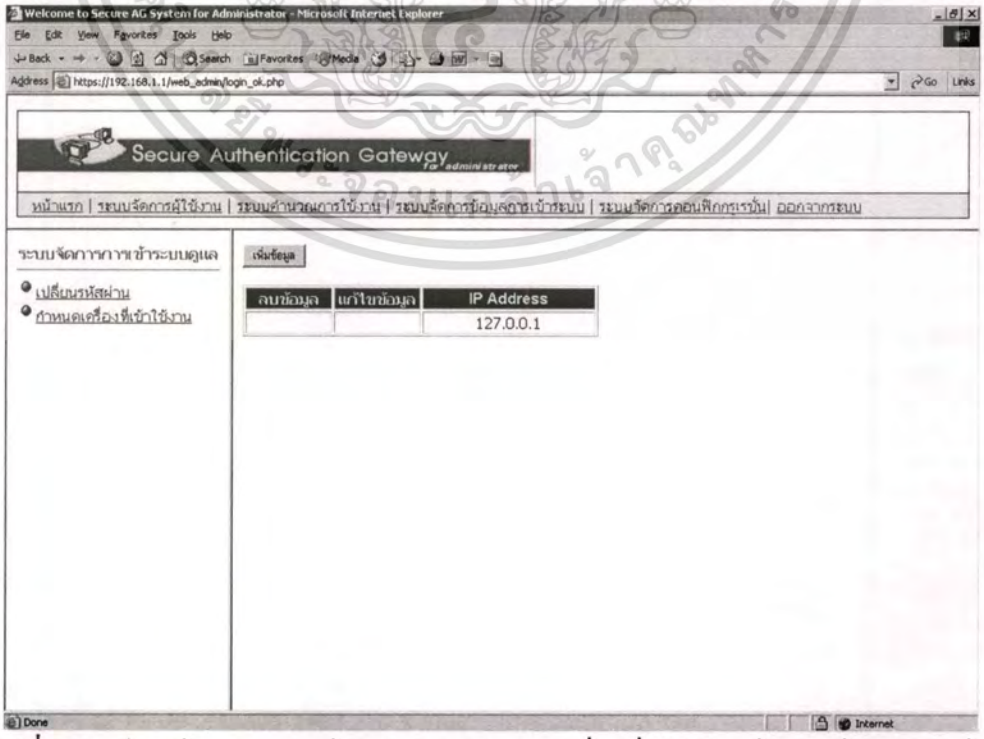
ถ้าผู้ดูแลระบบกรอกข้อมูลของการเปลี่ยนรหัสผ่านครบถ้วน ถูกต้องระบบจะแสดงการบันทึกข้อมูลใหม่ ตามรูปที่ 64

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 64 แสดงหน้าจอการบันทึกข้อมูลใหม่ของระบบเปลี่ยนรหัสผ่านที่เรียบร้อย

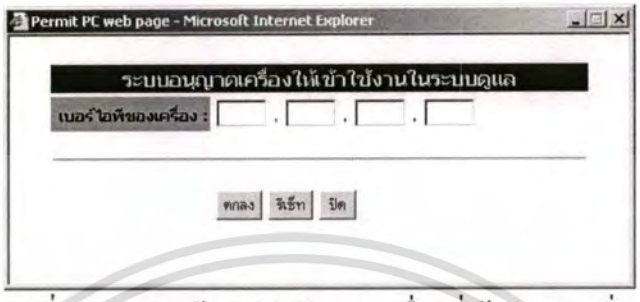
ถ้าผู้ดูแลระบบต้องการเลือกทำงานในระบบกำหนดเครื่องที่เข้าใช้งานในระบบควบคุมดูแล สามารถเลือกคลิกได้ที่เมนู โดยจะปรากฏหน้าจอดังรูป 65



รูปที่ 65 แสดงหน้าจอการทำงานของระบบกำหนดเครื่องที่เข้าใช้งานในระบบควบคุมดูแล

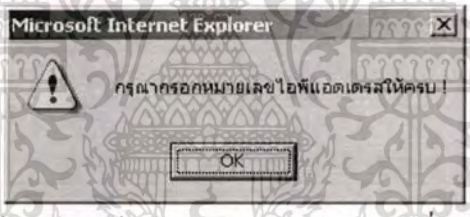
เอกสารนี้เป็นทรัพย์สินทางปัญญาของจุฬาลงกรณ์มหาวิทยาลัย ห้ามมิให้ทำซ้ำ ดัดแปลง เผยแพร่ หรือนำไปใช้ประโยชน์ทางการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภายในระบบกำหนดเครื่องที่เข้าใช้งานในระบบควบคุมดูแล ผู้ดูแลสามารถจะเลือกกำหนด แก้ไขและลบข้อมูลของระบบได้ โดยถ้าผู้ดูแลระบบทำการเลือกกำหนดเครื่องที่เข้าสู่ระบบเพิ่ม จะปรากฏหน้าจอ ตามรูป 66



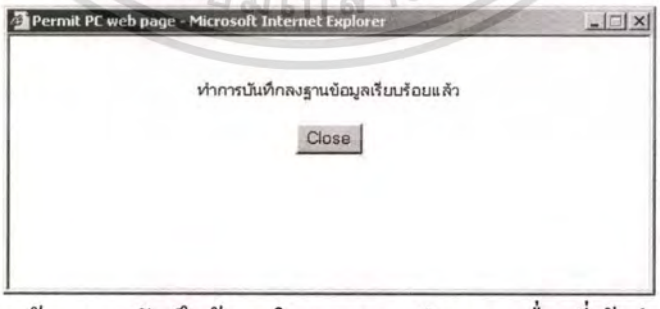
รูปที่ 66 แสดงหน้าจอการกำหนดเครื่องที่เข้าสู่ระบบเพิ่ม

โดยภายในระบบการเพิ่มข้อมูลของเครื่องนี้จะมีการตรวจสอบข้อมูลที่จะบันทึกลงในระบบด้วยว่ามีความครบถ้วนหรือไม่ หากไม่ครบถ้วนระบบจะมีการแจ้งเตือน โดยมีตัวอย่างหน้าจอการแจ้งเตือน ตามรูปที่ 67



รูปที่ 67 แสดงหน้าจอการแจ้งเตือนของระบบกำหนดเครื่องในการเข้าสู่ระบบ

แต่ถ้าข้อมูลที่กรอกมีความครบถ้วน ถูกต้องแล้วระบบจะมีการแสดงการบันทึกข้อมูลเข้าสู่ระบบฐานข้อมูลเรียบร้อย ตามที่ปรากฏในหน้าจอ รูปที่ 68

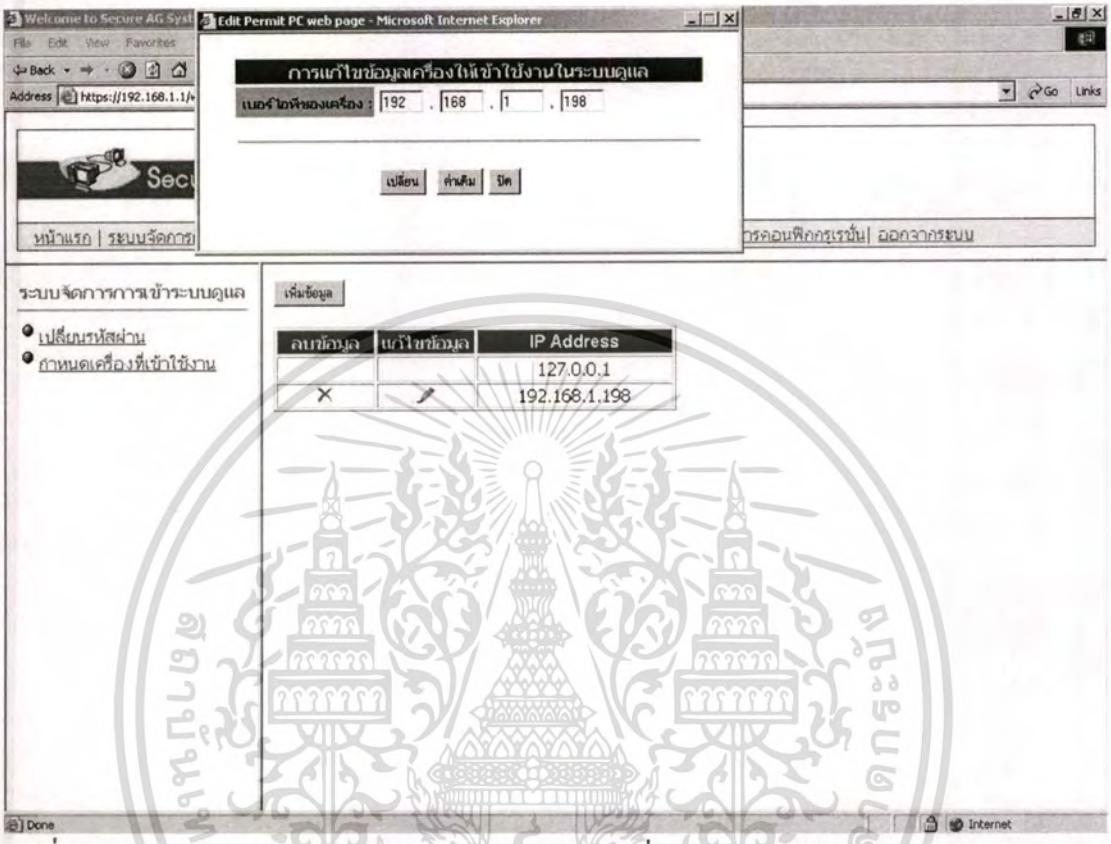


รูปที่ 68 แสดงหน้าจอการบันทึกข้อมูลในระบบการกำหนดเครื่องที่เข้าสู่ระบบเรียบร้อย

ถ้าผู้ดูแลระบบต้องการแก้ไขข้อมูลในระบบกำหนดเครื่องในการเข้าใช้งานในระบบควบคุมดูแล ก็สามารถเลือกที่จะแก้ไขข้อมูลโดยทำการกดคลิกที่ไอคอนรูปแว่นขยายได้ โดยจะ

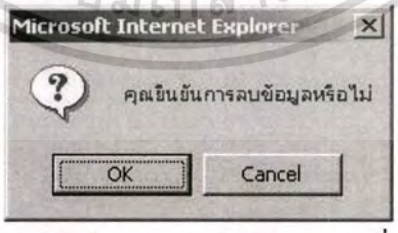
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปรากฏหน้าจอตามรูปที่ 69 ซึ่งการตรวจสอบข้อมูลก่อนการบันทึกข้อมูลจะมีการทำงานเหมือนกับการกำหนดเครื่องเพิ่ม



รูปที่ 69 แสดงหน้าจอการแก้ไขข้อมูลในระบบกำหนดเครื่องในการเข้าใช้งานในระบบควบคุมดูแล

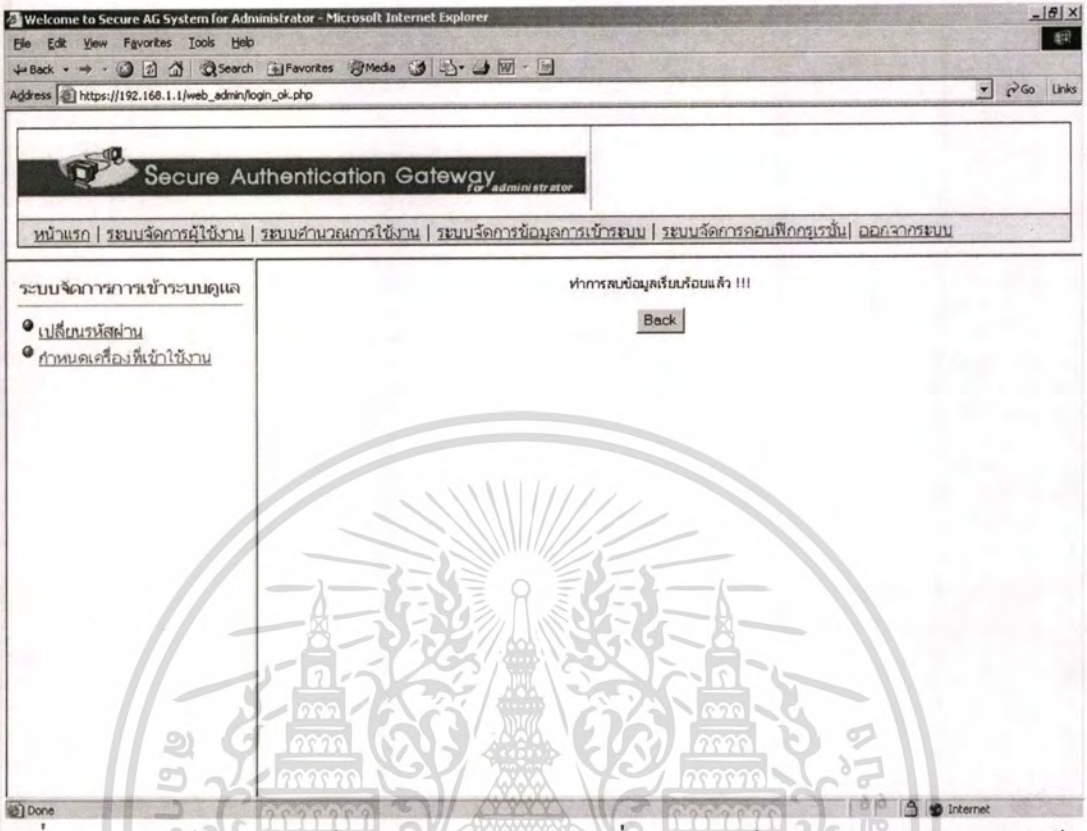
แต่ถ้าผู้ดูแลระบบต้องการเลือกที่จะลบข้อมูลในระบบกำหนดเครื่องในการเข้าใช้งานในระบบควบคุมดูแล ก็จะปรากฏหน้าจอการยืนยันการลบข้อมูลขึ้น ตามรูปที่ 70



รูปที่ 70 แสดงหน้าจอยืนยันการลบข้อมูลของระบบกำหนดเครื่องในการเข้าใช้งานในระบบควบคุมดูแล

เมื่อระบบทำการลบข้อมูลเรียบร้อยแล้ว ระบบจะแสดงหน้าจอเพื่อให้ผู้ดูแลได้ทราบ โดยหน้าจอจะเป็นไปตามรูป 71

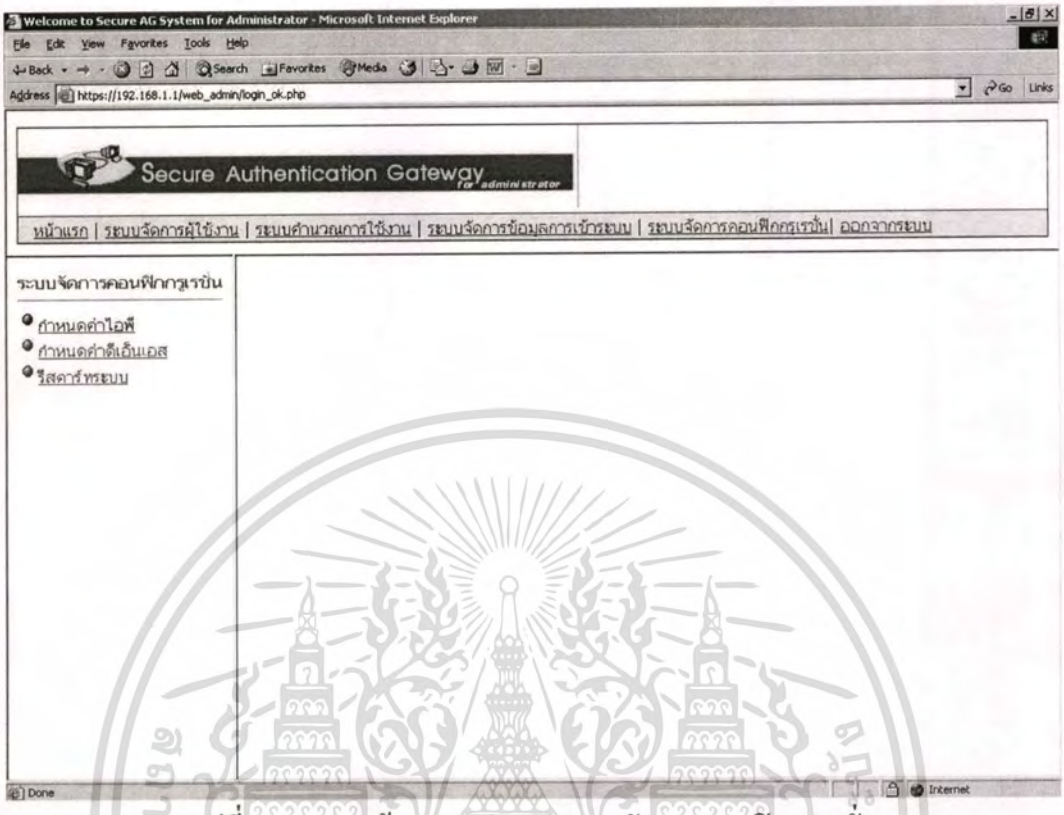
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 71 แสดงหน้าจอการลบข้อมูลของระบบกำหนดเครื่องในการเข้าสู่ระบบควบคุมดูแลเรียบร้อย

ถ้าผู้ดูแลระบบต้องการที่จะเข้าทำงานในระบบจัดการคอนฟิกกรูเรชั่น ก็สามารถเลือกทำงานได้จากกดคลิกที่เมนู ซึ่งจะปรากฏหน้าจอดังรูป 72

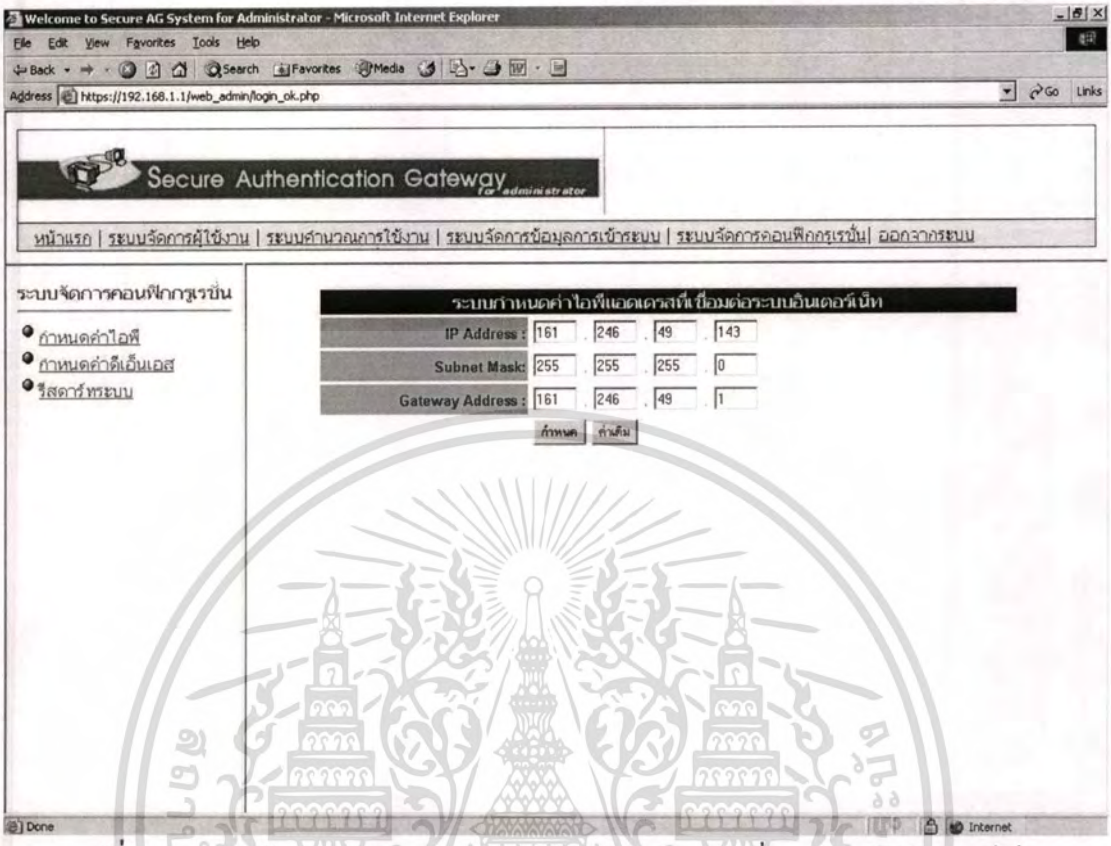
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 72 แสดงหน้าจอการทำงานระบบจัดการคอนฟิกกรูเรชั่น

โดยภายในระบบจัดการคอนฟิกกรูเรชั่นนี้จะมีการทำงานย่อย 3 ส่วนคือส่วนของการกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท ส่วนของการกำหนดหมายเลขไอพีดีเอ็นเอสสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท และส่วนของการรีสตาร์ทระบบพิสูจน์ตัวจริง โดยถ้าผู้ดูแลระบบเลือกที่จะทำการกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท จะปรากฏหน้าจอ ตามรูปที่ 73

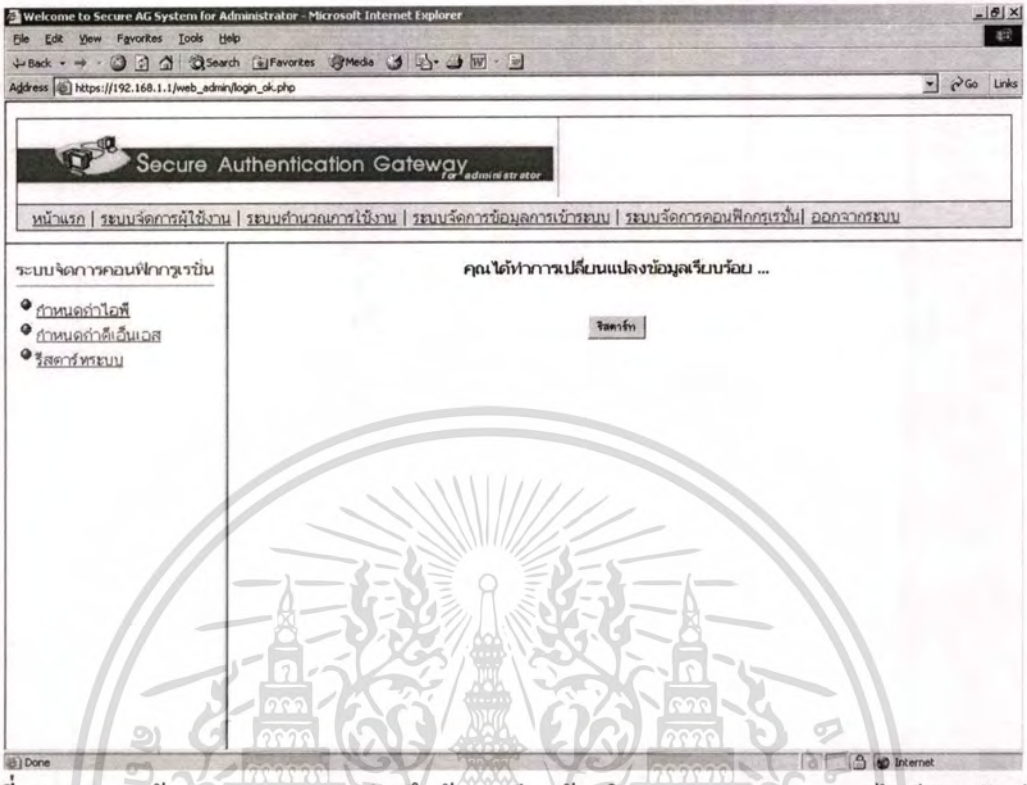
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 73 แสดงหน้าจอการกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท

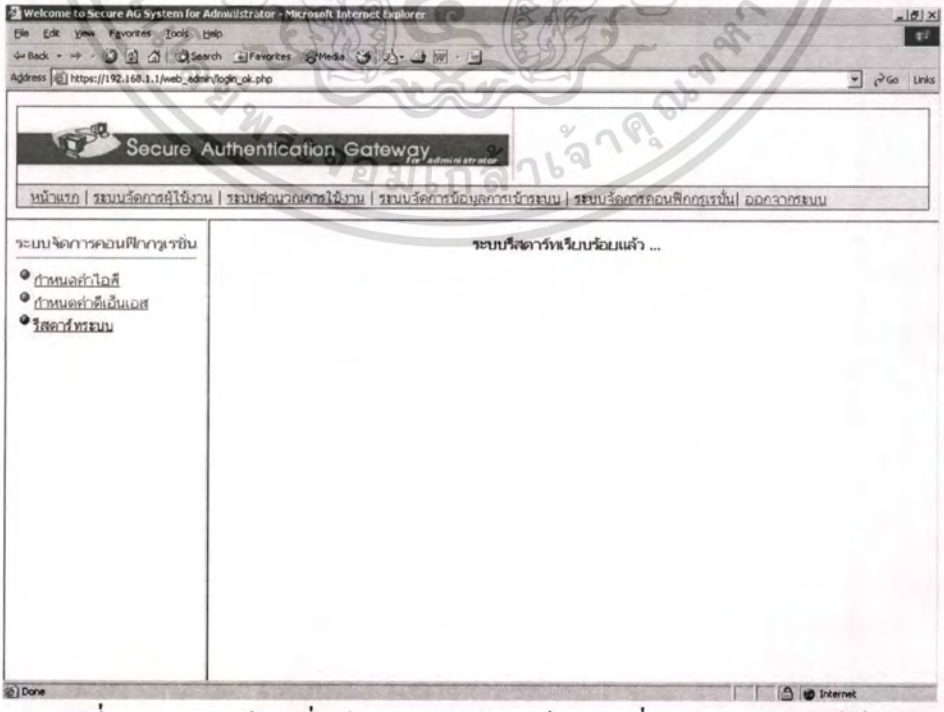
เมื่อผู้ดูแลทำการกรอกข้อมูลเรียบร้อยแล้ว ระบบจะมีการแสดงการบันทึกข้อมูลเรียบร้อย และจะแสดงปุ่มให้ผู้ดูแลระบบทำการรีสตาร์ทส่วนของการเชื่อมต่อระบบอินเตอร์เน็ทเพื่อใช้ข้อมูลหมายเลขไอพีใหม่ที่มีการกำหนดไป ซึ่งจะมีหน้าจอตามรูป 6.74

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 74 แสดงหน้าจอการแสดงการบันทึกข้อมูลเรียบร้อยในการกำหนดหมายเลขไอพีสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท

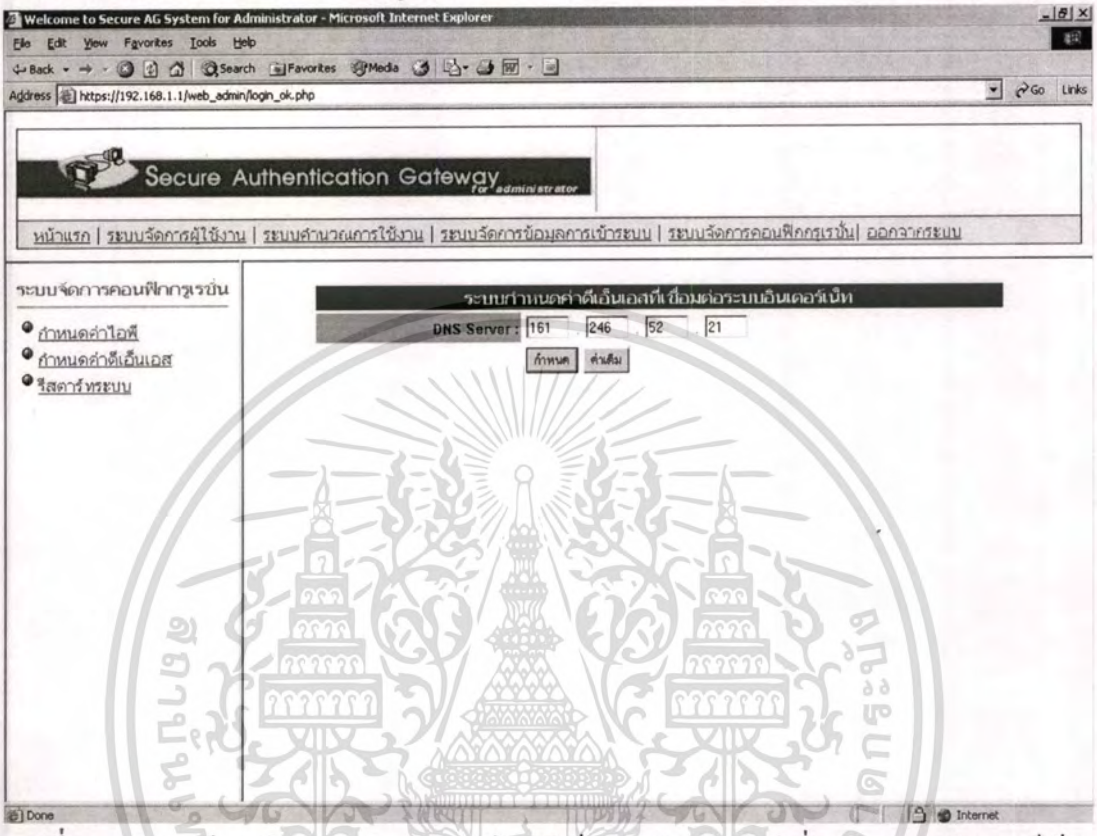
โดยถ้าผู้ดูแลระบบทำการรีสตาร์ทระบบก็จะแสดงข้อความให้ทราบ ตามรูปที่ 6.75



รูปที่ 75 แสดงหน้าจอที่มีข้อความการรีสตาร์ทส่วนเชื่อมระบบอินเตอร์เน็ท

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

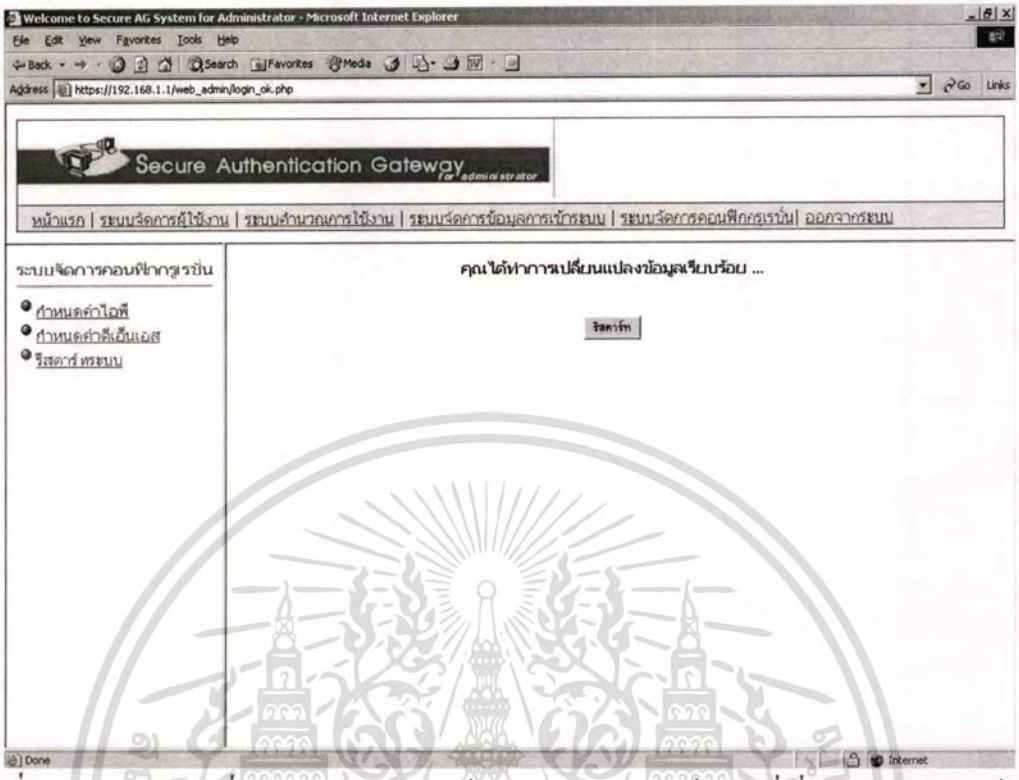
ถ้าผู้ดูแลระบบต้องการที่จะกำหนดหมายเลขไอพีดีเอ็นเอสสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท สามารถเลือกคลิกที่เมนูได้ โดยจะปรากฏหน้าจอตามรูป 76



รูปที่ 76 แสดงหน้าจอการกำหนดหมายเลขไอพีดีเอ็นเอสสำหรับส่วนเชื่อมต่อระบบอินเตอร์เน็ท

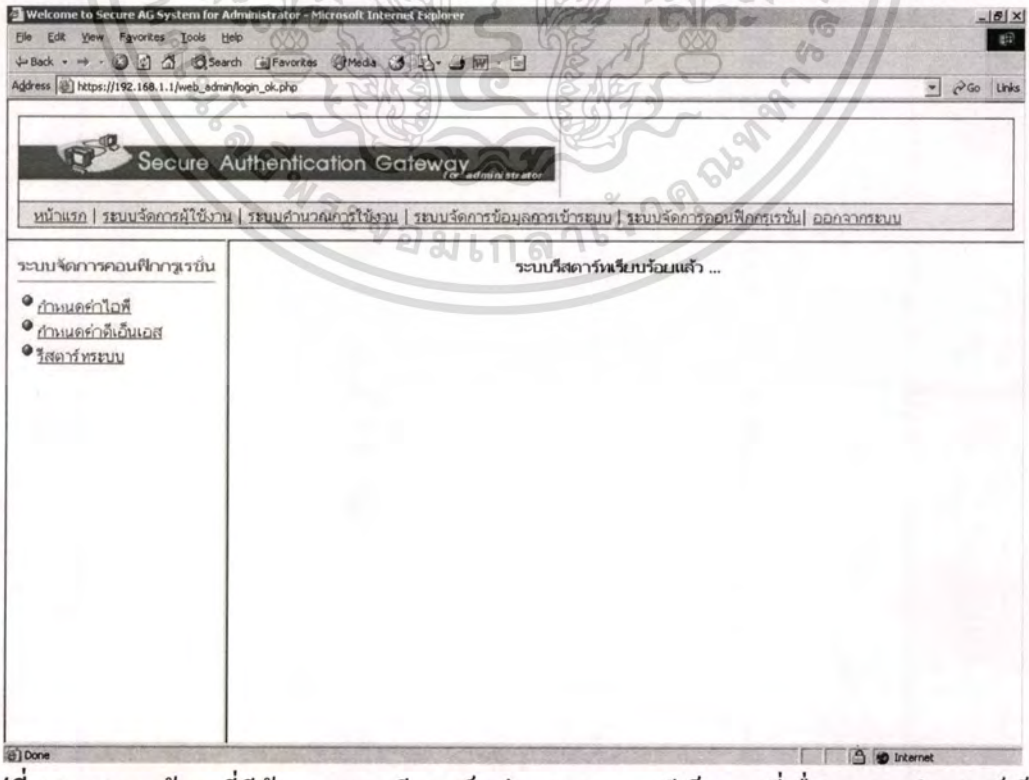
เมื่อผู้ดูแลระบบทำการกรอกข้อมูลเรียบร้อยแล้ว ระบบจะมีแสดงให้ผู้ดูแลทราบ พร้อมทั้งให้ผู้ดูแลทำการรีสตาร์ทระบบในส่วนของดีเอ็นเอสในส่วนเชื่อมต่อระบบอินเตอร์เน็ท ซึ่งจะมีหน้าจอดังรูป 77

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 77 แสดงหน้าจอที่มีข้อความการรีสตาร์ทส่วนของระบบดีเอ็นเอสที่เชื่อมระบบอินเตอร์เน็ท

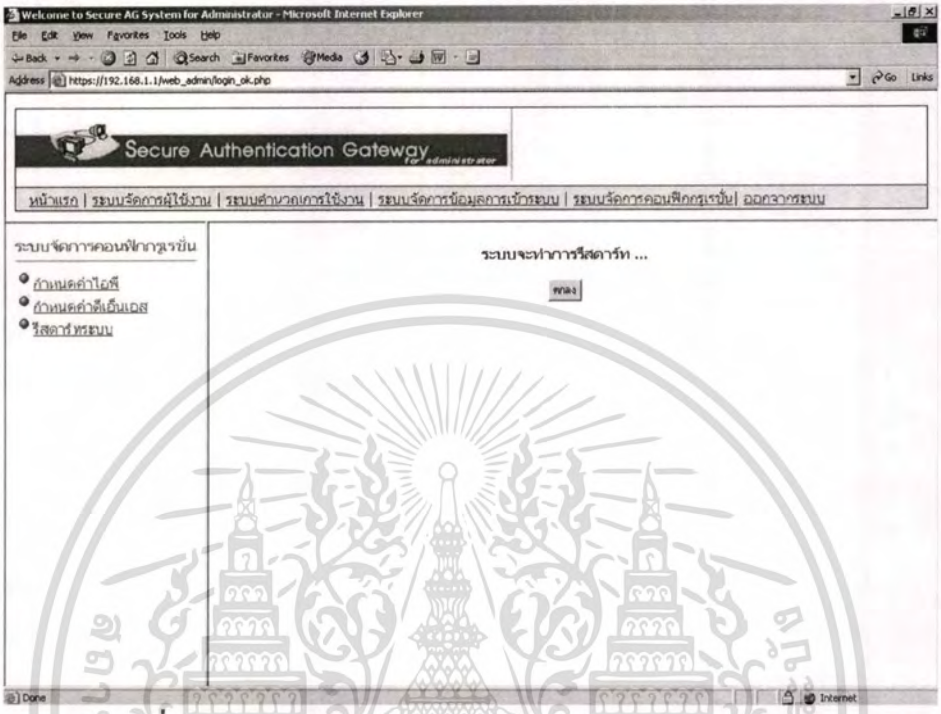
โดยถ้าผู้ดูแลระบบทำการรีสตาร์ทระบบก็จะแสดงข้อความให้ทราบ ตามรูปที่ 6.78



รูปที่ 78 แสดงหน้าจอที่มีข้อความการรีสตาร์ทส่วนของระบบดีเอ็นเอสที่เชื่อมระบบอินเตอร์เน็ท

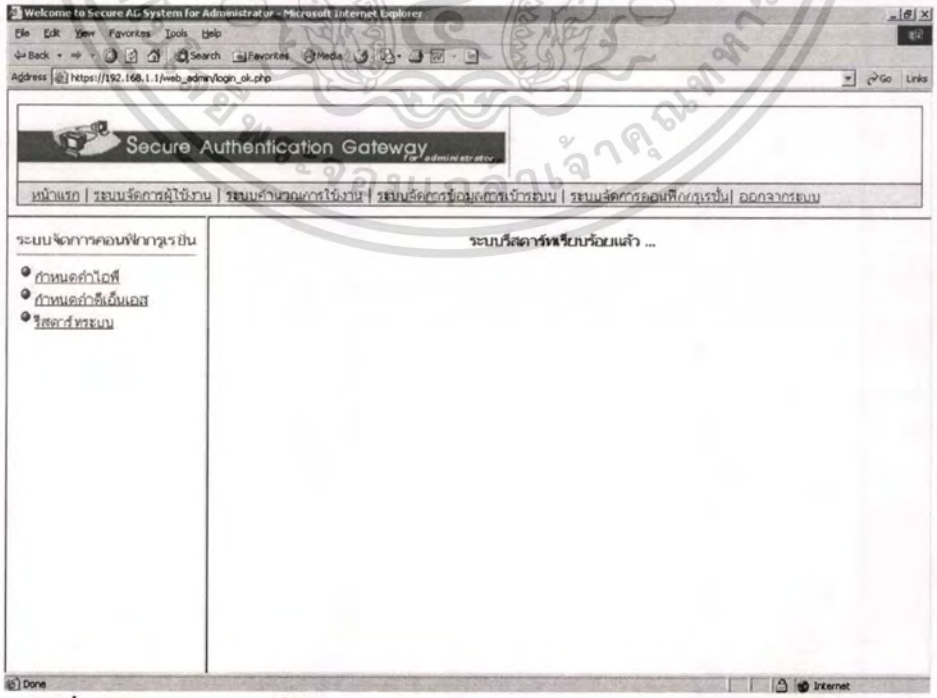
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ จำหน่าย จ่ายแจก หรือนำไปใช้ประโยชน์ในเชิงการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถ้าผู้ดูแลระบบต้องการที่จะรีสตาร์ทระบบพิสูจน์ตัวจริง สามารถที่จะเลือกคลิกที่เมนูได้ โดยจะปรากฏหน้าจอ ดังรูปที่ 79 เพื่อให้ยืนยันการรีสตาร์ทอีกครั้ง



รูปที่ 79 แสดงหน้าจอการยืนยันการรีสตาร์ทระบบพิสูจน์ตัวจริง

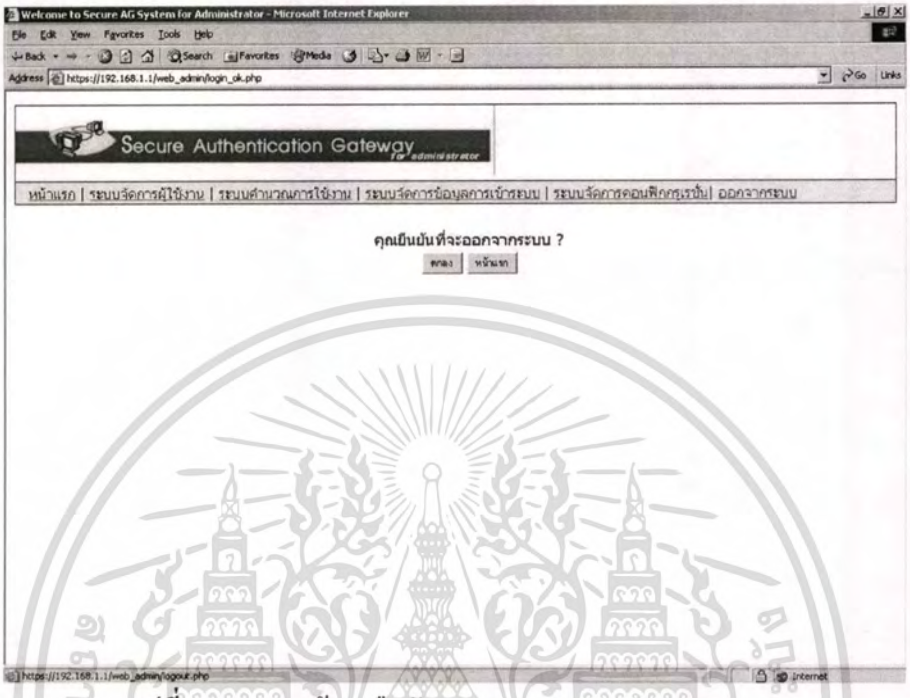
โดยเมื่อมีการรีสตาร์ทระบบเรียบร้อยแล้วระบบจะมีการแสดงข้อความ ตามหน้าจอที่ 80



รูปที่ 80 แสดงหน้าจอที่มีข้อความการรีสตาร์ทระบบพิสูจน์ตัวจริงเรียบร้อยแล้ว

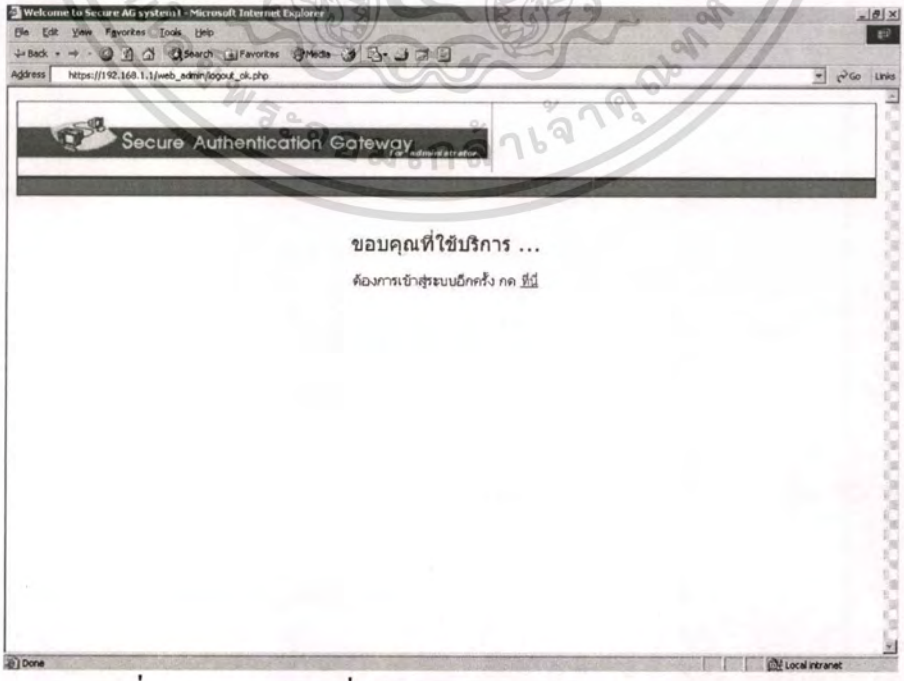
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ถ้าผู้ดูแลระบบต้องการที่จะออกจากระบบ สามารถทำการคลิกที่เมนูได้ โดยจะปรากฏหน้าจอยืนยันการออกจากระบบ ตามรูปที่ 81



รูปที่ 81 แสดงหน้าจอยืนยันการออกจากระบบควบคุมดูแล

หลังจากนั้นระบบจะแสดงข้อความการออกจากระบบของผู้ดูแลระบบ ตามหน้าจอ 82 โดยเป็นการสิ้นสุดการทำงานของระบบ



รูปที่ 82 แสดงหน้าจอที่มีข้อความการออกจากระบบควบคุมดูแล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียนโครงงาน

ชื่อผู้จัดทำโครงงาน	นายยงยุทธ ชูชัยเจริญ
วันเดือนปีเกิด	4 ตุลาคม 2521
สถานที่เกิด	กทม.
ประวัติการศึกษา	
ประถมศึกษา	โรงเรียนแม่พระฟาติมา กทม.
มัธยมศึกษาตอนต้น	โรงเรียนวัดบวรนิเวศ กทม.
ประกาศนียบัตรวิชาชีพ	วิทยาเขตพณิชยการพระนคร กทม.
ประกาศนียบัตรวิชาชีพชั้นสูง	วิทยาเขตพณิชยการพระนคร กทม.
ปริญญาตรี	ม.มหิดล กทม.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้