

ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

การพัฒนาโปรแกรมบริหารผู้ใช้งานผ่าน Web โดยใช้ LDAP

Software Development of Web-based User Management System using LDAP

โดย

นายคทาวัช ตริเทพชาญชัย

รหัส 44067097



H001992

อาจารย์ที่ปรึกษา

อาจารย์อักรินทร์ คุณกิตติ

วัน เดือน ปี..... 24 พ.ค. 2550

เลขทะเบียน..... 01992

เลขเรียกหนังสือ..... วรท. ศ 138 ก 2545

"ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล."

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 2 ปีการศึกษา 2545
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การพัฒนาโปรแกรมบริหารผู้ใช้งานผ่าน Web โดยใช้ LDAP
นักศึกษา	นายคทาวุธ ตริเทพาญชัย
อาจารย์ที่ปรึกษา	อาจารย์อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตร์มหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

ปัจจุบันระบบคอมพิวเตอร์ได้ถูกนำไปใช้อย่างกว้างขวาง แต่แต่ละระบบมีการเก็บทรัพยากรแยกออกจากกัน ทำให้การกำหนดบริหารจัดการทรัพยากร และสิทธิการใช้งานทรัพยากรมีความยุ่งยากและซับซ้อน โครงการพัฒนาโปรแกรมบริหารผู้ใช้งานผ่าน Web โดยใช้ LDAP เป็นการพัฒนาระบบเพื่อบริหารผู้ใช้งาน โดยระบบได้ถูกออกแบบส่วนติดต่อผู้ใช้งานผ่าน Web-Based เพื่อให้ง่ายต่อการใช้งานรวมทั้งระบบสามารถที่จะทำการแก้ไขหรือเพิ่มเติม ข้อมูลผู้ใช้งานระบบจากฐานข้อมูลผู้ใช้งานที่ถูกบันทึกไว้ที่ LDAP Server และระบบสามารถยังมีความสามารถในการตรวจสอบความผิดพลาดของการป้อนข้อมูล รวมทั้งตรวจสอบการซ้ำซ้อนของข้อมูลได้นอกจากนี้ระบบจะมีการเก็บข้อมูลผลการดำเนินการต่าง ๆ ไว้เพื่อให้สามารถตรวจสอบได้ผ่าน Log File

การพัฒนาระบบใช้ภาษา PHP เนื่องจากสามารถเขียนโปรแกรมประยุกต์เชื่อมต่อกับทั้ง Web Server และ LDAP Server ได้เป็นอย่างดี มีการติดต่อทำ Authentication ระหว่างระบบปฏิบัติการกับ LDAP ผ่านโมดูล PAM_LDAP ทำให้สามารถนำเข้าใช้งานระบบ Unix บัญชีผู้ใช้งานไปใช้งานที่เก็บอยู่บนระบบ LDAP ได้

Title	Software Development of Web-based User Management System using LDAP
Student	Mr. Katawut Tritepchanchai
Advisor	Mr. Akharin Khunkitti
Lever of Study	Master of Science in information Technology
Major	Information Science
Academic Year	2002

ABSTRACT

Today the computer system is used in the all kind of business popularly. Each system has own resource separately. It makes more complex and difficult to manage organization's resource. Software development of Web-base User Management System using LDAP Project is used for manage using resource. Software is designed to interface user with Web-based to make comfortable for use. Software can add, edit or delete user account that store on LDAP Server and have function to alert user when some error occoure include user information duplication. This system have log file to keep all action that occoure for audit later.

Software development using PHP language, It's can interface between with web service and Ldap service easily. This Software can interface with OS pass PAM_LDAP module that mean Unix User account can store and manage pass LDAP.

กิตติกรรมประกาศ

งานโครงการพัฒนาโปรแกรมบริหารผู้ใช้งานผ่าน Web โดยใช้ LDAP ที่ได้จัดทำขึ้นนี้ ข้าพเจ้าได้รับการสนับสนุนจากบุคคลหลายท่าน จึงส่งผลให้โครงการนี้สามารถเสร็จสิ้น ลุล่วงตามเป้าหมายที่วางไว้ ข้าพเจ้าจึงขอขอบคุณบุคคลดังต่อไปนี้

1. บิดาและมารดา ที่ได้ดูแลเอาใจใส่ และเป็นกำลังใจให้ข้าพเจ้าเสมอมา
2. อาจารย์อักรินทร์ คุณกิตติ ที่ให้คำปรึกษา ชี้แนะแนวทางในการพัฒนาระบบงาน ต่าง ๆ ให้เป็นอย่างดี
3. คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง และอาจารย์ทุก ๆ ท่าน ที่ได้มอบความรู้ทางวิชาการต่างๆ เพื่อนำมาใช้ในการพัฒนา

คทาวุธ ตริเทพชาญชัย
ผู้จัดทำ

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	I
บทคัดย่อภาษาอังกฤษ	II
กิตติกรรมประกาศ	III
สารบัญ	IV
สารบัญตาราง	VI
สารบัญภาพ	VII

บทที่

1. บทนำ	
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการพัฒนาระบบงาน	1
1.3 ขอบเขตของการศึกษาและพัฒนาระบบงาน	2
1.4 ขั้นตอนการศึกษาและพัฒนาระบบ	2
1.5 รายละเอียดของเครื่องคอมพิวเตอร์และเครื่องมือที่ใช้ในการพัฒนาระบบ	3
1.6 รายละเอียดของแต่ละบท	4
2. Directory Service	
2.1 ระบบ Directory Service	5
2.2 Lightweight Directory Access Protocol (LDAP)	8
2.3 หลักการทำงานของ Lightweight Directory Access Protocol (LDAP)	9
2.4 โครงสร้างระบบ Account บนระบบปฏิบัติการ Unix	10
3. การวิเคราะห์และการออกแบบ	
3.1 ปัญหาของระบบปัจจุบัน	12
3.2 ความต้องการของระบบ	15
3.3 การออกแบบระบบการทำงาน	15
3.4 ส่วนประกอบของโปรแกรม	19

3.5 กระบวนการทำงานของระบบ.....	19
3.6 โครงสร้าง Schema.....	21
3.7 รูปแบบเพิ่มข้อมูลของโปรแกรม.....	25
3.8 ส่วนติดต่อผู้ใช้งาน (User Interface)	26
4. การพัฒนาระบบงาน	
4.1 ขั้นตอนพัฒนาระบบไคลเอนต์.....	32
4.2 การติดตั้งเครื่องมือที่ใช้ในการพัฒนาโปรแกรม	32
4.3 การพัฒนาโปรแกรม User Management	33
4.4 วิธีการทำงานกับโปรแกรม	34
4.5 ทดสอบการใช้งานโปรแกรม	34
5. สรุปผลการค้นคว้าและพัฒนาระบบ	
5.1 ผลที่ได้จากการพัฒนาระบบ.....	48
5.2 ผลจากการทดสอบโปรแกรม.....	48
5.3 อุปสรรคในการพัฒนาระบบ.....	49
5.4 ข้อเสนอแนะ.....	49
บรรณานุกรม	
ภาคผนวก	
ภาคผนวก ก. ตัวอย่าง Configuration file ของ โปรแกรม Apache	52
ภาคผนวก ข. ตัวอย่าง Configuration file ของ โปรแกรม OpenLDAP.....	54
ภาคผนวก ค. ตัวอย่าง โครงสร้าง File LDIF	55
ภาคผนวก ง. การติดตั้งโปรแกรม.....	56
ภาคผนวก จ. Source Code ของโปรแกรม Import Unix Account to LDIF.....	60
ภาคผนวก ฉ. Source Code ของโปรแกรม Import Unix Group to LDIF.....	63
ภาคผนวก ช. Source ของโปรแกรมที่ใช้ Start/Stop Openldap	65
ประวัติผู้เขียน.....	66

สารบัญตาราง

หน้า

ตารางที่

ตาราง 4.1 แสดงรายชื่อของโปรแกรมที่ในการพัฒนาระบบงาน 33



สารบัญภาพ

หน้า

ภาพที่

2.1	แสดงรูปแบบโครงสร้าง Information model	6
2.2	แสดงลักษณะโครงสร้าง Directory Service	7
2.3	แสดงลักษณะโครงสร้าง Tree และ Entry	7
2.4	แสดงโครงสร้างของ Directory Structure	9
2.5	แสดงรูปแบบโครงสร้างของ File /etc/passwd	10
2.6	แสดงรูปแบบโครงสร้างของ File /etc/group	11
3.1	แสดง Context Diagram ของระบบ User Management (New)	15
3.2	แสดง Data Flow Diagram Level 1 ของระบบ User Management	16
3.3	แสดง Data Flow Diagram Level 2 ของระบบ User Management	17
3.4	แสดง Data Flow Diagram Level 3 ของระบบ User Management	18
3.5	แสดงกระบวนการทำงานของโปรแกรม	20
3.6	แสดงหน้าจอตรวจสอบสิทธิการใช้งาน	26
3.7	แสดงหน้าจอการค้นหายุทธวิธีรายชื่อผู้ใช้งานในระบบ	27
3.8	แสดงผลการค้นหารายชื่อผู้ใช้งานจากระบบ	28
3.9	แสดงหน้าจอที่ใช้ในการตรวจสอบและรับรองผลการทำงานของเจ้าหน้าที่	29
3.10	แสดงหน้าจอการสร้าง Group ใหม่	30
3.11	แสดงหน้าจอการแก้ไขข้อมูลผู้ใช้งานในระบบ	30
3.12	แสดงการกำหนดค่าเบื้องต้นเพื่อใช้เป็นค่าพื้นฐานของระบบ	31
4.1	รูปแสดงหน้าจอของโปรแกรม Edit Plus	34
4.2	แสดงหน้าจอค้นหาข้อมูลผู้ใช้งานของผู้ใช้งานระดับ Staff	35
4.3	แสดงหน้าจอของการแก้ไขข้อมูลผู้ใช้งาน ของผู้ใช้งานระดับ Staff	36
4.4	แสดงให้เห็นถึงการแสดงข้อความเตือนในกรณีที่ไม่ได้มีข้อมูลในช่อง Firstname	37

4.5	แสดงข้อมูลที่ถูกล็อกเก็บลงใน UM_Approve.log	38
4.6	แสดงหน้าจอการค้นหาผู้ใช้งานของผู้ใช้งานระดับ Admin	39
4.7	แสดงหน้าจอผลการค้นหารายชื่อผู้ใช้งานของผู้ใช้งานระดับ Admin	40
4.8	แสดงหน้าจอแจ้งเตือน UID ซ้ำกับผู้ใช้งานในระบบ และ GID ไม่มีอยู่จริงในระบบ	41
4.9	แสดงหน้าจอแจ้งเตือนค่าของ GID ของกลุ่มผู้ใช้งานมีอยู่แล้วในระบบ	42
4.10	แสดงหน้าจอ Approve ของผู้ใช้งานระดับ Admin	43
4.11	แสดงหน้าจอรายละเอียดผู้ใช้งาน ก่อนทำการ Approve	44
4.12	แสดงหน้าจอรายละเอียดผู้ใช้งาน หลังทำการ Approve	45
4.13	แสดงหน้ารายละเอียดผู้ใช้งาน ก่อนทำการแก้ไขข้อมูลของ Home Directory	46
4.14	แสดงหน้ารายละเอียดผู้ใช้งาน หลังทำการแก้ไขข้อมูลของ Home Directory	47



บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ระบบเทคโนโลยีสารสนเทศของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ได้ถูกออกแบบและใช้งานในการให้บริการนักศึกษาและบุคลากรของสถาบันในด้านต่าง ๆ ปัจจุบันสถาบันฯ มีส่วนงานที่มีหน้าที่ในการดูแลและให้บริการระบบสารสนเทศแก่นักศึกษาและบุคลากรในสถาบันฯ แบ่งออกเป็น 3 ฝ่ายงานด้วยกันคือ ฝ่ายควบคุมเครื่อง ฝ่ายระบบเครือข่ายและการสื่อสารข้อมูล และ ฝ่ายระบบและโปรแกรม แต่ละฝ่ายงานมีการเก็บข้อมูลของบัญชีผู้ใช้งานของนักศึกษา และบุคลากรแยกอิสระจากกัน จึงทำให้เกิดความซ้ำซ้อนและขาดประสิทธิภาพในการสื่อสารข้อมูล

ระบบ Directory Service เป็นระบบฐานข้อมูลเนกประสงค์ ที่มีความสามารถในการค้นหาข้อมูล ได้อย่างรวดเร็ว และมีความยืดหยุ่นในการนำไปประยุกต์ใช้งานได้หลาย ซึ่งเราสามารถนำระบบ Directory Service มาประยุกต์ใช้งาน เพื่อลดความซ้ำซ้อนในการเก็บข้อมูลผู้ใช้งานระบบ

1.2 วัตถุประสงค์ของการพัฒนาระบบงาน

- 1.2.1 เพื่อสร้างระบบบริหารบัญชีผู้ใช้งาน และมีการบริหารการใช้งานจากศูนย์กลาง เพื่อเพิ่มประสิทธิภาพในการจัดการ และลดความซ้ำซ้อนของการเก็บข้อมูลผู้ใช้งานไว้ในหลายที่
- 1.2.2 เพื่อให้สามารถให้บริการการบริหารบัญชีผู้ใช้งาน ได้อย่างรวดเร็ว มีประสิทธิภาพ และสามารถตรวจสอบได้
- 1.2.3 เพื่อเพิ่มความน่าเชื่อถือในด้านการทำงานของระบบ และข้อมูลมีความถูกต้อง และปลอดภัย
- 1.2.4 เพื่อให้การพัฒนาโปรแกรมในการให้บริการผู้ใช้งานเป็นไปในแนวทางเดียวกัน และพัฒนาได้อย่างรวดเร็วและมีประสิทธิภาพรวมทั้งสามารถรองรับปริมาณงานที่เพิ่มขึ้นในอนาคต

1.3 ขอบเขตของการศึกษาและพัฒนาระบบงาน

โครงการพัฒนาโปรแกรมบริหารผู้ใช้งานผ่าน Web โดยใช้ LDAP นี้จะทำการศึกษาถึงการทำงานของโปรแกรม Openldap ซึ่งเป็น โปรแกรมที่ใช้เป็น Directory Server โดยที่ไม่เสียค่าลิขสิทธิ์ในการใช้งาน โดยระบบจะทำการเก็บข้อมูลผู้ใช้งาน ลงในฐานข้อมูลของ Openldap และมีการติดต่อกับผู้ใช้งาน ผ่านระบบเครือข่าย Internet โดยมีรูปแบบการติดต่อผ่าน Browser

โปรแกรมที่ถูกพัฒนาขึ้นจะมีความสามารถ ดังต่อไปนี้

- 1.3.1 ระบบงานที่พัฒนาขึ้นสามารถทำการเชื่อมต่อเข้าใช้บริการ Directory Service ในการ เพิ่มบัญชีผู้ใช้งาน หรือ ลบบัญชีผู้ใช้งาน รวมทั้งสามารถค้นหาบัญชีผู้ใช้งานตามที่เราได้
- 1.3.2 ระบบงานมีการติดต่อกับผู้ใช้งานผ่านระบบ Web-Based เพื่อเพิ่มความสะดวกในการใช้งาน
- 1.3.3 มีการเก็บผลการดำเนินการที่ได้มีการดำเนินการ ไปแล้วเพื่อทำการตรวจสอบผลการดำเนินการได้ภายหลัง
- 1.3.4 สามารถกำหนดสิทธิ์การใช้งานให้กับผู้ใช้งาน ได้ เพื่อเพิ่มความปลอดภัยและไม่น่าเชื่อถือให้กับข้อมูล

1.4 ขั้นตอนการศึกษาและพัฒนาระบบ

ขั้นตอนการศึกษาและพัฒนาระบบงาน ได้มีการกำหนดหัวข้อหลัก ๆ เอาไว้ดังต่อไปนี้

- ขั้นตอนที่ 1 ศึกษาการทำงานของระบบ Directory Service ตลอดจน ทฤษฎีต่าง ๆ ที่มีส่วนเกี่ยวข้องเพื่อนำมาใช้ในการออกแบบระบบ
- ขั้นตอนที่ 2 ศึกษาการใช้งานระบบปฏิบัติการ แนวทางในการพัฒนาระบบงาน และเครื่องมือ ที่จะใช้ในการพัฒนาโปรแกรม
- ขั้นตอนที่ 3 วิเคราะห์และออกแบบระบบงาน รวมถึงออกแบบการทำงานของโปรแกรม ภายใต้ขอบเขตการศึกษาและพัฒนาระบบงาน ตามที่ได้กำหนดไว้
- ขั้นตอนที่ 4 ทำการพัฒนาโปรแกรม ทดสอบ การทำงานของโปรแกรม ให้สามารถทำงานได้ตามที่ได้ออกแบบไว้

ขั้นตอนที่ 5 ทำการตรวจสอบข้อผิดพลาดและ ปรับแต่งการทำงานของโปรแกรม
เพื่อให้สามารถนำไปใช้งานได้มีประสิทธิภาพต่อไป

1.5 รายละเอียดของเครื่องคอมพิวเตอร์และเครื่องมือที่ใช้ในการพัฒนาระบบ

เนื่องจากโปรแกรมที่ทำการพัฒนามีหลักการทำงานอยู่บนพื้นฐานของ Client/Server ดังนั้นเพื่อให้มีสภาวะการทำงานที่เสมือนมีการใช้งานจริงมากที่สุด จึงได้มีการติดตั้ง Unix Server ขึ้น โดยได้นำเอา Solaris X86 มาติดตั้งบนเครื่องคอมพิวเตอร์ ทำหน้าที่เป็นเครื่องผู้ให้บริการ Web และ ในขณะเดียวกันก็ทำหน้าที่เป็น LDAP Server ด้วย ส่วนทางด้าน Client นั้นได้มีการจัดหาเครื่องคอมพิวเตอร์ อีก 1 เครื่องที่มีทำงานบนระบบปฏิบัติการ Microsoft Window ใช้ในการพัฒนาโปรแกรมตลอดจนการจัดทำเอกสารต่าง ๆ แต่เนื่องจาก ระบบปฏิบัติการ Solaris X86 ต้องการ Hardware ที่เหมาะสมและสามารถใช้งานร่วมกันได้ ทางผู้พัฒนาโปรแกรมจึงต้องทำการจัดเตรียมเครื่องที่มีความเหมาะสมในการใช้งานดังมีรายละเอียดดังต่อไปนี้

1.5.1 เครื่อง Web Server & LDAP Server

CPU	Pentium III 677 MHz
Memory	256 MB
Hard-Disk	10 GB
Network-Card	3 Com 3c590
Graphic-Card	nVidia TNT 2
OS	Solaris X86
Application	Openldap 2.1.12
	Apache 1.3.1
	PHP 4.3.1

1.5.2 เครื่องที่ทำหน้าที่เป็น Client

CPU	AMD 500 MHz
Memory	256 MB
Hard-Disk	10 GB
Network-Card	Novell NE2000
Graphic-Card	Sis 6326

OS Windows 98

1.5.3 ระบบเครือข่าย

Linksys 10/100 Hup 5 Ports

1.5.4 เครื่องมือที่ใช้ในการพัฒนา

GNU Gcc 3.2.1

SED 4.0

1.6 รายละเอียดของแต่ละบท

สำหรับเนื้อหาของเอกสารประกอบการพัฒนาโปรแกรมฉบับนี้ ได้มีการแบ่งเนื้อหาออกเป็นบทต่าง ๆ ดังต่อไปนี้

บทที่ 2 จะกล่าวถึง Directory Service และทฤษฎีที่เกี่ยวข้อง คำนิยามและความหมายต่าง ๆ ที่ควรทราบ รวมถึงวิธีการทำงานอย่างคร่าว ๆ ของ LDAP โครงสร้างการเก็บข้อมูล รวมถึงบริการที่ LDAP มีให้

บทที่ 3 จะเป็นการวิเคราะห์และออกแบบระบบ ซึ่งจะกล่าวถึงปัญหาของระบบปัจจุบัน รวมถึงการออกแบบโครงสร้างการทำงาน และรูปแบบการติดต่อกับผู้ใช้งาน

บทที่ 4 จะเป็นขั้นตอนการพัฒนาโปรแกรม ตามที่ได้ทำการออกแบบไว้ในบทที่ 3 รวมถึงการตรวจสอบความถูกต้องของโปรแกรมที่พัฒนาขึ้น

บทที่ 5 เป็นการสรุปผลการพัฒนา ประโยชน์ที่ได้รับจากการพัฒนาโปรแกรม ตลอดจนอุปสรรคต่าง ๆ และข้อเสนอแนะเพื่อเป็นประโยชน์แก่ผู้ที่นำไปใช้งาน หรือ พัฒนาโปรแกรมต่อไป

บทที่ 2

Directory Service

2.1 ระบบ Directory Service

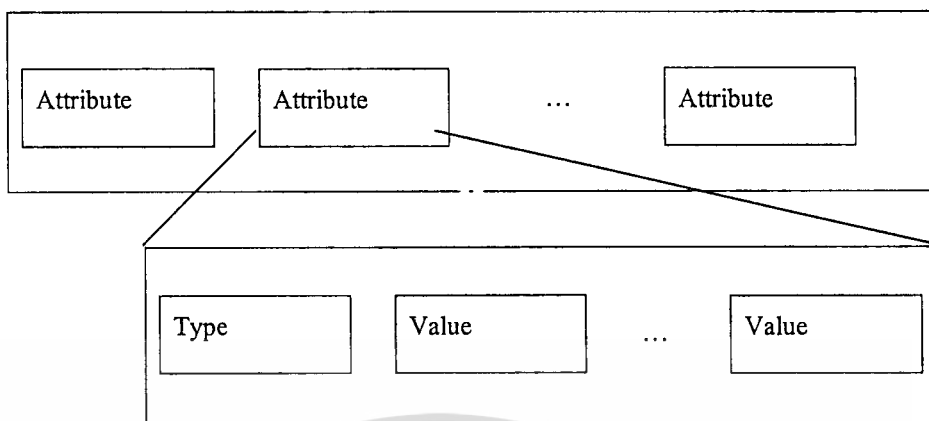
ระบบ Directory Service นั้นมีโครงสร้างเป็นฐานข้อมูลเนกประสงค์ที่มีการเก็บข้อมูลเป็นลำดับชั้น ข้อมูลที่ทำการจัดเก็บ นิยมที่ใช้เก็บฐานข้อมูลของผู้ใช้งานและ ข้อมูลของระบบเครือข่าย เป็นหลัก เนื่องมาจากระบบ Directory Service ไม่ขึ้นกับระบบปฏิบัติการ และข้อมูลต่าง ๆ เช่น ข้อมูลของผู้ใช้งานอาจต้องทำการเก็บไว้ทั้งบน Directory Service และ ในระบบปฏิบัติการนั้น ๆ ได้ โดยเราสามารถกำหนดให้ทำการค้นหาข้อมูลจาก Directory Service เป็นอันดับแรกได้ เมื่อไม่พบข้อมูลจึงทำการค้นหาไปยังฐานข้อมูลที่อยู่บนระบบปฏิบัติการนั้น ๆ

Directory Service จะมีการกำหนดรูปแบบ การเก็บข้อมูลและการให้บริการที่เป็นมาตรฐาน โดยจะอธิบายลักษณะข้อมูลที่สามารถเก็บใน Directory Service ได้และถึงวิธีการในการจัดการข้อมูลที่อยู่ใน Directory Service โดยจะมีการแบ่งออกเป็นชนิดต่าง ๆ ดังนี้

- Information model จะเป็นมาตรฐานในการกำหนด รูปแบบของข้อมูลที่สามารถที่จะจัดเก็บใน Directory Service ได้
- Naming model จะเป็นมาตรฐานในการกำหนดรูปแบบของโครงสร้างของข้อมูลที่ถูกจัดเก็บอยู่ใน Directory Service รวมทั้งวิธีการอ้างอิงข้อมูล
- Functional model เป็นการกำหนด รูปแบบการติดต่อและบริการต่างๆ ที่เราสามารถเรียกใช้งาน เพื่อทำการบริหารข้อมูลใน Directory Server
- Security model เป็นการกำหนด รูปแบบในการป้องกันการเข้าถึงข้อมูลจากบุคคลที่ไม่มีสิทธิ์ในการใช้งานข้อมูล

2.1.1 Information model

ข้อมูลที่ถูกเก็บใน Directory Service จะประกอบไปด้วย ส่วนที่เรียกว่า entry โดยแต่ละ entry จะเก็บข้อมูลของสิ่งที่เราสนใจไว้ เช่น entry ของบุคคล อาจมีการเก็บ ชื่อ นามสกุล อายุ เพศ ซึ่งหัวข้อของคุณสมบัติที่เราสนใจนั้น เราเรียกว่า attribute และในแต่ละ attribute จะมีการกำหนด ชนิดของข้อมูลและค่าของข้อมูลที่จะทำการเก็บ

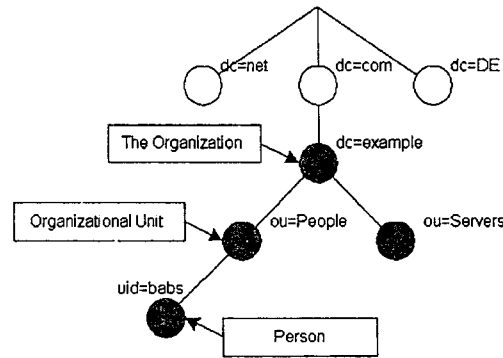


รูป 2.1 แสดงรูปแบบ โครงสร้าง Information model

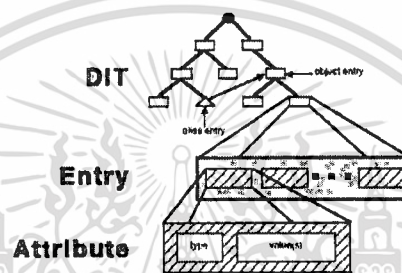
โดยที่ชนิดของ attribute หรือ Type นั้นจะต้องสัมพันธ์กับ รูปแบบชนิดของข้อมูล หรือ Syntax ซึ่ง Syntax จะเป็นตัวกำหนดว่าข้อมูลชนิดใดบ้างที่ Directory Server สามารถเก็บได้ เช่น Attribute ของหมายเลขโทรศัพท์ จะมีชนิดของข้อมูลเป็น caseIgnoreString ซึ่งรูปแบบข้อมูลนี้จะไม่สนใจเครื่องหมาย “-” และช่องว่างในระหว่างการทำกรค้นหามหาหมายเลขโทรศัพท์

2.1.2 Naming Model

โดยปกติแล้ว entry ของข้อมูลจะมีโครงสร้างแบบ Tree ซึ่งจะมีโครงสร้างตามความสัมพันธ์ ของข้อมูลที่เราทำการจัดเก็บลงไป แต่ละ entry จะมีชื่อเรียกโดยชื่อนี้จะอ้างอิงถึงตำแหน่งของข้อมูลตามลำดับชั้น เราเรียกชื่อที่ใช้อ้างอิงนี้ว่า Distinguished name (DN) และสำหรับการอ้างอิงถึงส่วนประกอบต่าง ๆ ใน DN เราจะใช้ Relative distinguished name (RDN) ในการอ้างอิง



รูป 2.2 แสดงรูปแบบโครงสร้าง Directory Service



รูป 2.3 แสดงลักษณะโครงสร้าง Tree และ Entry

จากรูป จะเห็นว่า Directory Service จะเก็บรายละเอียดของข้อมูลต่างๆ ใน DIB (Directory Information Base) โดย DIB จะถูกจัดเก็บในรูปแบบของ Tree เรียกว่า DIT (Directory Information Tree) โครงสร้าง DIB ประกอบไปด้วย ส่วนที่เรียกว่า Entry ซึ่งแต่ละ Entry จะทำหน้าที่เก็บข้อมูลของ Object ได้ Object หนึ่ง โดยในแต่ละ Entry จะประกอบไปด้วยส่วนที่เรียกว่า Attributes ซึ่งแต่ละ Attribute อาจมีข้อมูลเก็บอยู่เพียงหนึ่งค่า หรืออาจจะมีการเก็บค่าหลายค่าไว้ใน Attribute ก็ได้ ชนิดของ Attribute จะขึ้นอยู่กับ Class ของ Object ที่ Entry นั้นๆ ซึ่งได้ถูกกำหนดขึ้นมา

2.1.3 Functional Model

ในส่วนของ Functional Model จะเป็นส่วนที่กำหนดวิธีการจัดการข้อมูลที่อยู่ใน Directory Service โดยจะแบ่งลักษณะการทำงานออกเป็นกลุ่ม ๆ ได้ดังนี้

- กลุ่มการค้นหาและเปรียบเทียบข้อมูล โดยจะมีคำสั่ง Search และ Compare อยู่ในกลุ่มนี้
- กลุ่มคำสั่งการแก้ไขข้อมูล โดยในกลุ่มนี้จะประกอบไปด้วยคำสั่ง Add, Delete, Modify, Modify RDN

- กลุ่มคำสั่งทางด้านการตรวจสอบสิทธิ์ ประกอบด้วยคำสั่ง Bind, Unbind, Abandon โดยที่คำสั่ง Bind และ Unbind ทำหน้าที่ในการตรวจสอบสิทธิ์การเข้าถึงข้อมูลใน Directory Service ส่วนคำสั่ง Abandonใช้ในการ ยกเลิกการทำงานที่กำลังดำเนินการอยู่

2.1.4 Security Model

ในส่วนนี้จะกล่าวถึงจะกล่าวถึงในส่วนของการตรวจสอบสิทธิ์การใช้งานข้อมูลและการเข้ารหัสข้อมูลเพื่อป้องกันการดักจับข้อมูลเมื่อทำการส่งข้อมูลผ่านระบบเครือข่าย โดยใน LDAP จะมีการป้องกันการเข้าถึงข้อมูล 3 แบบคือ

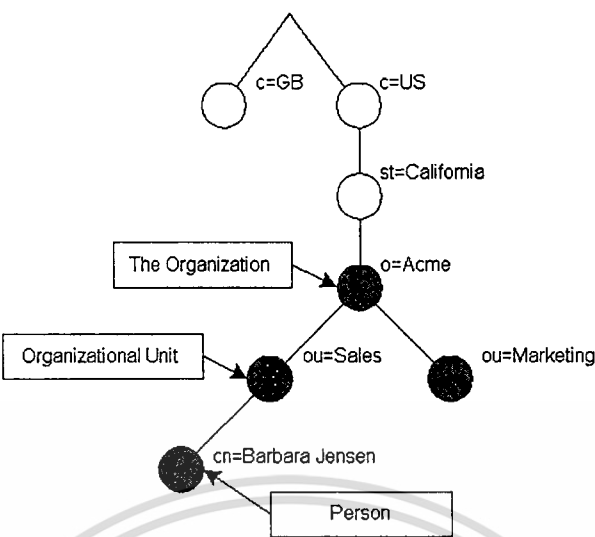
- ไม่มีการป้องกันการเข้าถึงข้อมูล ใช้ในกรณีที่ข้อมูลนั้นเป็นข้อมูลที่เปิดเผยและสามารถเรียกดูได้จากทุกคน เช่น สมุดโทรศัพท์ แต่จะมีการป้องกันการเข้าถึงข้อมูลบางอย่างได้
- การตรวจสอบสิทธิ์การเข้าถึงข้อมูลแบบปกติ
- การตรวจสอบสิทธิ์การเข้าถึงข้อมูลและการเข้ารหัสข้อมูล (Simple Authentication and Security Layer)

2.2 Light Weight Directory Access Protocol (LDAP)

Lightweight Directory Service Protocol เป็นโปรโตคอลที่ทำหน้าที่ในการเข้าถึงข้อมูลใน Directory Server ในส่วนของ LDAP เองมีการทำงานอยู่บนพื้นฐานของ โปรโตคอล TCP/IP อีกทีหนึ่ง ในส่วนของข้อกำหนดต่าง ๆ ของ LDAP จะสามารถหาได้จาก RFC2251 “The Lightweight Directory Access Protocol (V3)”

ในการเก็บข้อมูลลงไปยังระบบ Directory Service นั้น ในส่วนโครงสร้างของ LDAP จะมีวิธีการเก็บข้อมูลตามโครงสร้างของ “Entries” โดยในแต่ละ Entries นั้นจะประกอบไปด้วย Attributes ที่มีค่าไม่ซ้ำกันเลย ที่เรียกว่า Distinguished Name (DN) ดังนั้นเราจึงนำเอา DN มาใช้ในการอ้างอิงถึง Entries ที่อยู่ใน LDAP ในแต่ละ Attribute จะประกอบไปด้วย ชนิดของข้อมูลที่เก็บใน Attribute นั้น ๆ และ ค่าของข้อมูลที่เก็บใน Attribute นั้น ซึ่งอาจจะมีเพียงค่าเดียวหรือ หลายค่าก็ได้ โดยส่วนมากแล้วชนิดของข้อมูลมักเป็นชนิดตัวอักษร ส่วนรูปแบบของค่าที่สามารถเก็บได้นั้นจะขึ้นอยู่กับชนิดของ Attribute

ใน LDAP Entries จะถูกทำการจัดเรียงในรูปแบบโครงสร้างต้นไม้ โดยปกติแล้วรูปแบบโครงสร้างจะเป็นอย่างไรนั้น ขึ้นอยู่กับโครงสร้างของข้อมูลที่เราต้องการ



รูป 2.4 แสดงโครงสร้างของ Directory Structure

เราสามารถทำการอ้างอิงข้อมูลที่เราต้องการได้ โดยใช้สิ่งที่เรียกว่า Distinguished name ซึ่งประกอบมาจากชื่อของแต่ละ Entry นำมาประกอบกัน (ชื่อของ Entry บางครั้งถูกเรียกว่า Relative Distinguished Name หรือ RDN)

2.3 หลักการทำงานของ Light Weight Directory Access Protocol (LDAP)

การทำงานของ LDAP จะทำงานบนพื้นฐานของการทำงานแบบ Client/Server โดยที่ LDAP Server มีการเก็บข้อมูลในสิ่งที่เรียกว่า Directory information tree (DIT) ส่วนที่ทำหน้าที่ Client จะทำการขอใช้บริการโดยส่งคำร้องขอไปยัง Server เมื่อ Server ได้รับคำร้องขอแล้ว Server จะทำการประมวลผลแล้วทำการตอบกลับมายัง Client โดยสิ่งที่ตอบกลับอาจเป็นผลลัพธ์ หรือ อาจเป็น Pointer ที่ชี้ไปยัง LDAP Server ตัวอื่นที่มีข้อมูลที่ Client ต้องการเก็บไว้

2.4 โครงสร้างระบบ Account บนระบบปฏิบัติการ Unix

Unix เป็นระบบปฏิบัติการแบบหลายผู้ใช้หลายงาน (Multiuser/Multitasking) คือระบบสามารถทำงานได้หลายอย่างพร้อมกันในเวลาเดียวกัน ระบบอนุญาตให้ผู้ใช้หลายคนเข้ามาใช้งานระบบ โดยที่ระบบมีวิธีการในการจำแนกผู้ใช้แต่ละคน ซึ่งใช้งานอยู่บนระบบเดียวกันได้ ผู้ใช้หลายคนสามารถใช้งานเครื่องเดียวกันพร้อมกันได้ โดยใช้ลักษณะของการแบ่งเวลา (Time sharing) และแบ่งทรัพยากร (Resource sharing)

บนระบบ Unix จะต้องทำการเก็บข้อมูลของผู้ที่จะทำการตรวจสอบสิทธิ์ไว้ด้วย โดยปกติบนระบบ Unix จะมี File ที่ชื่อ /etc/passwd ซึ่งจะทำการเก็บข้อมูลของผู้ใช้งานทั้งหมดบนระบบไว้ แต่ละบรรทัดของ File จะประกอบด้วยข้อมูลต่าง ๆ ของผู้ใช้งานระบบแต่ละคน

Name	Password	UserID	GroupID	Gecos	Home Directory	Shell
------	----------	--------	---------	-------	----------------	-------

รูป 2.5 แสดงรูปแบบโครงสร้างของ File /etc/passwd

ค่าของข้อมูลแต่ละค่าในแฟ้มข้อมูล /etc/passwd จะถูกคั่นด้วยเครื่องหมาย “:” โดยแต่ละค่ามีความหมายดังนี้

Name	เป็นการระบุถึงชื่อของผู้ใช้งาน โดยชื่อของผู้ใช้งานต้องขึ้นด้วยตัวอักษรและไม่มีค่าซ้ำกันในระบบ
Password	จะประกอบไปด้วยสัญลักษณ์ “*” ซึ่งจะบ่งบอกถึงว่าผู้ใช้งานมีการกำหนดรหัสผ่านไว้แล้ว แต่ส่วน password จะถูกเข้ารหัสแล้วนำไปเก็บไว้ในแฟ้มข้อมูลอื่น
UserID	เป็นค่าตัวเลขประจำตัวของผู้ใช้งานแต่ละคนซึ่งจะต้องไม่ซ้ำกันในระบบ ค่าเลขประจำตัวนี้ใช้ในการกำหนดสิทธิการใช้งาน
GroupID	เป็นค่าตัวเลขแทนค่าของกลุ่มที่ผู้ใช้งานแต่ละคนประจำอยู่
Gecos	เป็นข้อความแสดงรายละเอียดของผู้ใช้งาน ซึ่งระบบไม่ได้นำค่าที่อยู่ใน Field นี้ไปใช้งาน
HomeDirectory	เป็นค่าของตำแหน่งเริ่มต้นของตำแหน่งแฟ้มข้อมูล ที่ผู้ใช้งานจะพบเมื่อเข้าใช้งานระบบ
Shell	เป็นการกำหนด ว่าเมื่อผู้ใช้งานเข้ามาใช้งานระบบ ระบบจะทำการประมวลผลโปรแกรมใด เพื่อรองรับการใช้งานของผู้ใช้งาน

โดยปกติแล้ว File /etc/passwd จะไม่มีการเก็บรหัสผ่านของผู้ใช้งานระบบไว้จะมีเพียงตัวบ่งบอกว่าผู้ใช้งานมีการเก็บบันทึกรหัสผ่านไว้หรือไม่ ส่วนรหัสผ่านจะถูกเก็บไว้ใน File ต่างหากที่ชื่อว่า /etc/shadow โดยจะนำเอารหัสผ่านของผู้ใช้งานมาทำการเข้ารหัสแบบ Data Encryption Standard (DES) และจึงทำการบันทึกไว้ใน File

นอกจากนี้บนระบบ Unix ยังมีการแบ่งกลุ่มผู้ใช้งาน ออกเป็นกลุ่ม ๆ อีกด้วยเพื่ออำนวยความสะดวกในการกำหนดสิทธิ์การเข้าถึง โดยการแบ่งแยกกลุ่มจะถูกระบุอยู่ใน File /etc/group โครงสร้างของ File จะประกอบไปด้วย ข้อมูลของกลุ่มที่มีอยู่ในระบบนั้น ๆ โดยจะมีรูปแบบดังต่อไปนี้

Name	Password	GroupID	User1	User...	Usern
------	----------	---------	-------	---------	-------

รูป 2.6 แสดงรูปแบบโครงสร้างของ File /etc/group

ค่าของข้อมูลแต่ละค่าในแฟ้มข้อมูล /etc/group จะถูกคั่นด้วยเครื่องหมาย “:” โดยแต่ละค่ามีความหมายดังนี้

- Name ชื่อของกลุ่ม โดยในระบบใด ๆ ชื่อของกลุ่มจะไม่ซ้ำกัน
- Password เป็นตำแหน่งเก็บค่าของรหัสที่ใช้ในการตรวจสอบสิทธิ์ของการเข้ามาใช้งานระบบแบบกลุ่ม แต่ปกติไม่ได้นำมาใช้งาน
- Group ID เป็นการระบุหมายเลขประจำกลุ่ม ค่าที่นำมาใช้ในการระบุ ในระบบใด ๆ ต้องไม่ซ้ำกันและค่าที่นำมาใช้จะต้องเป็นค่าจำนวนเต็มเท่านั้น
- User,...,Usern เป็นการระบุถึงบุคคลที่มีสิทธิ์ในกลุ่ม

บทที่ 3

การวิเคราะห์และออกแบบ

บทนี้จะกล่าวถึงการศึกษาความต้องการของระบบ การวิเคราะห์ระบบ โครงสร้างการทำงาน ของระบบโดยรวม รวมทั้งการออกแบบ Schema การกำหนดค่า Configuration การกำหนดเพิ่มของโปรแกรม และการออกแบบส่วนติดต่อผู้ใช้งาน

3.1 ปัญหาของระบบปัจจุบัน

สำนักวิจัยและบริการคอมพิวเตอร์ ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เป็นหน่วยงานมีหน้าที่ดูแลระบบสารสนเทศ และให้บริการระบบคอมพิวเตอร์เพื่อประโยชน์ทางด้านวิชาการ การเรียนการสอน และงานบริหารแต่ละ และหน่วยงานต่างๆ ของมหาวิทยาลัยฯ โดยมีฝ่ายงานที่ความเกี่ยวข้องกับข้อมูลบัญชีผู้ใช้งานมี 3 ฝ่าย คือ ฝ่ายระบบและโปรแกรม ฝ่ายควบคุมเครื่อง ฝ่ายระบบเครือข่าย

3.1.1 ฝ่ายงานและความรับผิดชอบ

1. ฝ่ายควบคุมเครื่อง ทำหน้าที่ จัดการบัญชีผู้ใช้งาน ดูแลเครื่องคอมพิวเตอร์ให้สามารถบริการผู้ใช้งาน สร้างบริการต่างๆ เพื่อตอบสนองความต้องการของผู้ใช้ และดูแล ซ่อมบำรุง เครื่องและบริการต่างๆ ให้ทำงานได้อย่างมีประสิทธิภาพ ซึ่งมีงานบริการหลัก ดังนี้

- งานบริการด้านอินเทอร์เน็ต ใช้เครื่องคอมพิวเตอร์ชื่อ เจ้าคุณ (Chaokhun) เป็นผลิตภัณฑ์ของ SUN SPARC S2000E เพื่อตอบสนองงานบริการและ โปรแกรมประยุกต์ ทางอินเทอร์เน็ต แก่ข้าราชการ นักศึกษาของสถาบัน เช่น Web Browser, ftp, email และอื่นๆ
- งานบริการด้านโปรแกรมประยุกต์ ใช้เครื่องคอมพิวเตอร์ชื่อ แคแสด (Khaesad) เป็นผลิตภัณฑ์ของ SUN SPARC S2000E เพื่อบริการ โปรแกรมประยุกต์งานออกแบบทางวิศวกรรม
- งานบริการด้านฐานข้อมูล ใช้เครื่องคอมพิวเตอร์ชื่อ ร่มเกล้า (Romklo) เป็นผลิตภัณฑ์ของ HP T-520 ใช้ซอฟต์แวร์ ORACLE เพื่อรองรับระบบสารสนเทศของสถาบันฯ ที่มีการใช้ระบบฐานข้อมูล
- งานบริการคอมพิวเตอร์ทำงานแบบขนานความเร็วสูง ใช้เครื่องคอมพิวเตอร์ชื่อ นวมาส (Nawamas) เป็นผลิตภัณฑ์ของ HP-CONVEX Exemplar SPP1600/XA ให้บริการแก่ นัก

ศึกษา ข้าราชการ ทั้งภายในและ ภายนอกสถาบัน ที่ต้องการ ทำงานวิจัย ที่ต้องใช้การ
คำนวณความเร็วสูงมาก

2. ฝ่ายระบบเครือข่าย ทำหน้าที่ควบคุมและจัดการบริการบนเครือข่าย ดูแลการเชื่อมต่อ
ของระบบเครือข่ายทั้งหมดภายในสถาบันฯ ดูแลการเชื่อมต่อระบบอินเทอร์เน็ต และดูแลการให้
บริการใช้งานระบบจากการทำงานระยะไกลผ่านการเชื่อมต่อคอมพิวเตอร์ผ่านโมเด็ม ซึ่งในส่วน
ของการเชื่อมต่อคอมพิวเตอร์ผ่านโมเด็ม จะมี PC Server ให้บริการอยู่ 2 เครื่อง เครื่องแรกทำงาน
บนระบบปฏิบัติการ Microsoft Windows NT Advanced Server Version 3.51 และ Microsoft Back-
Office มีโปรแกรม Shiva Manager เพื่อดูแลการบริการเชื่อมต่อผ่านโมเด็ม ส่วนอีกเครื่องทำงาน
ระบบปฏิบัติการ Sun เพื่อทำหน้าที่เป็น Authentication Server ให้แก่เครื่องเครื่องแรก

3. ฝ่ายระบบและโปรแกรม ทำหน้าที่เขียนโปรแกรมและพัฒนาระบบงานต่างๆ เพื่อใช้ใน
สถาบันฯ เช่น ระบบทะเบียนนักศึกษา ระบบการลงทะเบียนผ่านอินเทอร์เน็ต ระบบบุคลากรของ
สถาบัน ระบบการเงิน กองคลัง เงินรายได้ ระบบหลักสูตร ระบบอาคารสถานที่ พัสดุ ครุภัณฑ์
ระบบยานพาหนะ ระบบทุนการศึกษา เป็นต้น ซึ่งเป็นการทำงานจะเป็นการเขียนระบบโปรแกรม
เพื่อติดต่อกับฐานข้อมูล ORACLE ซึ่งให้บริการอยู่บนเครื่องรวมเกล้า ตัวอย่างระบบงานของฝ่าย
ระบบและโปรแกรม คือ ระบบทะเบียนนักศึกษา ซึ่งสามารถให้บริการ โดยต้องทำการขอรหัส
จากหน้าจอผ่านอินเทอร์เน็ต จากนั้นระบบจะส่งรหัสผ่าน สำหรับผู้ใช้ไปทางอีเมลล์ของผู้ใช้ที่มีอยู่
กับทางสถาบันฯ จึงนำเอา ชื่อผู้ใช้และรหัสผ่านมา ที่หน้าจอเดิมเพื่อให้บริการต่างๆ ต่อไป

3.1.2 ขั้นตอนการปฏิบัติงาน

ระบบที่เกี่ยวข้องกับข้อมูลบัญชีรายชื่อผู้ใช้ มีข้อมูลที่เกี่ยวข้อง คือ ชื่อเข้าใช้และรหัสผ่าน
ของนักศึกษาและบุคลากรทั้งในและนอกสถาบันฯ มีการทำงานเริ่มจากทะเบียนมีการรายชื่อของ
นักศึกษา หรือบุคลากรใหม่ที่เพิ่มเข้ามา จะมีการกำหนดรหัสประจำตัวนักศึกษา หรือบุคลากรขึ้นมา
ให้กับแต่ละคน และทำการสร้างรหัสผ่านโดยการสุ่ม เพื่อใช้งาน หรือเพื่อต้องการดูข้อมูล ซึ่งจะมี
การเก็บในฐานข้อมูล ORACLE บนเครื่องเซิร์ฟเวอร์รวมเกล้า

ระบบควบคุมเครื่องจะต้องการรายชื่อ รหัสประจำตัว และรหัสคณะ เพื่อนำไปสร้างรายชื่อ
ผู้ใช้งานในระบบอีเมลล์และระบบผู้ใช้งานบนเครื่องเซิร์ฟเวอร์ จะทำการร้องขอเจ้าหน้าที่ของฝ่าย
ระบบและโปรแกรมให้ส่ง รายชื่อ รหัสประจำตัว และรหัสคณะมาให้ เมื่อได้รายชื่อ และข้อมูล
ต่างๆ แล้ว เพื่อให้รายชื่อใหม่สามารถใช้งานบนเครื่องเซิร์ฟเวอร์เข้าคุณ ซึ่งทำงานบนระบบปฏิบัติ
การ Unix เพื่อให้สามารถบริการอินเทอร์เน็ต และอีเมลล์ได้ โดยเจ้าหน้าที่จะทำการเปลารายชื่อที่ได้

ให้เป็นไฟล์ข้อความโดยแก้ไข และเพิ่มข้อมูลสำหรับรายละเอียดของผู้ใช้บนระบบปฏิบัติการ Unix ที่จำเป็น และได้เปลี่ยนแปลงข้อมูลบางส่วน โดยเพิ่มตัวอักษรเข้าไปข้างหน้าของรหัสประจำตัว เพื่อใช้เป็น Username ส่วน Password จะทำการสุ่มขึ้นมาใหม่ กลุ่มของผู้ใช้และส่วนอื่นๆ ก็ถูกกำหนดเพิ่มให้ครบ ซึ่งทำงานด้วยโปรแกรมที่เขียนจากภาษาซี โดยไฟล์ข้อความที่เกิดจากโปรแกรมสามารถนำไปต่อกับข้อมูลของผู้ใช้ระบบ Unix เดิมได้ทันที

ในฝ่ายระบบเครือข่าย ระบบที่เกี่ยวข้องกับบัญชีผู้ใช้งาน คือบริการเชื่อมต่อคอมพิวเตอร์ผ่านโมเด็ม ซึ่งจะใช้ชื่อและรหัสผ่านตัวเดียวกับฝ่ายควบคุมเครื่อง ซึ่งในปัจจุบันจะทำโดยใช้วิธีการดักไฟล์ผู้ใช้จากเครื่องเจ้าคุณ ของฝ่ายควบคุมเครื่อง ไปสู่เครื่องของฝ่ายระบบเครือข่ายที่มีระบบปฏิบัติการเดียวกัน เพื่อให้ได้ข้อมูลของ ชื่อและรหัสผ่าน จากนั้นจะใช้โปรแกรม Shiva Manager ซึ่งเป็นโปรแกรมควบคุมการใช้งานของผู้ใช้ที่เชื่อมต่อคอมพิวเตอร์ผ่านโมเด็ม ซึ่งทำงานบนเครื่องระบบปฏิบัติการ Window NT ดึงข้อมูลชื่อและรหัสจาก เครื่องระบบปฏิบัติการ Sun ที่ได้รับข้อมูลบัญชีผู้ใช้ที่คัดลอกมา ทำหน้าที่เป็น Authentication Server อีกที

3.1.3 ปัญหาและข้อจำกัดของระบบงานเดิม

1. ข้อมูลในแต่ละฝ่าย ทั้งฝ่ายควบคุมเครื่อง ฝ่ายระบบเครือข่าย และฝ่ายระบบและโปรแกรมมีการแยกเก็บเป็นของตนเอง ทำให้เมื่อมีการปรับปรุงข้อมูล ข้อมูลไม่มีการเปลี่ยนทันทีในทุกฝ่าย ทำให้ข้อมูลอาจมีความขัดแย้ง ไม่ตรงกัน
2. ข้อมูลของผู้ใช้ ฝ่ายควบคุมเครื่องกับฝ่ายระบบและโปรแกรม มีลักษณะที่แตกต่างกัน และใช้รหัสผ่านของผู้ใช้เป็นคนละตัวกัน ทำให้มีลักษณะเป็นข้อมูลคนละชุด ซึ่งทำให้การใช้งานต้องจำรหัสผ่านหลายชุด ทำให้ผู้ใช้เกิดความไม่สะดวกในการใช้งาน
3. ข้อมูลของผู้ใช้เชื่อมต่อคอมพิวเตอร์ผ่านโมเด็ม ของฝ่ายระบบเครือข่าย ซึ่งใช้วิธีการดักข้อมูลบัญชี ผู้ใช้จากฝ่ายควบคุมเครื่อง มาไว้ที่เครื่องที่ทำหน้าที่ Authentication Server ซึ่งไม่ได้ใช้ประโยชน์อย่างอื่น ทำให้สูญเสียทรัพยากร เนื่องจากไม่ได้ใช้งานเครื่องให้เต็มประสิทธิภาพ
4. การปรับปรุงข้อมูลของบัญชีผู้จากระบบหนึ่งไปสู่อีกระบบ ใช้วิธีการคัดลอก และใช้แรงงานคน ถึงแม้ในปัจจุบัน ไม่มีปัญหาในการใช้งาน แต่ก็ทำให้เกิดความไม่สะดวก และใช้เวลานานกว่าระบบอัตโนมัติ
5. ขาดความยืดหยุ่นในการขยายระบบในอนาคต เนื่องจากเมื่อมีการเพิ่มเครื่องเซิร์ฟเวอร์แล้วต้องใช้แรงงานคนในการคัดลอกข้อมูลบัญชีผู้ใช้ไปให้ระบบใหม่ ซึ่งจะเป็นการไม่สะดวก และอาจทำมีปัญหาในอนาคต

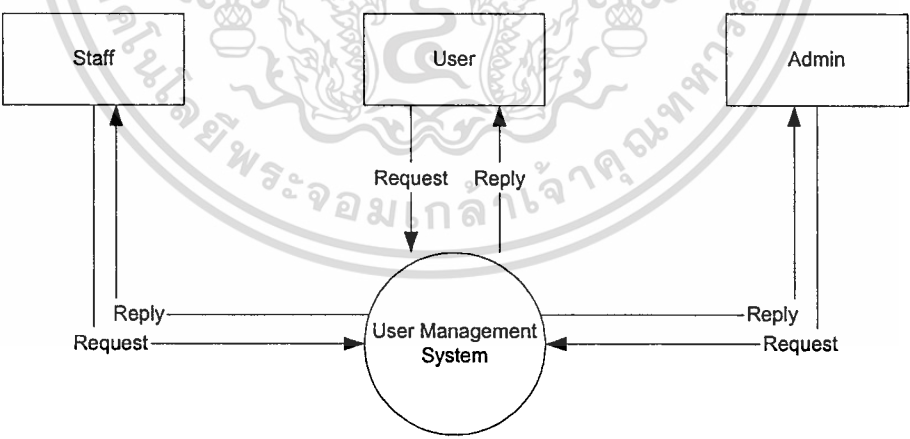
3.2 ความต้องการของระบบ

จากการศึกษาระบบที่ผ่านมา รวมทั้งพิจารณาทฤษฎีที่เกี่ยวข้องในบทที่ผ่านมา จึงสามารถกำหนดความต้องการเพื่อให้ระบบที่พัฒนาขึ้นสามารถแก้ปัญหาต่างๆ ดังต่อไปนี้ได้

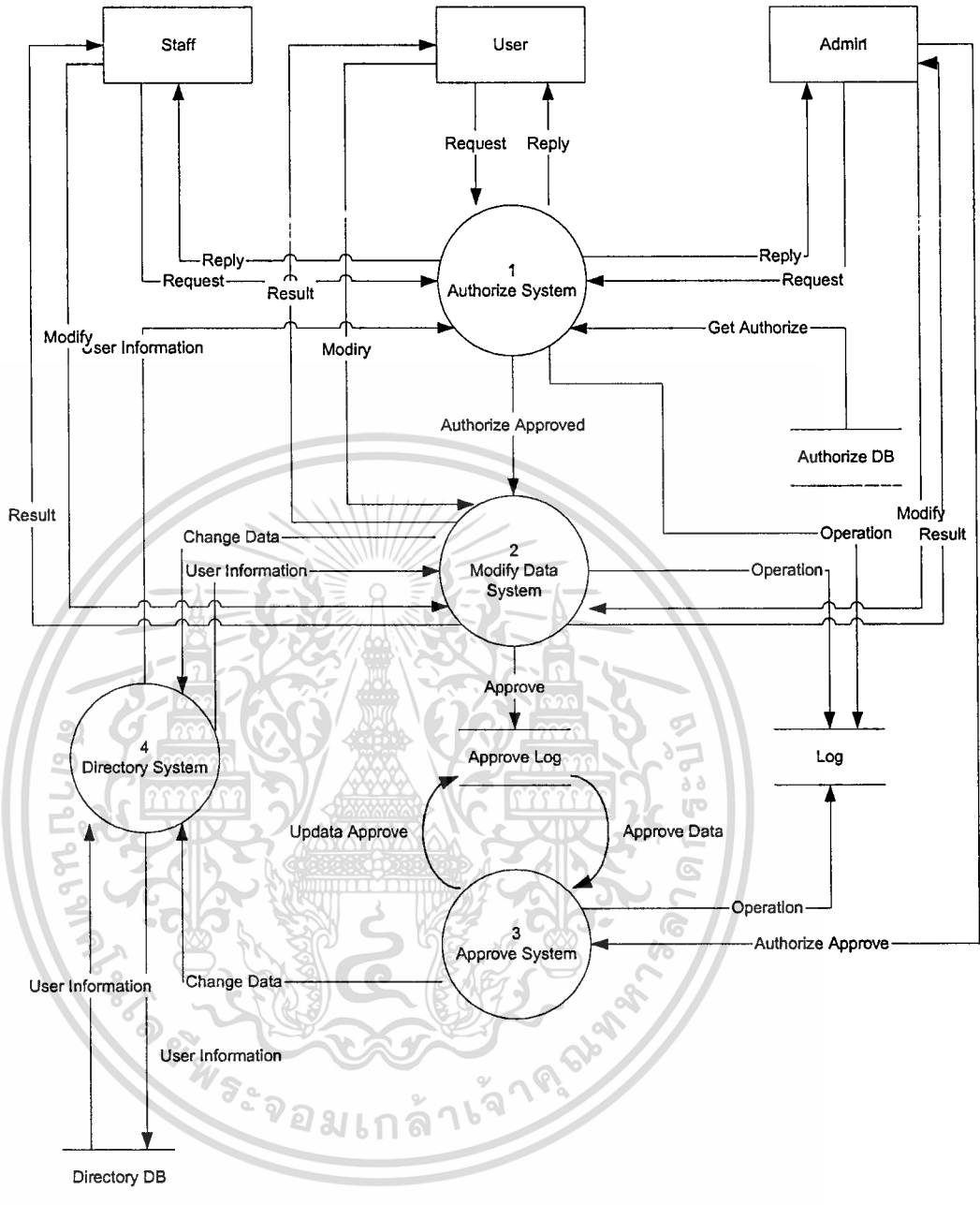
- 1.สามารถลดความซ้ำซ้อน และการใช้งานจากศูนย์กลางในการบริหารบัญชีผู้ใช้งาน
- 2. สามารถสร้างระบบที่น่าเชื่อถือ ทั้งทางด้านการทำงาน และความปลอดภัย เพื่อใช้เก็บข้อมูลบัญชีรายชื่อของผู้ใช้
- 3. สามารถสร้างระบบที่ใช้เก็บข้อมูลบัญชีผู้ใช้งานที่มีมาตรฐานชัดเจน และทำให้สามารถใช้ร่วมกับระบบอื่น ทั้งที่มีอยู่แล้ว และระบบใหม่ ๆ ที่จะนำมาใช้งานในอนาคตได้ โดยผ่านโปรโตคอล LDAP
- 4. เพื่อให้การทำงานของระบบเป็นระบบที่ใช้งานได้ง่าย สามารถให้บริการผู้ใช้งานด้วยข้อมูลมีความทันสมัย รวดเร็ว และสะดวกสบาย ลดเวลาในการเรียนรู้
- 5. สามารถสร้างระบบที่มีความสามารถในการอ่านข้อมูล ค้นหาข้อมูล ดูและเปรียบเทียบข้อมูล ได้อย่างถูกต้อง และรวดเร็ว

3.3 การออกแบบระบบการทำงาน

เมื่อได้ศึกษาถึงความต้องการของระบบแล้ว จึงทำการวิเคราะห์ระบบในเชิงการไหลของข้อมูล ดังแสดงได้ตาม Data Flow Diagram ต่อไปนี้



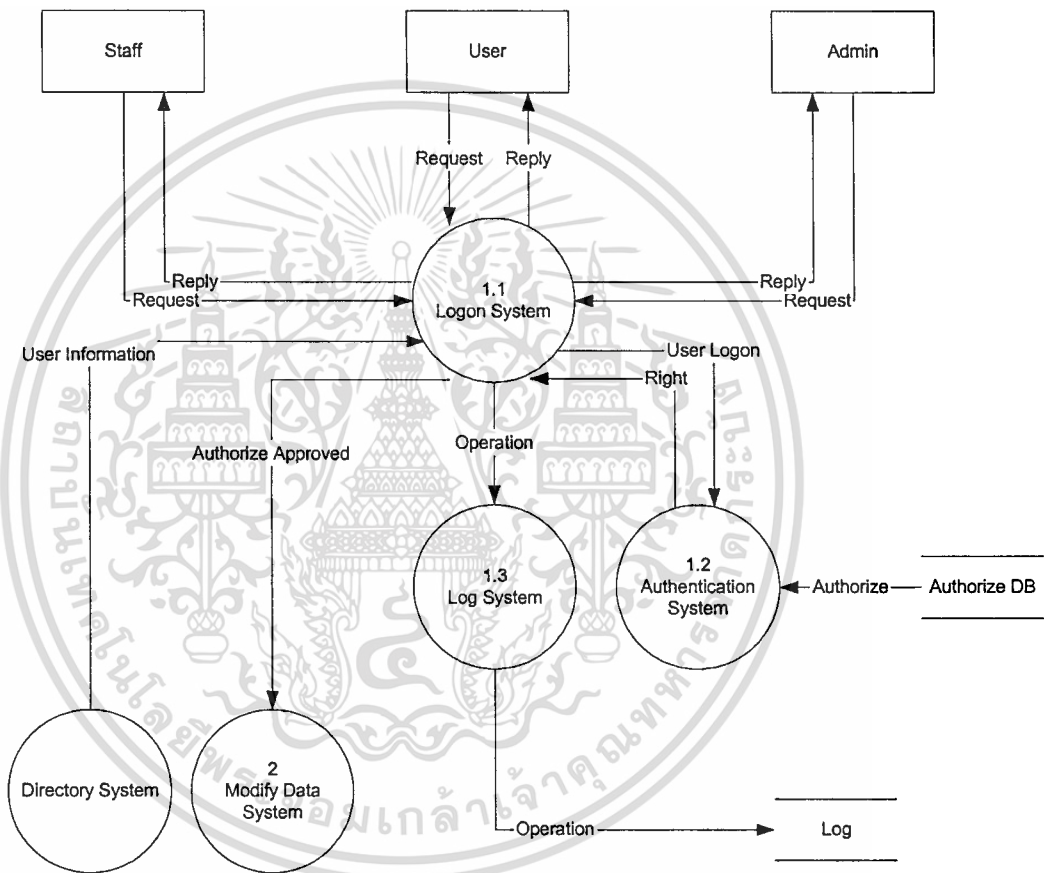
ภาพที่ 3.1 ภาพแสดง Context Diagram ของระบบ User Management (New)



ภาพที่ 3.2 ภาพแสดง Data Flow Diagram Level 1 ของระบบ User Management

ใน Data flow diagram ในภาพ 3.2 เป็นการแสดงการทำงานของ ระบบโดยรวม โดยจะมี ส่วนการทำงานของระบบแบ่งออกเป็นสามส่วน เริ่มที่ระบบ Authorization System ที่ระบบนี้มี หน้าที่ทำการตรวจสอบสิทธิ์การใช้งานระบบ โดยเราสามารถทำการตรวจสอบผู้ใช้งานระบบได้ 2 ระดับ ระดับแรกคือเจ้าหน้าที่ที่มีหน้าที่แก้ไข ข้อมูลของผู้ใช้งานระบบ ในระดับถัดมาคือเป็นเจ้า

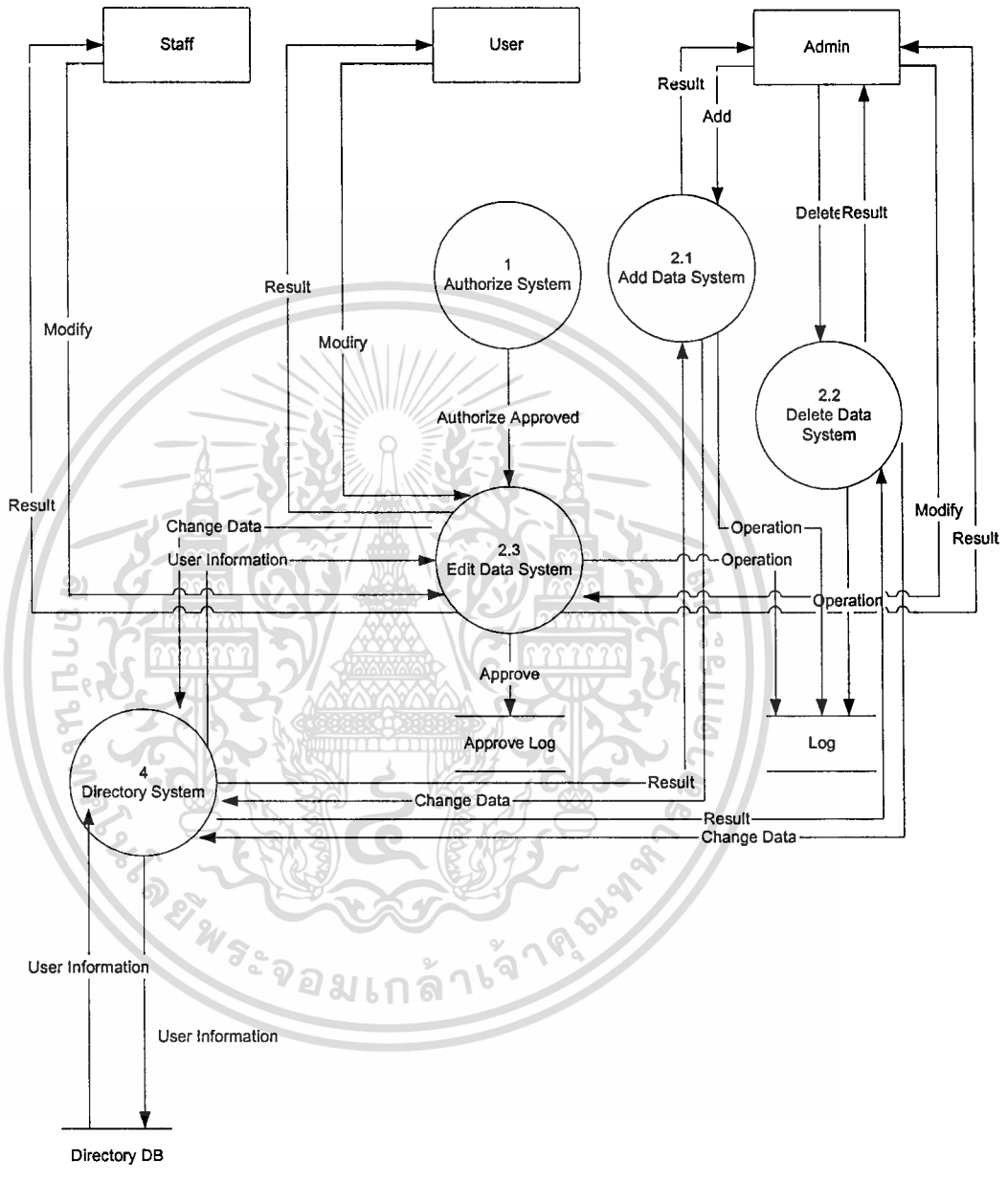
หน้าที่ที่มีหน้าที่ทำการตรวจสอบการแก้ไขข้อมูลของเจ้าหน้าที่ระดับที่ 1 เมื่อเจ้าหน้าที่ได้ทำการตรวจสอบสิทธิ์การใช้งานโดยใส่ รหัสผู้ใช้งานและ รหัสผ่าน เป็นที่เรียบร้อยแล้วระบบจะทำการตรวจสอบถ้าเป็นผู้ที่มีสิทธิ์จริงระบบ จะเข้าสู่หน้าจอหลักต่อไป สำหรับเจ้าหน้าที่ระดับผู้ดูแลระบบ จะสามารถตรวจสอบการทำงานของ เจ้าหน้าที่ระดับที่ 1 ได้โดยผ่านทางระบบ Approve System ส่วนระบบ Modify Data System จะเป็นระบบกลางที่ใช้ในการทำการแก้ไขข้อมูลโดยระบบเองมี สามารถทำการตรวจสอบความถูกต้อง ครบถ้วนของข้อมูล



ภาพที่ 3.3 ภาพแสดง Data Flow Diagram Level 2 ของระบบ User Management

ในภาพ 3.3 แสดงถึงรายละเอียดการทำงานของระบบ Authorize System แบ่งออกเป็นสามส่วนย่อย ๆ โดยแต่ละส่วนมีหน้าที่ดังนี้ ส่วน Logon System ทำหน้าที่ทำการตรวจสอบรหัสผ่าน ส่วนระบบ Authentication System ทำหน้าที่ในการกำหนดสิทธิ์การใช้งานระบบโดยดึงสิทธิ์มาจาก

Authorize DB และระบบย่อยสุดท้ายคือระบบ Log มีหน้าที่ในการเขียนขั้นตอนการทำงาน โปรแกรมเก็บลงใน Log File



ภาพที่ 3.4 ภาพแสดง Data Flow Diagram Level 3 ของระบบ User Management

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในภาพ 3.4 แสดงถึงระบบย่อยของระบบ Modify Data System ซึ่งประกอบไปด้วยระบบ Add Data System ทำหน้าที่ในการเพิ่ม User หรือ Group เข้าไปยังระบบ User Management ระบบ Delete Data System ทำหน้าที่ในการลบ User หรือ Group ออกจากระบบ User Management จาก Diagram จะสังเกตเห็นว่า ผู้ใช้งานระบบที่สามารถใช้งาน ระบบดังกล่าวข้างต้นได้นั้นต้องมีสิทธิ์เป็น Admin เท่านั้น ส่วนระบบ Edit Data System ทำหน้าที่แก้ไขข้อมูลที่เกี่ยวข้องกับระบบ User Management ในระบบนี้ผู้ใช้งานที่มีสิทธิ์นอกเหนือจากสิทธิ์ Admin สามารถที่จะใช้งานได้

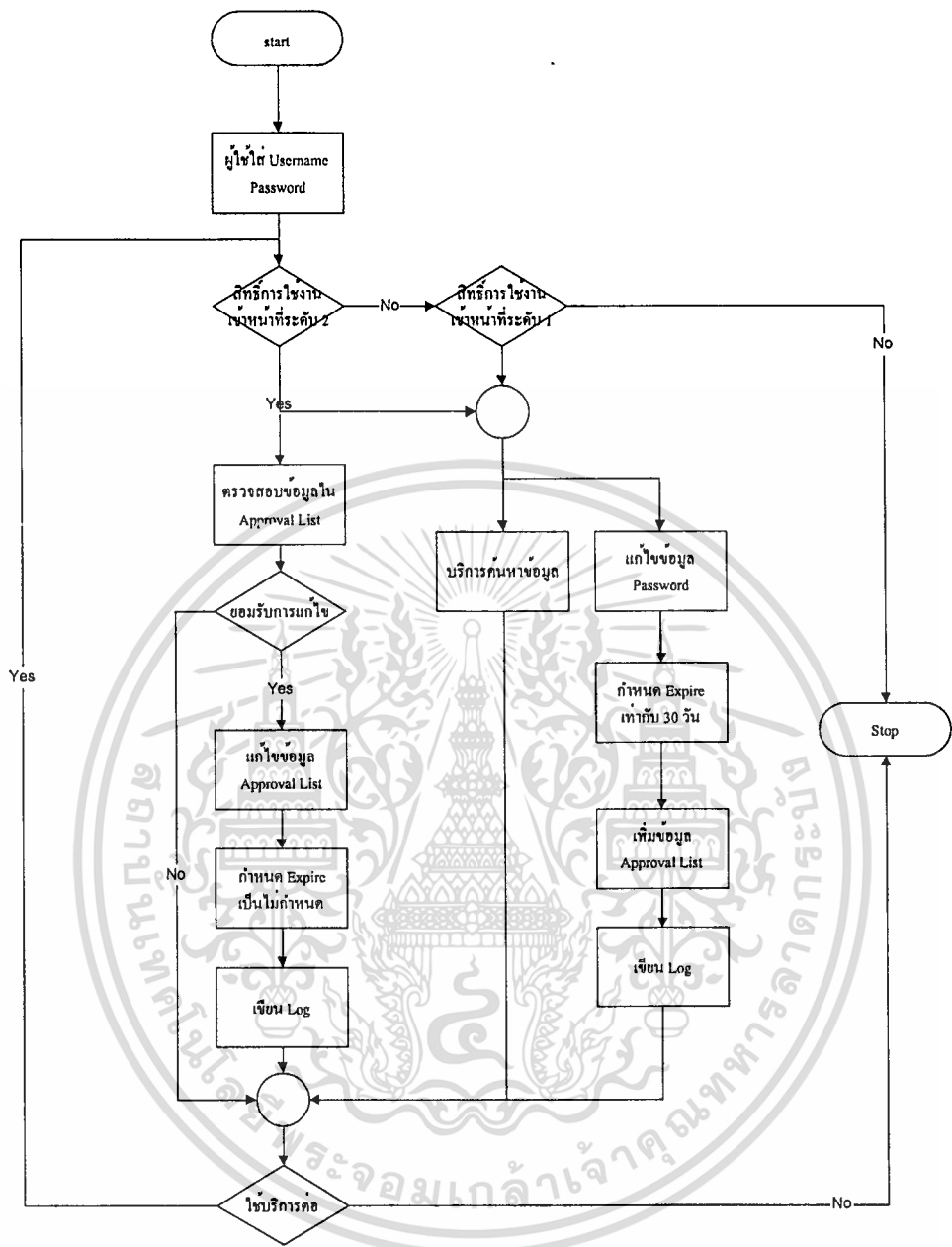
3.4 ส่วนประกอบของโปรแกรม

จากการออกแบบการทำงาน โปรแกรมบริหารข้อมูลผู้ใช้งาน ประกอบด้วย 2 ขั้นตอน โดยขั้นตอนแรกทำหน้าที่รับคำร้องเพื่อเปลี่ยนแปลงข้อมูล และส่วนที่สองทำหน้าที่ยืนยันข้อมูล

- ในส่วนของการแก้ไขข้อมูล ระบบสามารถที่จะแสดงข้อมูลที่ต้องการแก้ไขได้โดย การค้นหา ทำได้จาก การค้นหาตามรหัสนักศึกษา หลังจากนั้นระบบสามารถแสดงข้อมูลที่เกี่ยวข้องกับส่วนของข้อมูลที่จะดำเนินการแก้ไขได้เพื่อป้องกันความผิดพลาดในการแก้ไขข้อมูล เมื่อเสร็จสิ้นขบวนการ ส่วนของการแก้ไขข้อมูลจะทำการ เก็บการดำเนินการและผลของการดำเนินการไว้ รวมทั้งทำการแก้ไขข้อมูลตามที่เจ้าหน้าที่แก้ไข นอกจากนี้ระบบจะทำการส่งข้อมูลการดำเนินการไปยังระบบรับรองการแก้ไขข้อมูลด้วย
- ระบบรับรองการแก้ไขข้อมูล ทำหน้าที่รับรองการแก้ไขข้อมูลโดยเจ้าหน้าที่ที่สามารถเข้ามาใช้งานระบบรับรองการแก้ไขข้อมูลจะเป็นเจ้าหน้าที่ที่มีสิทธิ์พิเศษ ซึ่งจะสามารถใช้งานระบบการแก้ไขข้อมูลได้ด้วย เมื่อเกิดการรับรองการแก้ไขข้อมูล ระบบจะทำการแก้ไขข้อมูลบางส่วนของผู้ใช้งาน และทำการเก็บข้อมูลลง Log File

3.5 กระบวนการทำงานของระบบ

การทำงานในระบบเดิมนั้น เมื่อนักศึกษา ต้องการที่จะทำการเปลี่ยนแปลงข้อมูล เช่น ในกรณีที่นักศึกษามีรหัสผ่าน ของตนเอง นักศึกษาต้องทำการยื่นคำร้องที่ฝ่ายควบคุมเครื่อง เมื่อคำร้องถูกพิจารณาแล้ว ทางฝ่ายควบคุมเครื่องจะทำการแก้ไขข้อมูลของนักศึกษตามที่นักศึกษาร้องขอ จะเห็นได้ว่าระบบเก่า ผู้ที่ทำหน้าที่แก้ไขข้อมูลของนักศึกษาได้นั้นมีเพียง พนักงานที่ทำหน้าที่ดูแลระบบงานที่เกี่ยวข้องกับนักศึกษาโดยตรงเท่านั้น



รูป 3.5 แสดงกระบวนการทำงานของโปรแกรม

การทำงานของระบบเริ่มจากนักศึกษาติดต่อขอใช้บริการแก้ไขข้อมูลกับเจ้าหน้าที่ที่ได้รับมอบหมาย เจ้าหน้าที่ทำการเปิด Web Browser เพื่อทำการติดต่อกับหน้าจอการแก้ไขข้อมูล หลังจากนั้น เจ้าหน้าที่จะทำการ Logon เข้าสู่ระบบ โดยใช้ User และ Password ของตนเอง ทำการค้นหาข้อมูลของนักศึกษาที่ต้องการเปลี่ยนแปลงแก้ไขข้อมูล โดยค้นหาได้จาก รหัสนักศึกษา เมื่อเจ้าหน้าที่ทำการแก้ไขข้อมูลให้นักศึกษาแล้ว ระบบจะทำการเก็บข้อมูลของงานที่ทำได้ไว้ใน Log File เพื่อใช้ใน

การตรวจสอบ ในกรณีที่นักศึกษาได้ทำการขอรหัสผ่านใหม่ เนื่องจากลืมรหัสผ่านเดิม ระบบจะทำการแก้ไขรหัสผ่านให้แต่ รหัสผ่านใหม่นี้จะสามารถใช้ได้เพียง 30 วัน หลังจากที่ได้ทำการ Update ข้อมูลแล้ว ทำการเขียนข้อมูลลงใน Approval List เพื่อส่งผลการตัดสินใจ ให้กับเจ้าหน้าที่ผู้ทำหน้าที่ตรวจสอบ เมื่อเจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบอนุมัติรับรองการทำงาน ระบบจะนำเอาข้อมูลการขอ Approval ออกจาก List ในกรณีที่เป็นการขอรหัสผ่านระบบจะทำการตั้งค่าการใช้งานรหัสผ่านได้ไม่จำกัด หลังจากนั้นระบบจะทำการบันทึกผลการทำงานลง Log File ทุกครั้ง

3.6 โครงสร้างของ Schema

ในการเก็บข้อมูลของผู้ใช้งานระบบเพื่อให้สามารถเก็บข้อมูลของผู้ใช้งานในระบบได้อย่างครบถ้วนและถูกต้อง เราจึงต้องออกแบบลักษณะของข้อมูลและกลุ่มของข้อมูลที่มีความสัมพันธ์ โดยจะแบ่งออกเป็นกลุ่ม ดังนี้

Attribute type

cn

(2.5.4.3 NAME 'cn' SUP name)

description

(2.5.4.13 NAME 'description' EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024})

userPassword

(2.5.4.35 NAME 'userPassword' EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128})

uid

(0.9.2342.19200300.100.1.1
NAME ('uid' 'userid')
DESC 'RFC1274: user identifier'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch

SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256})

uidNumber

(nisSchema.1.0 NAME 'uidNumber'

DESC 'An integer uniquely identifying a user in an
administrative domain'

EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE)

gidNumber

(nisSchema.1.1 NAME 'gidNumber'

DESC 'An integer uniquely identifying a group in an
administrative domain'

EQUALITY integerMatch SYNTAX 'INTEGER' SINGLE-VALUE)

gecos

(nisSchema.1.2 NAME 'gecos'

DESC 'The GECOS field; the common name'

EQUALITY caseIgnoreIA5Match

SUBSTRINGS caseIgnoreIA5SubstringsMatch

SYNTAX 'IA5String' SINGLE-VALUE)

homeDirectory

(nisSchema.1.3 NAME 'homeDirectory'

DESC 'The absolute path to the home directory'

EQUALITY caseExactIA5Match

SYNTAX 'IA5String' SINGLE-VALUE)

loginShell

(nisSchema.1.4 NAME 'loginShell'

DESC 'The path to the login shell'

EQUALITY caseExactIA5Match
 SYNTAX 'IA5String' SINGLE-VALUE)

shadowLastChange

(nisSchema.1.5 NAME 'shadowLastChange'
 EQUALITY integerMatch
 SYNTAX 'INTEGER' SINGLE-VALUE)

shadowMin

(nisSchema.1.6 NAME 'shadowMin'
 EQUALITY integerMatch
 SYNTAX 'INTEGER' SINGLE-VALUE)

shadowMax

(nisSchema.1.7 NAME 'shadowMax'
 EQUALITY integerMatch
 SYNTAX 'INTEGER' SINGLE-VALUE)

shadowWarning

(nisSchema.1.8 NAME 'shadowWarning'
 EQUALITY integerMatch
 SYNTAX 'INTEGER' SINGLE-VALUE)

shadowInactive

(nisSchema.1.9 NAME 'shadowInactive'
 EQUALITY integerMatch
 SYNTAX 'INTEGER' SINGLE-VALUE)

shadowExpire

(nisSchema.1.10 NAME 'shadowExpire'

EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE)

shadowFlag

(nisSchema.1.11 NAME 'shadowFlag'
EQUALITY integerMatch
SYNTAX 'INTEGER' SINGLE-VALUE)

memberUid

(nisSchema.1.12 NAME 'memberUid'
EQUALITY caseExactIA5Match
SUBSTRINGS caseExactIA5SubstringsMatch
SYNTAX 'IA5String')

Entry type

posixAccount เป็น Entry ที่ใช้แสดงถึงรายละเอียดเกี่ยวกับข้อมูลทั่วของผู้ใช้ และข้อมูลเกี่ยวกับข้อมูลที่จำเป็นสำหรับ Account บนระบบปฏิบัติการ Unix

(nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
DESC 'Abstraction of an account with POSIX attributes'
MUST (cn \$ uid \$ uidNumber \$ gidNumber \$ homeDirectory)
MAY (userPassword \$ loginShell \$ gecos \$ description))

shadowAccount เป็น Entry ที่ใช้แสดงถึงรายละเอียดเกี่ยวกับ รหัสผ่านของผู้ใช้ ซึ่งจะประกอบไปด้วยการกำหนดช่วงเวลาที่สามารถเข้ามาใช้งานระบบได้ รวมทั้งรหัสผ่านที่ได้มีการเข้ารหัสไว้

(nisSchema.2.1 NAME 'shadowAccount' SUP top AUXILIARY
DESC 'Additional attributes for shadow passwords'

```
MUST uid
MAY ( userPassword $ shadowLastChange $ shadowMin
    shadowMax $ shadowWarning $ shadowInactive $
    shadowExpire $ shadowFlag $ description ) )
```

posixGroup เป็น Entry เพื่อเป็นใช้ระบุถึงกลุ่มของผู้ใช้งาน ว่าผู้ใช้งานอยู่ในกลุ่มใด

```
( nisSchema.2.2 NAME 'posixGroup' SUP top STRUCTURAL
DESC 'Abstraction of a group of accounts'
MUST ( cn $ gidNumber )
MAY ( userPassword $ memberUid $ description ) )
```

3.7 รูปแบบเพิ่มข้อมูลของโปรแกรม

โปรแกรมนี้ได้รับการออกแบบให้มีการเก็บค่า Config และ Log ต่าง ๆอยู่ในรูปแบบของ File ทั้งหมด เนื่องจากง่ายต่อการเปลี่ยนแปลงแก้ไขโดยผู้ที่มีสิทธิ์เข้าถึง File นั้น ๆ ตามสิทธิ์ที่ได้กำหนดไว้ นอกจากนี้จะต้องมีการแยกแบบ และกำหนด Folder สำหรับเก็บข้อมูลและโปรแกรมที่ใช้ร่วมกันระบบเพื่อให้ง่ายต่อการเปลี่ยนแปลงแก้ไข และง่ายในการ Update ระบบในภายหลัง ซึ่งจะมีรายละเอียดดังต่อไปนี้

- 3.7.1 /opt/ apache_1.3.27 เป็น Directory ที่ใช้ในการเก็บโปรแกรม Apache ซึ่งทำหน้าที่เป็น Web Server
- 3.7.2 /opt/ db_4.1.25 เป็น Directory ที่ใช้ในการเก็บโปรแกรม Berkeley DB ทำหน้าที่ในการเก็บข้อมูลของผู้ใช้งานในระบบทั้งหมด
- 3.7.3 /opt/ openldap_2.1.12 เป็น Directory ที่ใช้ในการเก็บโปรแกรม Openldap ทำหน้าที่ในเป็น LDAP Server บริการบัญชีผู้ใช้งานในระบบทั้งหมด
- 3.7.4 /opt/ php_4.3.1 เป็น Directory ที่ใช้ในการเก็บโปรแกรม PHP ซึ่งทำหน้าที่เชื่อมการติดต่อระหว่าง Web Server กับ LDAP Server
- 3.7.5 /opt/web เป็น Directory ที่ใช้ในการเก็บหน้าจอ Web Page ที่จะส่งการแสดงผลไปยังผู้ใช้งานนอก

3.7.6 /opt/log เป็น Directory ที่ทำหน้าที่เก็บผลการทำงานทั้งหมดของโปรแกรม เพื่อใช้ในการตรวจสอบผลการทำงานได้ภายหลัง

3.8 ส่วนติดต่อผู้ใช้งาน (User Interface)

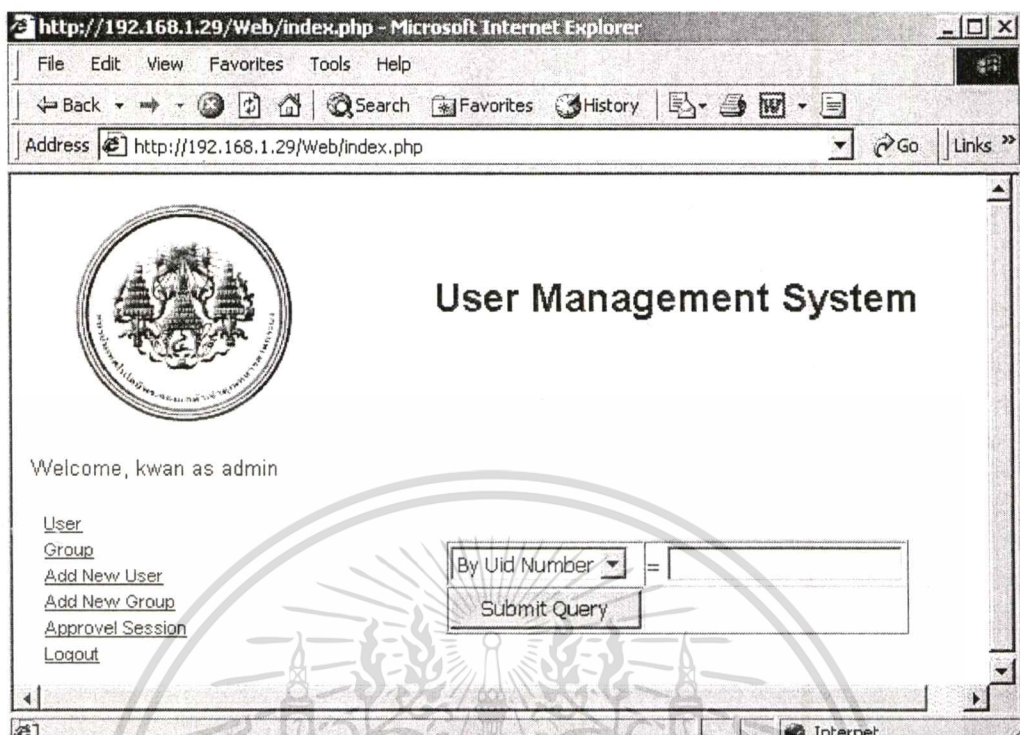
ในส่วนการติดต่อกับผู้ใช้งานนั้น หน้าจอได้ถูกออกแบบให้ง่ายต่อการใช้งาน และได้ทำการซ่อนการแสดงส่วนที่ไม่มีความจำเป็นต่อผู้ใช้งานเพื่อป้องกันความสับสนในการใช้งาน และยังสามารถลดความผิดพลาดในการใช้งานได้ด้วย



รูปที่ 3.6 แสดงหน้าจอตรวจสอบสิทธิ์การใช้งาน

ในการเข้าใช้งานโปรแกรมนั้นผู้ที่จะสามารถเข้าใช้งานได้ต้องเป็นผู้ที่ได้รับการอนุญาตจากผู้ดูแลระบบ Directory Service โดยเมื่อผู้ที่มีสิทธิ์ในการบริหาร Directory Service ได้ทำการอนุญาตผ่านหน้าจอรับรองสิทธิ์แล้ว ระบบจะทำการจดจำรายชื่อของผู้ได้รับอนุญาตไว้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



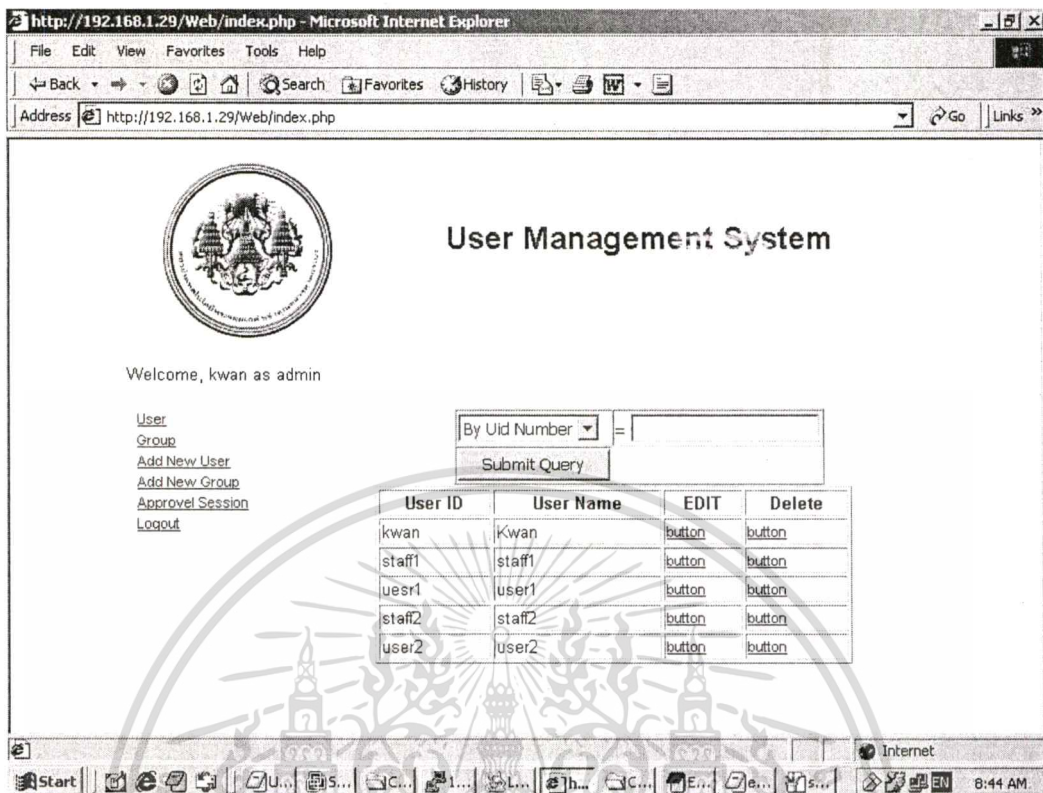
รูป 3.7 แสดงหน้าจอการค้นหามัธยมศึกษาในระบบ

ในการค้นหามัธยมศึกษาในระบบสามารถทำการค้นหาแบ่งออกเป็นหัวข้อต่าง ๆ

ดังนี้

- ทำการค้นหาตามรหัสนักศึกษา
- ทำการค้นหาตามชื่อของผู้ใช้งานระบบ
- ทำการค้นหาตามกลุ่มที่ได้กำหนดไว้ (Group Name)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



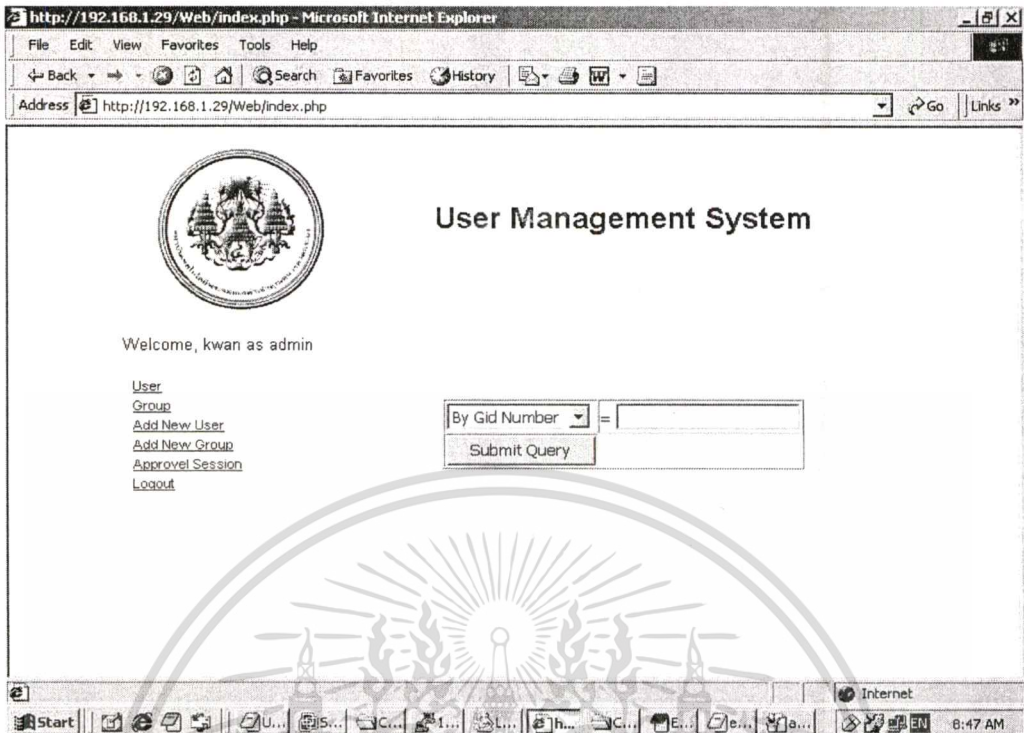
รูปที่ 3.8 แสดงผลการค้นหารายชื่อผู้ใช้งานจากระบบ

ในหน้าจอนี้ผู้ใช้งานสามารถทำการแก้ไขข้อมูลบางอย่างของบัญชีผู้ใช้งานในระบบ Directory ได้เช่น ชื่อของผู้ใช้งาน หรือ ค่าของรหัสผ่านเพียงทำการ Click ไปยังชื่อบุคคลที่ต้องการทำการแก้ไขข้อมูล

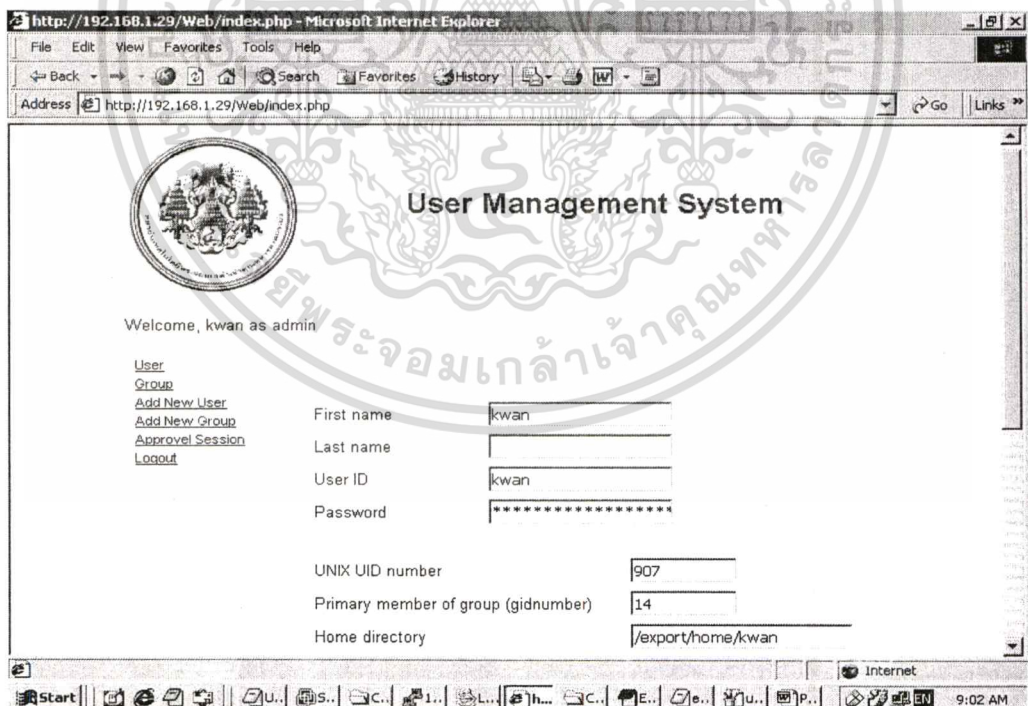


รูป 3.9 แสดงหน้าจอที่ใช้ในการตรวจสอบ และรับรองผลการทำงานของเจ้าหน้าที่

ในรูปที่ 3.9 แสดงให้เห็นถึงหน้าจอการตรวจสอบ และรับรองผลการทำงาน ซึ่งผู้ที่เข้ามาทำการรับรองผลการทำงานได้นั้น ต้องได้รับการอนุญาตจากผู้ควบคุมระบบ Directory Service โดยในหน้าจอผลอนุมัติผลการทำงาน นี้จะแสดงรายชื่อผู้ปฏิบัติงานและ วันเวลาที่ได้ทำการปฏิบัติงาน

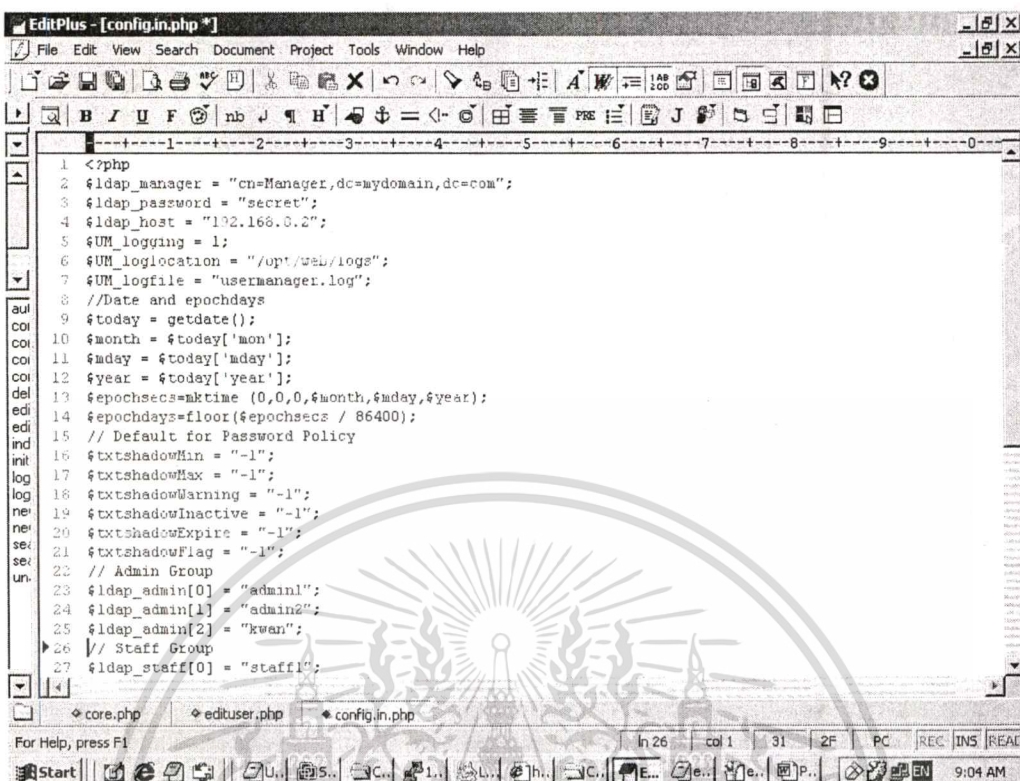


รูป 3.10 แสดงหน้าจอของการสร้าง Group ใหม่



รูปที่ 3.11 แสดงหน้าจอการแก้ไขข้อมูลผู้ใช้งานในระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



```

1 <?php
2 $ldap_manager = "cn=Manager,dc=mydomain,dc=com";
3 $ldap_password = "secret";
4 $ldap_host = "192.168.0.2";
5 $UM_logging = 1;
6 $UM_loglocation = "/opt/um/logs";
7 $UM_logfile = "usermanager.log";
8 //Date and epochdays
9 $today = getdate();
10 $month = $today['mon'];
11 $mday = $today['mday'];
12 $year = $today['year'];
13 $epochsecs=mktime (0,0,0,$month,$mday,$year);
14 $epochdays=floor($epochsecs / 86400);
15 // Default for Password Policy
16 $txtshadowMin = "-1";
17 $txtshadowMax = "-1";
18 $txtshadowWarning = "-1";
19 $txtshadowInactive = "-1";
20 $txtshadowExpire = "-1";
21 $txtshadowFlag = "-1";
22 // Admin Group
23 $ldap_admin[0] = "admin1";
24 $ldap_admin[1] = "admin2";
25 $ldap_admin[2] = "kwan";
26 // Staff Group
27 $ldap_staff[0] = "staff1";

```

รูปที่ 3.12 แสดงการกำหนดค่าเบื้องต้นเพื่อใช้เป็นค่าพื้นฐานของระบบ

จากรูปต่าง ๆ ที่ได้แสดงไปเป็นเพียงบางส่วนของความสามารถที่โปรแกรมสามารถทำงานได้ ซึ่งการออกแบบโปรแกรมเน้นให้ผู้ใช้งานสามารถใช้งานได้ง่าย จึงไม่ได้ทำการออกแบบในส่วนของการจัดการขั้นสูงไว้

บทที่ 4

การพัฒนาระบบงาน

4.1 ขั้นตอนพัฒนาระบบไคลเอนต์

1. ศึกษาระบบงานในปัจจุบัน ลักษณะการทำงานของระบบลักษณะโครงสร้างข้อมูลที่ใช้ในระบบ และความเป็นไปได้ในการพัฒนาระบบและกำหนดขอบเขตในการพัฒนาระบบ ซึ่งใช้วิธีซักถามจากเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบในระบบงานสารสนเทศในสถาบันฯ
2. ความต้องการของผู้ใช้งานในระบบ โดยค้นหาปัญหาที่เกิดจากการใช้งาน โดยใช้ข้อมูลที่ได้จากการศึกษาระบบงาน และมองถึงปัญหาที่อาจเกิดขึ้นในอนาคต
3. คุณสมบัติของระบบ ทำการกำหนดความสามารถของระบบที่จะทำการออกแบบและพัฒนา เพื่อให้สามารถรองรับกับความต้องการของผู้ใช้งานระบบ
4. ทำการศึกษาเลือกเครื่องมือที่จะใช้ในการพัฒนา โครงการ โดยพิจารณาตามความเหมาะสมในการใช้งาน
5. ทำการพัฒนาโปรแกรม และทำการทดสอบโปรแกรม เพื่อให้โปรแกรม ทำงานได้อย่างถูกต้อง และตรงตามความต้องการของผู้ใช้งาน

4.2 การติดตั้งเครื่องมือที่ใช้ในการพัฒนาโปรแกรม

ในการพัฒนาโปรแกรม ระบบปฏิบัติการที่ใช้เป็นระบบ Unix ของ บ. Sun Microsystems ที่ทำงานบนเครื่องคอมพิวเตอร์ส่วนบุคคล ดังนั้นในการติดตั้งโปรแกรมสนับสนุนจึงจำเป็นต้องหาโปรแกรมที่สามารถทำงานร่วมกันได้กับระบบปฏิบัติการดังกล่าว โดยจะมีวิธีการที่นิยมใช้กันอยู่ 2 วิธีด้วยกันคือ วิธีแรก หาโปรแกรมที่ได้ถูกทำการ Compile สำหรับระบบปฏิบัติการนั้น ๆ ไว้ล่วงหน้าแล้วนำมาติดตั้งใช้งานบนเครื่องของเรา และวิธีที่สอง ทำการ Compile โปรแกรมที่ต้องการบนระบบปฏิบัติการที่ใช้งานอยู่

โปรแกรมที่จะทำหน้าที่เป็น LDAP Server จะทำงานภายใต้ระบบปฏิบัติการ Unix ซึ่งในการติดตั้งโปรแกรมนั้น เราจำเป็นต้องมีการ Compile โปรแกรมใหม่ โดยจะให้ GCC 3.2 เป็น Compiler โดยสำหรับ GCC 3.2 สำหรับ Solaris X86 นั้นเราสามารถทำการ Download ได้โดยไม่มีค่าใช้จ่ายได้จาก <http://www.sunfreeware.com> สำหรับการติดตั้งโปรแกรม GCC นั้นก่อนอื่นต้องทำการคลายการบีบอัดก่อนโดยใช้คำสั่ง

```
"gunzip gcc-3.2.2-sol8-intel-local.gz"
```

หลังจากนั้นจึงสามารถทำการติดตั้งโปรแกรมได้โดยใช้สิทธิ์ root ในการติดตั้ง โดยการ Run คำสั่งดังต่อไปนี้

```
“pkgadd -d gcc-3.2.2-sol8-intel-local”
```

ในการติดตั้ง โปรแกรม GCC นี้ระบบจะทำการติดตั้งโปรแกรมภายใต้ Directory /usr/local นอกจากนี้ให้ทำการติดตั้งโปรแกรม [sed-4.0-sol8-intel-local.gz](http://www.sunfreeware.com) ซึ่งสามารถ Download ได้จากที่ <http://www.sunfreeware.com> เหมือนกับ GCC ส่วนวิธีการติดตั้งโปรแกรมก็ใช้วิธีเดียวกัน

โปรแกรมที่เราได้ทำการติดตั้งไปก่อนหน้านี้เป็นโปรแกรมที่ใช้ในการ Compile Software ที่เรานำมาติดตั้งเพิ่มเติม ดังนั้นหลังจากติดตั้งโปรแกรมดังกล่าวแล้วให้ทำการกำหนด Search Path ไปยังตำแหน่งที่โปรแกรมนั้นอยู่ด้วยโดยทำการกำหนดผ่าน ตัวกำหนดค่าที่ใช้ชื่อว่า “PATH” “PATH=/usr/local/bin:\$PATH “

ในส่วนการติดตั้ง โปรแกรมอื่นๆ ที่เกี่ยวข้องโดยตรงกับการพัฒนาระบบงานนั้น ยังคงมี โปรแกรมอีกหลายตัว ในที่นี้ผู้พัฒนา ได้เลือกใช้โปรแกรมที่เป็นรุ่นที่มีเสถียรภาพและใหม่ที่สุด ที่ โปรแกรมตัวนั้น ๆ มีให้ดังมีรายชื่อโปรแกรมดังต่อไปนี้

Software Name	Version	Software Web Site
Berkeley DB	4.1.25	http://www.sleepycat.com
Openldap	2.1.12	http://www.openldap.org
Apache	1.3.27	http://www.apache.org
PHP	4.3.1	http://www.php.net
Sodo	1.6.6	http://www.sunfreeware.com
Pam_ldap	-	http://www.padl.com

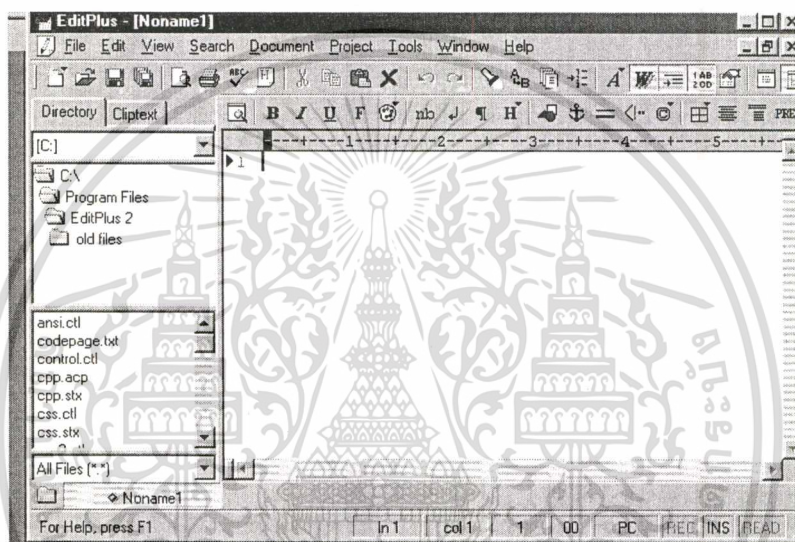
ตารางที่ 4.1 แสดงรายชื่อ Software ที่ใช้ในการพัฒนาระบบงาน

4.3 การพัฒนาโปรแกรม User Management

ในส่วนการพัฒนาโปรแกรม User Management นั้นส่วนการทำงานได้ถูกออกแบบให้มีการติดต่อผู้ใช้งานผ่าน Browser จึงจำเป็นที่ต้องติดตั้ง Web Server ขึ้นมาก่อนโดยได้เลือกใช้

โปรแกรม Web Server ของ Apache เนื่องจากสามารถทำงานได้อย่างรวดเร็ว และสามารถระบุเงื่อนไขการทำงานได้สะดวก และในส่วนของการติดต่อระหว่าง Web Server กับ LDAP นั้น เพื่อให้สามารถประสานการทำงานได้อย่างถูกต้องรวดเร็ว จึงได้นำเอา ภาษาสคริป PHP มาใช้งานร่วมกับ Apache Web Server เพื่อใช้ในการบริหาร จัดการข้อมูลใน LDAP

หลังจากได้ทำการติดตั้งโปรแกรมสนับสนุนต่าง ๆ แล้วก็มาถึงขั้นตอนการเขียนโปรแกรม ทางผู้เขียนเลือกใช้ โปรแกรม Edit Plus ในการเขียนโปรแกรมเนื่องจากมีขนาดเล็กและใช้งานง่าย



รูปที่ 4.1 แสดงหน้าจอของโปรแกรม Edit Plus

4.4 วิธีการทำงานร่วมกับโปรแกรม

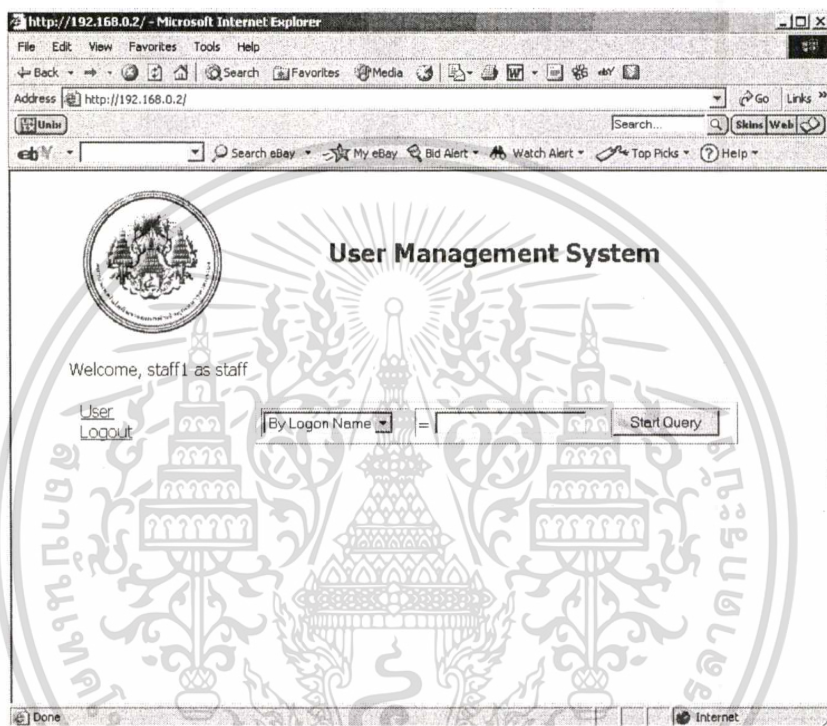
ในการทำงานร่วมกับโปรแกรม ก่อนที่เราจะทำการนำข้อมูลผู้ใช้งานใส่เข้าไปในฐานข้อมูลของ LDAP ได้นั้นเราต้องทำการสร้าง Schema รองรับไว้ก่อน โคน Schema ที่สร้างขึ้นจะเป็นการกำหนดโครงสร้างของ LDAP เพื่อรองรับข้อมูลของผู้ใช้งานตามที่ได้ทำการออกแบบเอาไว้

4.5 ทดสอบการใช้งานโปรแกรม

ในการใช้งานทดสอบการใช้งานโปรแกรมระดับผู้ใช้งาน จะมีการแบ่งระดับการใช้งาน เป็น 3 แบบกล่าวคือ การใช้งานของผู้ใช้งานทั่วไป การใช้งานของผู้ใช้งานระดับ Staff,

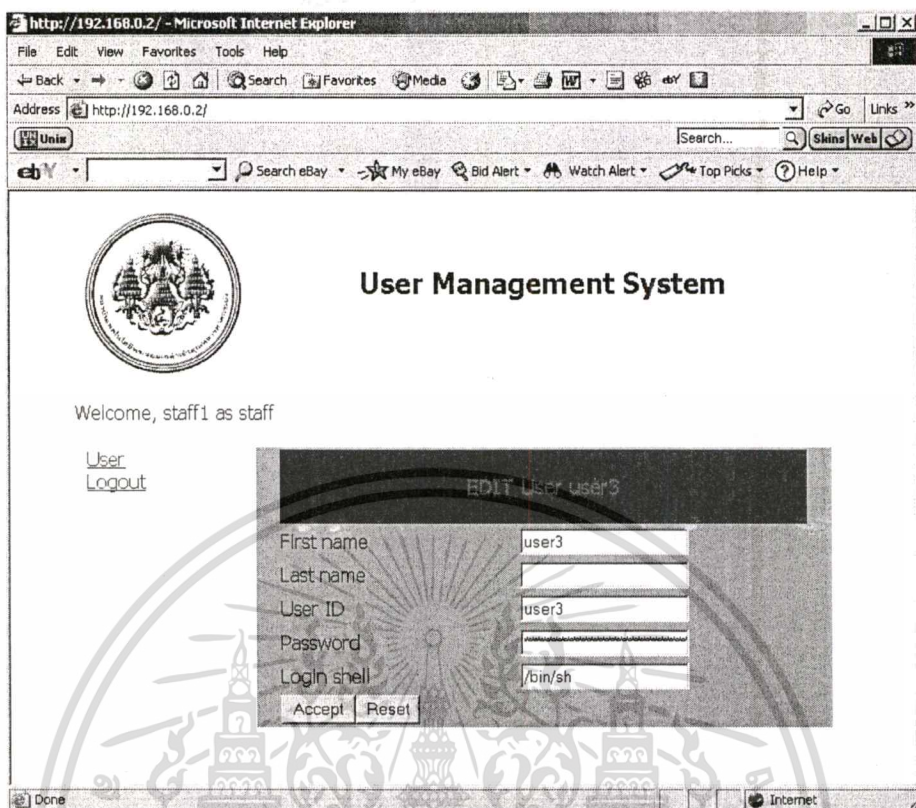
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การใช้งานของผู้ใช้งานระดับ Admin ในส่วนของการใช้งานระดับผู้ใช้งานทั่วไปกับการใช้งานระดับ Staff นั้นสิ่งที่แตกต่างกันคือการใช้งานระดับผู้ใช้งานทั่วไป จะแก้ไขข้อมูลได้เฉพาะ ของตนเองเท่านั้น ในขณะที่ผู้ใช้งานระดับ Staff จะสามารถแก้ไขข้อมูลของผู้ใช้งานทุกคนได้ แต่เป็นการแก้ไขข้อมูลเพียงบางส่วนเท่านั้น สำหรับการใช้งานระดับ Admin จะสามารถแก้ไขข้อมูลของผู้ใช้งานทั้งหมดได้ และสามารถ Approve การทำงานของ Staff ได้ด้วย



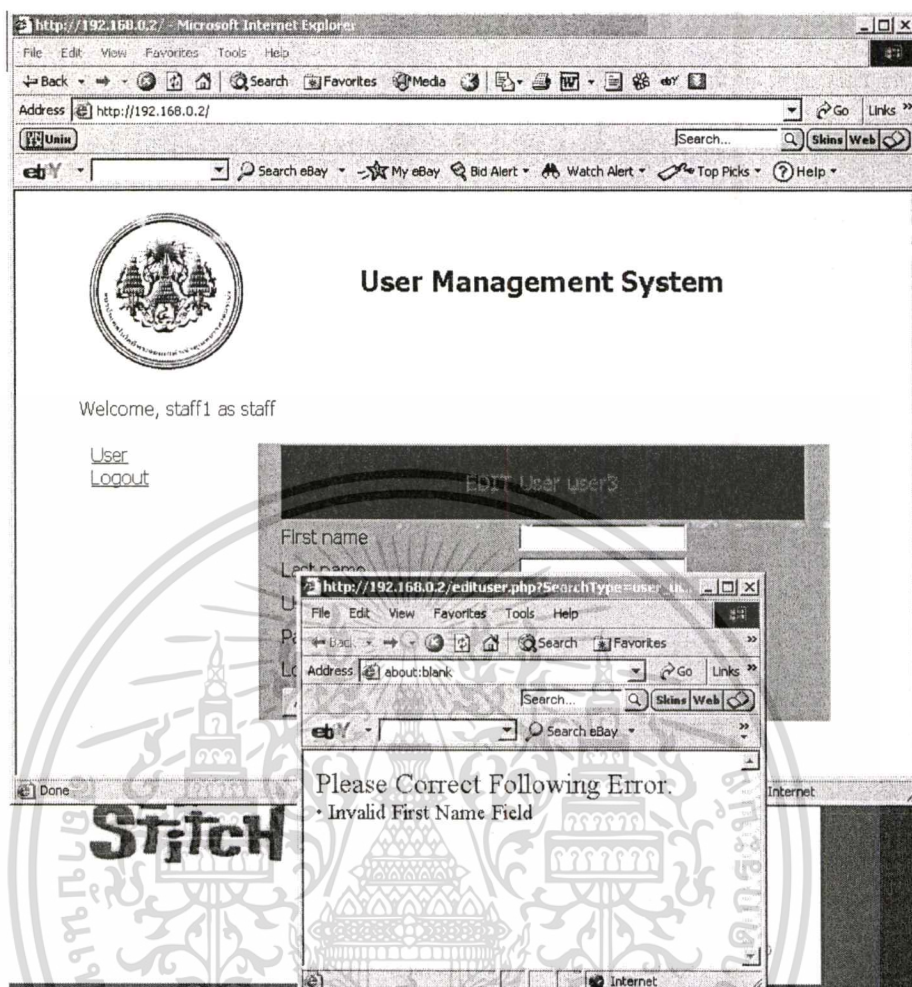
รูปที่ 4.2 แสดงหน้าจอค้นหาข้อมูลผู้ใช้งานของผู้ใช้งานระดับ Staff

จากรูปที่ 4.2 แสดงให้เห็นถึง หน้าจอติดต่อกับผู้ใช้งานระดับ Staff ซึ่งจะสามารถแก้ไขข้อมูลได้เฉพาะ ข้อมูลของผู้ใช้งานเท่านั้นนอกจากนั้นในกรณีที่ Staff ทำการแก้ไขข้อมูลของผู้ใช้งานการทำงานของ Staff จะถูกเก็บลง Approve Log



รูปที่ 4.3 แสดงหน้าจอของการแก้ไขข้อมูลผู้ใช้งาน ของผู้ใช้งานระดับ Staff

ในกรณีที่ทำการแก้ไขข้อมูลผู้ใช้งานหลังจากเลือกรายชื่อผู้ใช้งานที่จะทำการแก้ไขแล้ว ผู้ใช้งานระดับ Staff จะสามารถแก้ไขข้อมูลของผู้ใช้งานในระบบ ได้เพียงบางส่วนเท่านั้น ในส่วนของการแก้ไข Password นั้นหลังจากพิมพ์ Password ใหม่ลงไประบบจะทำการเก็บการแก้ไขลงใน Approve Log ในกรณีที่ใส่ข้อความไม่ครบระบบจะทำการตรวจสอบและแสดงข้อความเตือนออกมา ในรูปที่ 4.4 แสดงให้เห็นถึงการแก้ไขข้อมูลผู้ใช้งาน โดยไม่ได้ระบุ First Name ของผู้ใช้งาน



รูปที่ 4.4 แสดงให้เห็นถึงการแสดงข้อความเตือนในกรณีที่ไม่มีข้อมูลในช่อง Firstname

จากการทดลองใช้งานระบบสามารถตรวจสอบในกรณีที่ไม่มีข้อมูลในช่อง Firest Name และช่อง Password ได้เป็นอย่างดี หลังจากทำการแก้ไขข้อมูลผู้ใช้งานแล้วระบบจะทำการเก็บข้อมูลการแก้ไขลงใน Approve Log ซึ่งในรูปที่ 4.5 แสดงให้เห็นถึงการแก้ไขผู้ใช้งาน User3 ได้ถูกเก็บลง Approve Log แล้ว

```

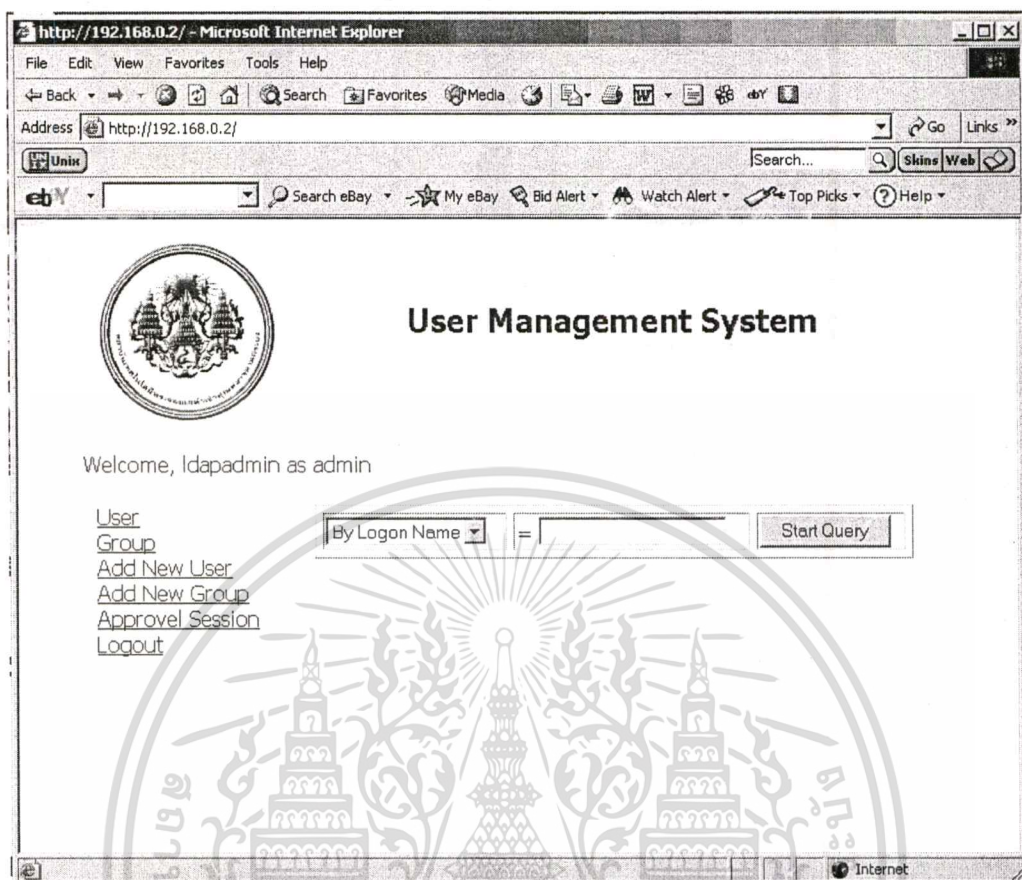
192.168.0.2 - PuTTY
bash-2.03#
bash-2.03# tail -20 um_approve.log
04.04.2003-20.04.24:staff:staff:192.168.0.1:Modify User:cn=user3,ou=people,dc=mydomain,dc=com
bash-2.03# tail -10 um.log
04.04.2003-20.04.41:staff:staff:192.168.0.1:login:cn=staff1,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.43:ldapadmin:admin:192.168.0.1:Authentication Pass:cn=ldapadmin,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.45:ldapadmin:admin:192.168.0.1:Reject Edit:cn=,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.48:ldapadmin:admin:192.168.0.1:Logout:cn=ldapadmin,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.49:staff:staff:192.168.0.1:Authentication Pass:cn=staff1,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.51:staff:staff:192.168.0.1:Modify User:cn=user2,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.54:staff:staff:192.168.0.1:Login:cn=staff1,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.55:ldapadmin:admin:192.168.0.1:Authentication Pass:cn=ldapadmin,ou=people,dc=mydomain,dc=com
04.04.2003-20.04.59:ldapadmin:admin:192.168.0.1:Approve Edit:cn=user2,ou=people,dc=mydomain,dc=com
bash-2.03#

```

รูปที่ 4.5 แสดงข้อมูลที่ถูกเก็บลงใน UM_Approve.log

ต่อไปจะทำการทดสอบในส่วนการใช้งานของผู้ใช้งานระดับ Admin หลังจากทำการใส่ระ
หวัผู้ใช้งาน และรหัสผ่านแล้วจะเข้าสู่หน้าจอของผู้ใช้งานระดับ Admin โดย ในหน้าจอผู้ใช้งาน
ระดับ Admin จะสามารถทำการแก้ไขข้อมูลต่างๆ ได้ทั้งหมด จากรูปที่ 4.6 จะเห็นว่า Admin
สามารถสร้างผู้ใช้งานใหม่ กลุ่มของผู้ใช้งานใหม่ รวมทั้งทำการแก้ไขข้อมูลของผู้ใช้งานหรือกลุ่ม
ของผู้ใช้งานที่ได้ทำการกำหนดไว้ก่อนได้ รวมทั้งสามารถทำการ Approve การทำงานของผู้ใช้งาน
ระดับ Staff ได้ด้วย

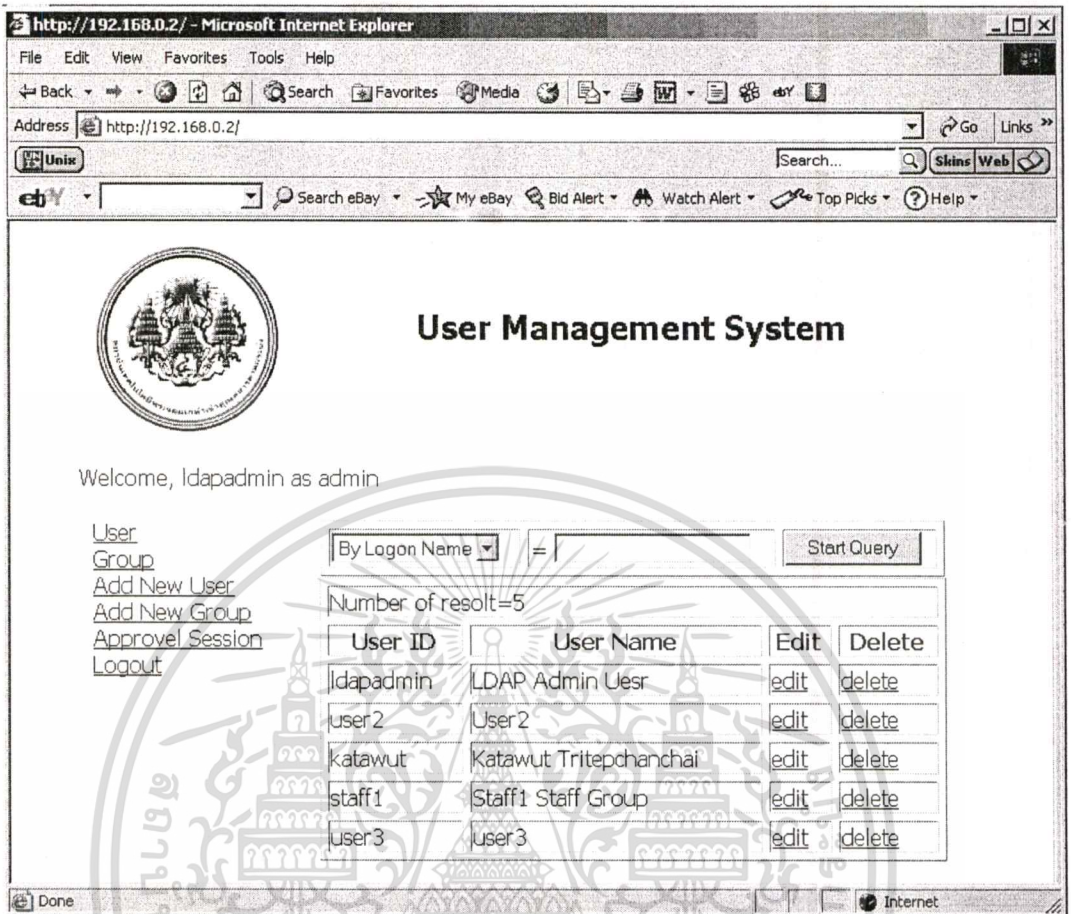
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.6 แสดงหน้าจอการค้นหาผู้ใช้งานของผู้ใช้งานระดับ Admin

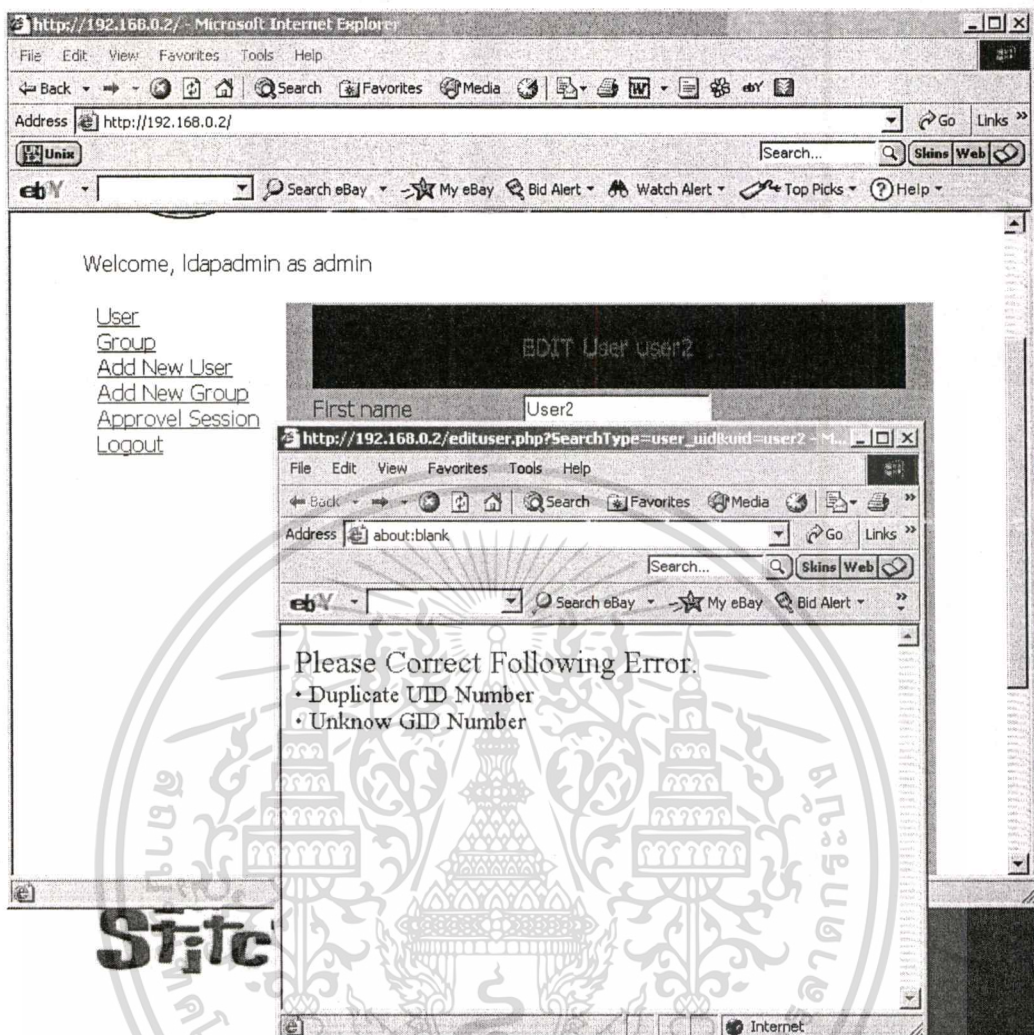
ในการทำการแก้ไขข้อมูลผู้ใช้งานผู้ใช้งานระดับ Admin จะทำการค้นหาข้อมูลผู้ใช้งานโดยทำการค้นหาจากระบบ และระบบจะแสดงรายชื่อผู้ใช้งานที่ตรงกับความต้องการขึ้นมาแสดงดังในรูป 4.7 ได้แสดงถึงการแสดงรายชื่อผู้ใช้งานทั้งหมดของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.7 แสดงหน้าจอผลการค้นหารายชื่อผู้ใช้งานของผู้ใช้งานระดับ Admin

ในกรณีที่ทำการแก้ไขข้อมูลผู้ใช้งานก็เพียงกด edit link ระบบก็จะแสดงรายละเอียดของผู้ใช้งานคนนั้นขึ้นมาและแสดงค่าของข้อมูลขึ้นมาพร้อมกัน นอกจากนั้นในกรณีที่การแก้ไขข้อมูลแล้วข้อมูลรหัสผู้ใช้งาน, UID, GID ของผู้ใช้งานไปตรงกับผู้อื่นที่มีอยู่ในระบบ ระบบจะแสดงข้อความเตือนและไม่ยอมเปลี่ยนแปลงค่าต่าง ๆ ของผู้ใช้งานนั้น จากรูป 4.8 จะแสดงให้เห็นว่าการแก้ไขข้อมูลของ User2 ค่า UID ไปตรงกับผู้ใช้งานอื่นในระบบ ส่วน GID นั้นเป็นค่า GID ที่ไม่มีในระบบ

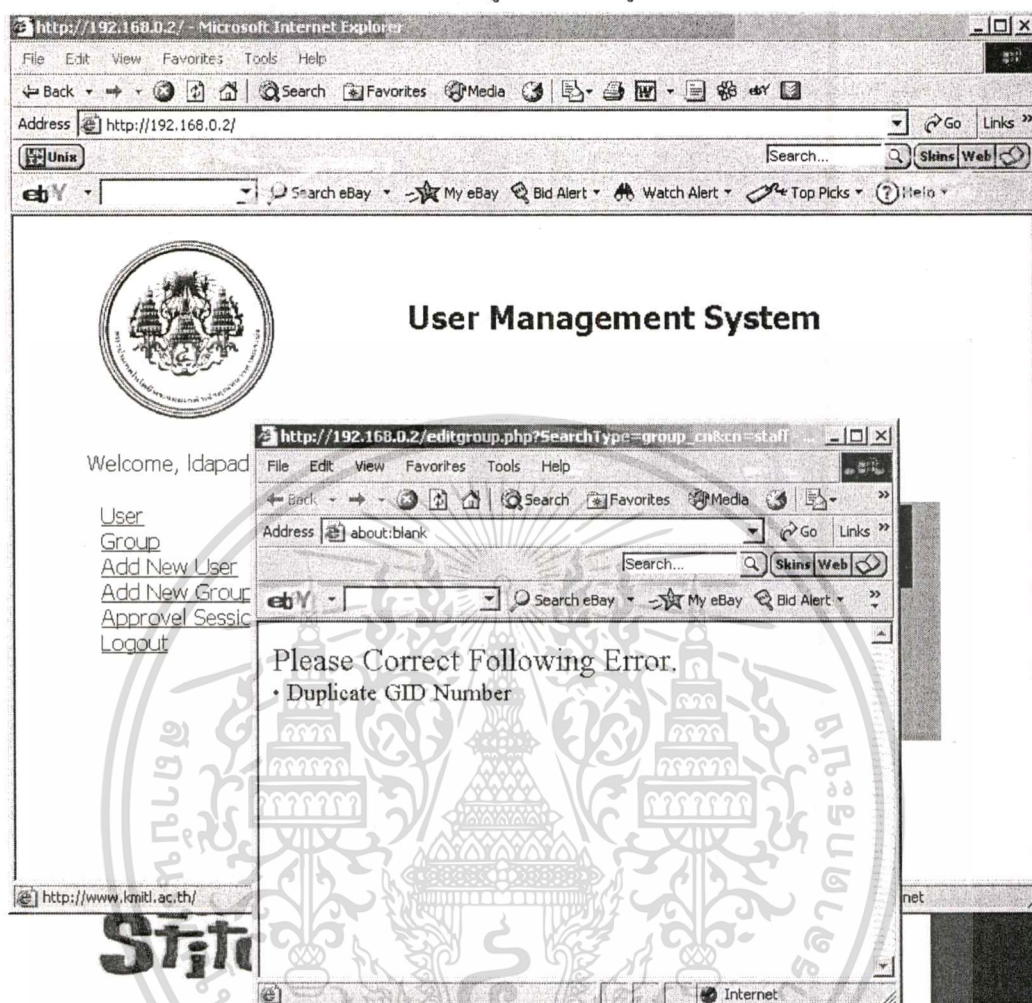


รูปที่ 4.8 แสดงหน้าจอแจ้งเตือน UID ซ้ำกับผู้ใช้งานในระบบ และ GID ไม่มีอยู่จริงในระบบ

นอกจากนี้ในส่วนของการแก้ไขกลุ่มผู้ใช้งานหลังจากที่ได้ทำการเลือกกลุ่มผู้ใช้งานที่จะทำการแก้ไขแล้ว ได้ทำการทดสอบการทำงานโดยทำการแก้ GID ให้ไปตรงกับค่า GID ที่มีอยู่แล้วใน

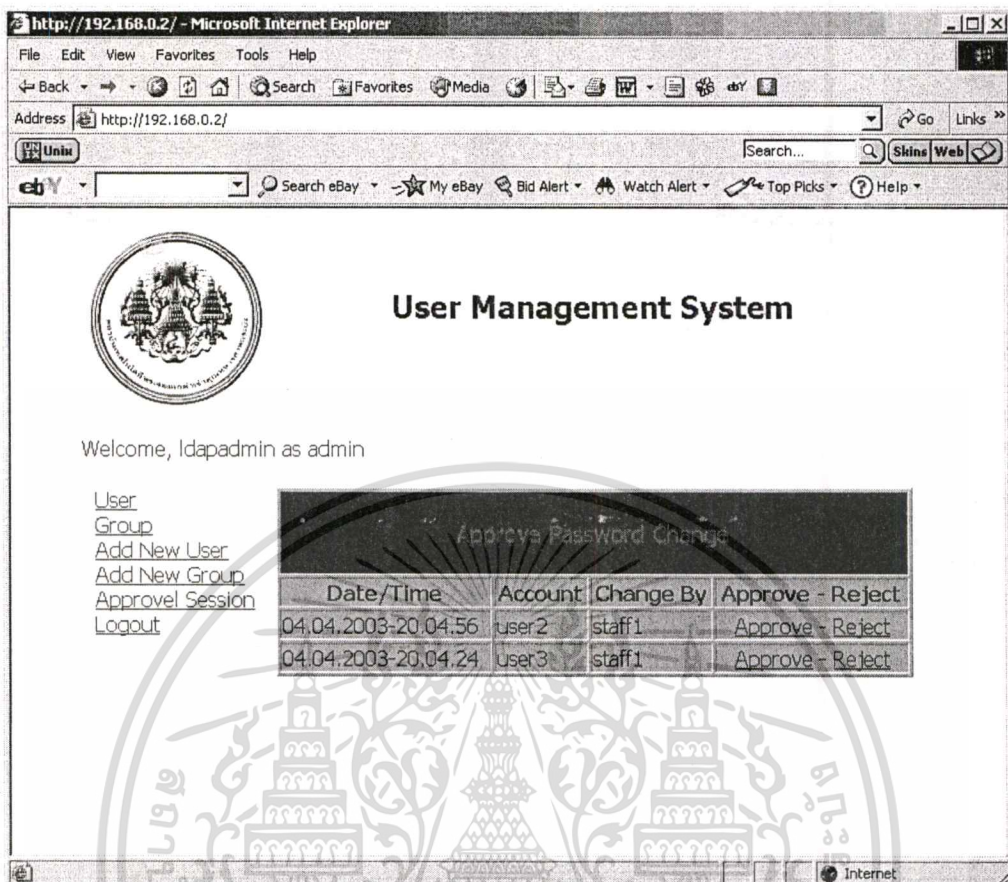
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบ โดยที่ระบบจะทำการแจ้งเตือนได้อย่างถูกต้องดังในรูป



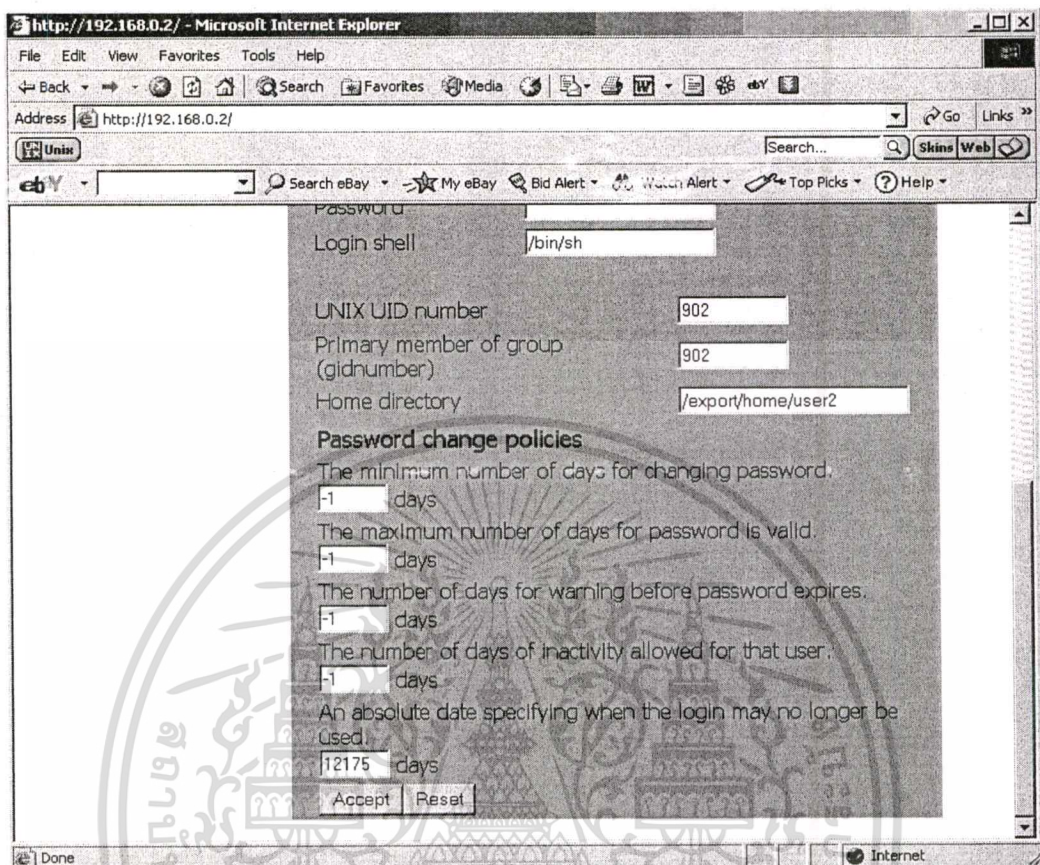
รูปที่ 4.9 แสดงหน้าจอแจ้งเตือนค่าของ GID ของกลุ่มผู้ใช้งานมีอยู่แล้วในระบบ

ในกรณีที่ผู้ใช้งานระดับ Admin จะทำการตรวจสอบการทำงานของผู้ใช้งานระดับ Staff ผู้ใช้งานระดับ Admin จะทำการเข้าสู่หน้าจอ Approve จากรูปจะเห็นว่าการแก้ไขข้อมูลผู้ใช้งาน password ของผู้ใช้งาน User2 และ User3 ซึ่งจะแสดงวันและเวลาที่ข้อมูลผู้ใช้งานถูกแก้ไข รวมทั้งข้อมูลผู้แก้ไขด้วย



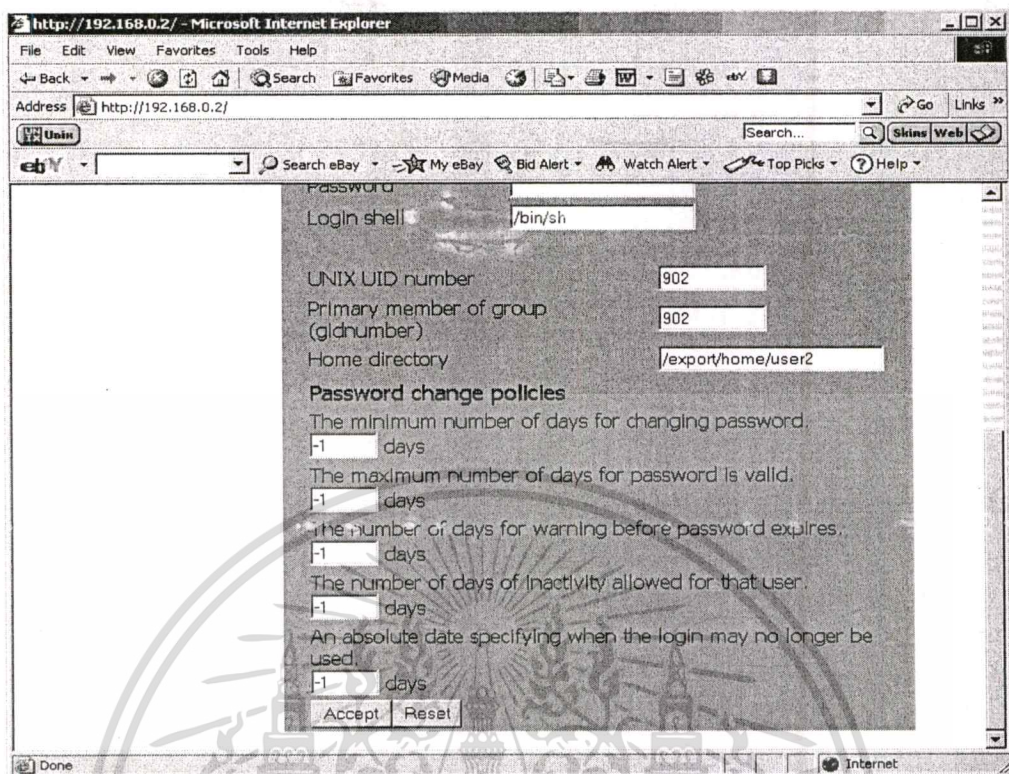
รูปที่ 4.10 แสดงหน้าจอ Approve ของผู้ใช้งานระดับ Admin

จากรูปที่ 4.11 แสดงให้เห็นถึงการแก้ไข Password ของผู้ใช้งานระดับ Staff โดยทำการแก้ไข password ของ User2 จะเห็นได้ว่าจะมีข้อมูลของวันหมดอายุของผู้ใช้งานผู้นี้อยู่ แสดงอยู่ในด้านล่างสุดของหน้าจอ ซึ่งข้อมูลนี้เป็นข้อมูลของผู้ใช้งานก่อนที่ผู้ใช้งานระดับ Admin จะทำการ Approve การทำงาน ซึ่งหากผู้ใช้งานระดับ Admin ไม่ Approve รหัสผู้ใช้งานนี้จะใช้ได้เพียง 30 วัน หลังจากทำการแก้ไข Password



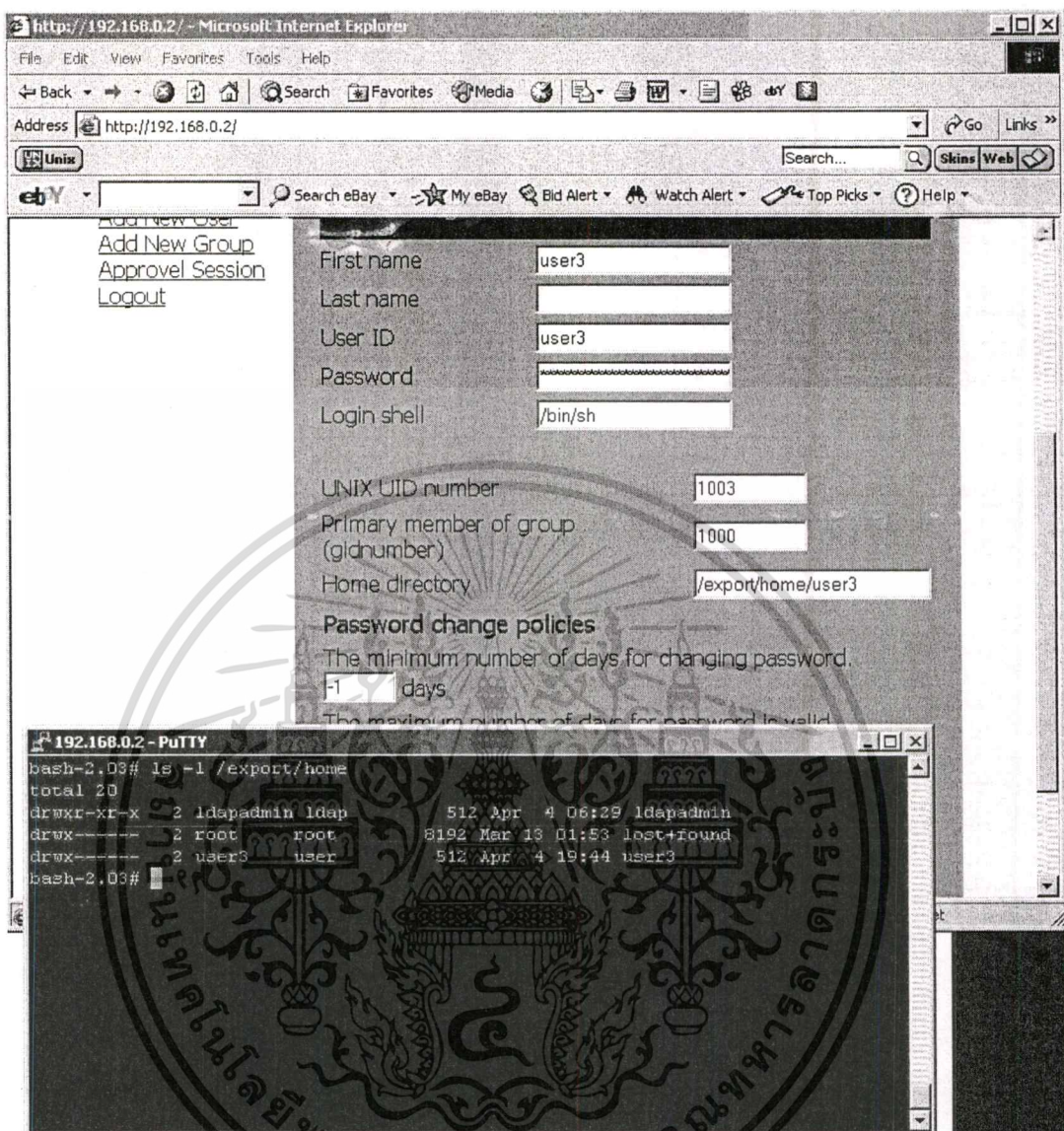
รูปที่ 4.11 แสดงหน้าจอรายละเอียดผู้ใช้งาน ก่อนทำการ Approve

หลังจากที่ได้ทำการ Approve ข้อมูลผู้ใช้งานแล้ว จะเห็นได้ว่าค่าของ UserExpire จะมีการเปลี่ยนแปลงไปเป็นค่า -1 ซึ่งหมายถึง Account นี้จะไม่มีวันหมดอายุ



รูปที่ 4.12 แสดงหน้าจอรายละเอียดผู้ใช้งาน หลังทำการ Approve

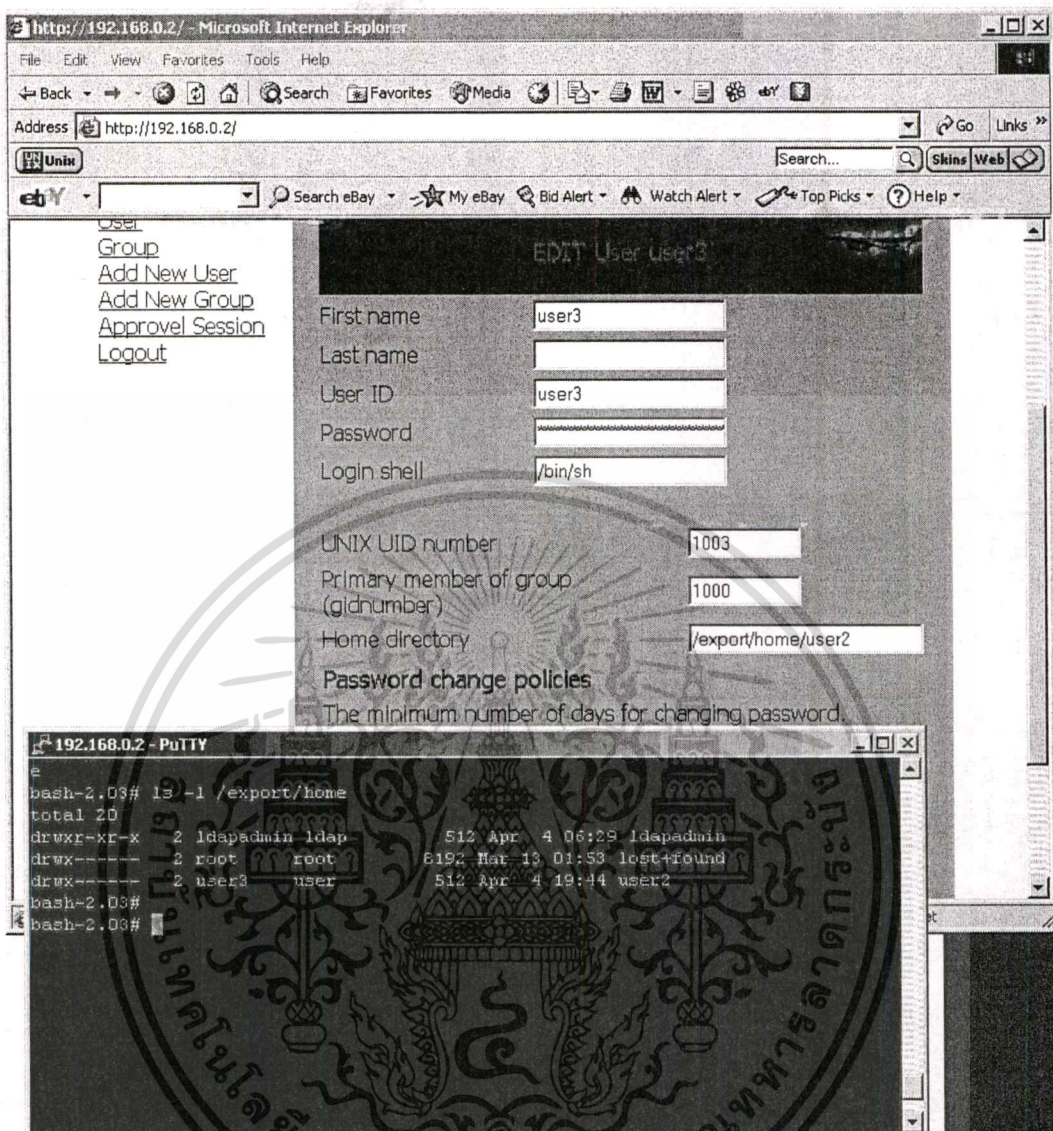
ในการแก้ไขข้อมูลของ Home Directory ของผู้ใช้งานระบบจะทำการตรวจสอบว่ามี Home directory อยู่หรือไม่ถ้ามี Home Directory อยู่ระบบจะทำการ ย้าย Home Directory ชื่อเก่าไปเป็น Home Directory ชื่อใหม่รวมทั้งหากมีการเปลี่ยนแปลง UID หรือ GID ระบบจะทำการแก้ไขให้ที่ Home Directory ให้ด้วย



รูปที่ 4.13 แสดงหน้ารายละเอียดผู้ใช้ก่อนทำการแก้ไขข้อมูลของ Home Directory

หลังจากที่ได้ทำการเปลี่ยนแปลงข้อมูล Home Directory ของผู้ใช้งานระบบแล้วจะได้ผลตามที่แสดงในรูปที่ 4.14

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.14 แสดงหน้ารายละเอียดผู้ใช้งาน หลังทำการแก้ไขข้อมูลของ Home Directory

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

สรุปผลการค้นคว้าและพัฒนาระบบ

5.1 ผลจากการพัฒนาระบบ

การพัฒนาระบบช่วยในการบริหารบัญชีผู้ใช้งาน จากผลการใช้งานสามารถสรุปผลได้ดังนี้

5.1.1 การศึกษาการทำงานของ Directory Service

ผลการศึกษาพบว่า Directory Service มีประโยชน์อย่างยิ่งในการช่วยบริหารจัดการระบบบัญชีผู้ใช้งาน ลดความซ้ำซ้อนของข้อมูลที่เกิดขึ้นในหลายๆ ระบบ มีผลทำให้ข้อมูลมีความน่าเชื่อถือ

5.1.2 การวิเคราะห์และออกแบบ

ในการวิเคราะห์และออกแบบ ได้ทำการออกแบบการบริหารการใช้งานของบัญชีผู้ใช้งานจากศูนย์กลาง ทำให้สามารถลดความยุ่งยากซับซ้อนในการจัดการ และเพิ่มความรวดเร็วในการให้บริการนักศึกษาได้เป็นอย่างดี

5.1.3 การพัฒนาระบบงาน

ได้ทำการออกแบบการทำงานผ่าน Browser ทำให้เพิ่มความสะดวกในการใช้งานเนื่องจากสามารถใช้งานโปรแกรมได้จากหลายๆ สถานที่ นอกจากนี้ระบบยัง มีการตรวจสอบสิทธิ์การใช้งานเพื่อป้องกันผู้ที่ไม่มีหน้าที่เกี่ยวข้องเข้าไปทำการแก้ไขข้อมูล

5.2 ผลจากการทดสอบโปรแกรม

จากการทดสอบการใช้งานโปรแกรมโดยได้ทำการใช้งานตามความสามารถหลักที่โปรแกรมสามารถทำงาน ได้รับผลลัพธ์ดังนี้

5.2.1 ทำการดึงข้อมูลจากระบบ Unix เข้าไปในฐานข้อมูล Directory Service สามารถทำงานได้เป็นอย่างดี

5.2.2 ทำการค้นหาข้อมูลผู้ใช้งานระบบโดยระบุ ชื่อผู้ใช้งาน, รหัสผู้ใช้งาน, รหัสกลุ่ม สามารถค้นหาและแสดงข้อมูลได้อยู่ถูกต้อง

5.2.3 ทำการแก้ไขข้อมูลของผู้ใช้งาน และ ข้อมูลของกลุ่ม สามารถทำการแก้ไขและสามารถป้องกันความผิดพลาดเนื่องจากการแก้ไขข้อมูลไปตรงกับ ข้อมูลที่มีอยู่

แล้วในระบบได้ รวมทั้งทำการค้นหาและแสดงช่องข้อมูลที่ทำกรใส่ข้อมูลไม่ครบถ้วนได้

- 5.2.4 ทำการเพิ่มผู้ใช้งานและกลุ่มผู้ใช้งานในระบบได้อย่างถูกต้อง
- 5.2.5 สามารถทำการตรวจสอบการทำงานทุกขั้นตอนผ่านระบบ Log File ได้
- 5.2.6 สามารถกำหนดสิทธิ์การใช้งานระบบได้ สามระดับ
 - 5.2.6.1 สิทธิ์ระดับ Admin สามารถทำการแก้ไข ปรับปรุง ข้อมูลทุกอย่างภายในระบบ Directory ได้ทั้งหมด
 - 5.2.6.2 สิทธิ์ระดับ Staff สามารถทำการแก้ไขข้อมูลชื่อของผู้ใช้งานได้ทุกคนและสามารถทำการแก้ไขข้อมูล Password ของผู้ใช้งานได้ทุกคน
 - 5.2.6.3 สิทธิ์ระดับ User สามารถทำการแก้ไขข้อมูลชื่อของผู้ใช้งานและแก้ไขข้อมูล Password เฉพาะของตนเองเท่านั้น
- 5.2.7 ผู้ใช้งานระบบ สิทธิ์ระดับ Admin สามารถรับรองผลการทำงานของผู้ใช้งานระบบ สิทธิ์ระดับ Staff ได้ในกรณีทำการแก้ไข Password ของผู้ใช้งานระบบ

5.3 อุปสรรคในการพัฒนาโปรแกรม

- 5.3.1 การพัฒนามีการนำโปรแกรม หลายชนิดมาใช้งานร่วมกันจึงเกิด ความยุ่งยากในการติดตั้งให้ โปรแกรมต่าง ๆ สามารถทำงานร่วมกันได้
- 5.3.2 ในการพัฒนาระบบเนื่องจาก LDAP Server ที่เลือกใช้ สามารถทำงานได้บนดีระบบปฏิบัติการ Unix จึงต้องมีการจัดเตรียมเครื่องเพื่อใช้เป็น LDAP Server โดยเฉพาะ
- 5.3.3 เนื่องจากระบบ Directory ยังค่อนข้างเป็นเทคโนโลยีที่ใหม่ทำให้มีเอกสารอ้างอิงไม่มากนัก ทำให้การทำความเข้าใจการทำงานต้องใช้เวลาศึกษามากกว่าที่ควร

5.4 ข้อเสนอแนะ

- 5.4.1 ในการติดตั้งโปรแกรมหรือทำการแก้ไขค่า Configuration ต่าง ๆ ของโปรแกรม ควรทำการสำรองข้อมูลเอาไว้ก่อนเพื่อป้องกันความผิดพลาดที่อาจจะเกิดขึ้นได้
- 5.4.2 ในกรณีที่ต้องการเปลี่ยนแปลงค่า Configuration ของ Directory ควรทำการแก้ไขในช่วงที่ไม่มีการใช้งาน
- 5.4.3 ในการติดตั้ง โปรแกรมที่ใช้ในการทำงานต่าง ๆ ควรทำการจดค่าที่ใช้ในการติดตั้งทุกครั้งเพื่อใช้ในการเตือนความจำ ถ้าต้องมาติดตั้งใหม่ภายหลัง

บรรณานุกรม

สำนักวิจัยและบริการคอมพิวเตอร์. 2002. Computer Research Service Center, KMITL [Online].

Available: <http://www.kmitl.ac.th/crsc/index.html>

Howard, L. 1998. Request for Comments 2307. [Online].

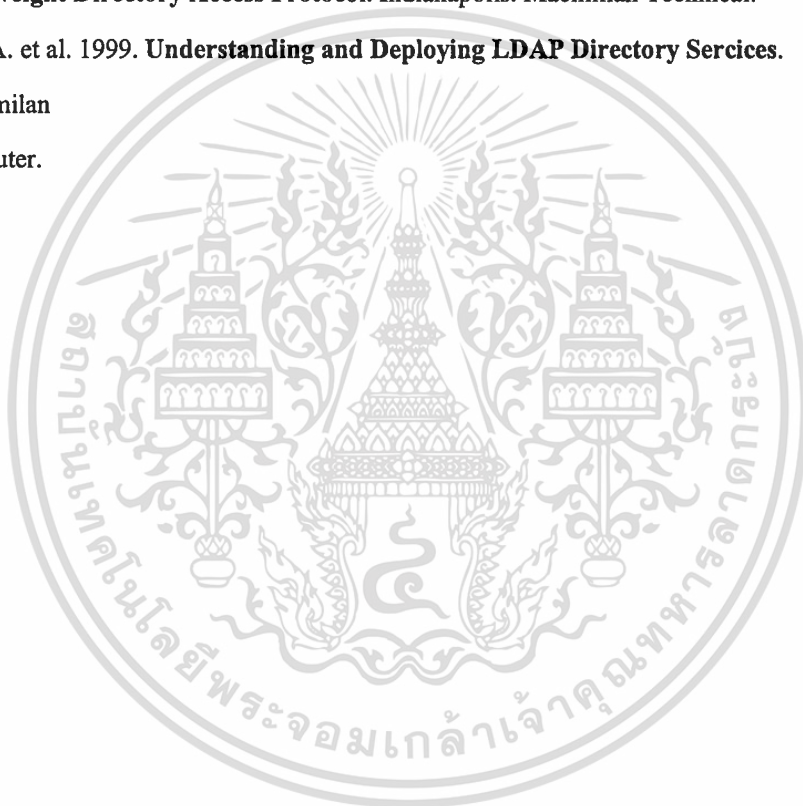
Available: <http://www.ietf.org/rfc/rfc2307.txt>

Howes, T. and Smith, M. 1997. **LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol**. Indianapolis. Macmillan Technical.

Timothy, A. et al. 1999. **Understanding and Deploying LDAP Directory Services**.

USA. Macmillan

Computer.



ภาคผนวก



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก.

ตัวอย่าง Configuration File ของโปรแกรม Apache

```

ServerType standalone
ServerRoot "/opt/apache_1.3.27"
PidFile /opt/apache_1.3.27/logs/httpd.pid
ScoreBoardFile /opt/apache_1.3.27/logs/httpd.scoreboard
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MinSpareServers 5
MaxSpareServers 10
StartServers 5
MaxClients 150
MaxRequestsPerChild 0
LoadModule php4_module      libexec/libphp4.so
Port 80
User nobody
Group nobody
ServerAdmin root@titan.com

```

```

DocumentRoot "/opt/web"
<Directory "/opt/web">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

```

```
<IfModule mod_dir.c>
```

```
    DirectoryIndex index.php index.html
```

```
</IfModule>
```

```
HostnameLookups Off
```

```
ErrorLog /opt/apache_1.3.27/logs/error_log
```



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข.

ตัวอย่าง Configuration File ของโปรแกรม Openldap

```
include      /opt/openldap_2.1.12/etc/openldap/schema/core.schema
include      /opt/openldap_2.1.12/etc/openldap/schema/cosine.schema
include      /opt/openldap_2.1.12/etc/openldap/schema/nis.schema
pidfile      /opt/openldap_2.1.12/var/slaped.pid
argsfile     /opt/openldap_2.1.12/var/slaped.args
backend      bdb
database     bdb
suffix       "dc=mydomain,dc=com"
rootdn       "cn=Manager,dc=mydomain,dc=com"
rootpw       secret
directory    /opt/openldap_2.1.12/var/openldap-data
index objectClass eq
```

ภาคผนวก ค.

ตัวอย่าง File LDIF

dn: dc=mydomain,dc=com
objectClass: top
objectClass: domain
dc: mydomain

dn: ou=People,dc=mydomain,dc=com
objectClass: top
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=mydomain,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Group



ภาคผนวก ง.

การติดตั้ง Program

ขั้นตอนการติดตั้งโปรแกรม Berkelay DB

1. `export CC=gcc`
2. `cd /root/src/db-4.1.25.NC/build_unix`
3. `./dist/configure --prefix=/opt/db_4.1.25`
4. `make`
5. `make install`

ขั้นตอนการติดตั้งโปรแกรม Openldap

1. `export CC=gcc`
2. `export CPPFLAGS="-I/opt/db_4.1.25/include"`
3. `export LDFLAGS="-L/opt/db_4.1.25/lib"`
4. `cd /root/src/openldap-2.1.12`
5. `./configure --prefix=/opt/openldap_2.1.12`
6. `make depend`
7. `make`
8. `make install`

ขั้นตอนการติดตั้งโปรแกรม APACHE

1. `/root/src/apache_1.3.27`
2. `./configure --prefix=/opt/apache_1.3.27 --enable-module=so`
3. `make`
4. `make install`

ขั้นตอนการติดตั้งโปรแกรม PHP

1. `./configure --prefix=/opt/php_4.3.1 --with-apxs=/opt/apache_1.3.27/bin/apxs --with-ldap=/opt/openldap_2.1.12`
2. `make`
3. `make install`

ขั้นตอนการติดตั้งโปรแกรม Pam_ldap

1. `./configure --prefix=/opt/pam_ldap_161 --with_ldap_lib=openldap`
2. `make`
3. `make install`

ขั้นตอนการติดตั้งโปรแกรม Sudo

1. `/root/src/sudo_1.6.6`
2. `./configure --prefix=/opt/sudo_1.6.6`
3. `make`
4. `make install`

การแก้ไขค่าของ Software Apache

แก้ไข File `httpd.conf`

```
<IfModule mod_dir.c>
```

```
DirectoryIndex index.html เปลี่ยนเป็น DirectoryIndex index.php index.html
```

```
</IfModule>
```

```
AddType application/x-httpd-php .php
```

การแก้ไขค่าของ Software Open LDAP

ทำการกำหนดค่าต่างๆ ใน File /opt/openldap_2.1.12/etc/openldap/slapd.conf
 โดยทำการเพิ่ม ค่าเหล่านี้เข้าไป

```
include      /opt/openldap_2.1.12/etc/openldap/schema/cosine.schema
include      /opt/openldap_2.1.12/etc/openldap/schema/nis.schema
backend      bdb
suffix       "dc=mydomain,dc=com"
rootdn       "cn=Manager,dc=mydomain,dc=com"
```

การแก้ไขค่าของ Software Pam_ldap

```
cp /opt/pam_ldap_161/etc/ldap.conf /etc/ldap.conf
vi /etc/ldap.conf
    host 127.0.0.1
    base dc=mydomain,dc=com
    pam_crypt local

ldd /opt/pam_ldap_161/lib/security/pam_ldap.so
cp -p /opt/pam_ldap_161/lib/security/pam_ldap.so.1 /usr/lib/security/pam_ldap.so.1
ln -s /usr/lib/security/pam_ldap.so.1 /usr/lib/security/pam_ldap.so

vi /var/ldap/ldap_client_cred
    NS_LDAP_BINDDN= cn=Manager,dc=mydomain,dc=com
    NS_LDAP_BINDPASSWD= secret

vi /var/ldap/ldap_client_file
    NS_LDAP_FILE_VERSION= 1.0
    NS_LDAP_SERVERS= localhost
    NS_LDAP_SEARCH_BASEDN= dc=mydomain,dc=com
    NS_LDAP_AUTH= NS_LDAP_AUTH_NONE
    NS_LDAP_TRANSPORT_SEC= NS_LDAP_SEC_NONE
```

```

NS_LDAP_SEARCH_REF= NS_LDAP_FOLLOWREF
NS_LDAP_DOMAIN=
NS_LDAP_EXP= 1050487053
NS_LDAP_SEARCH_SCOPE= NS_LDAP_SCOPE_ONELEVEL
NS_LDAP_SEARCH_TIME= 30
NS_LDAP_BIND_TIME= 30

```

vi /etc/pam.conf

```

login auth sufficient /usr/lib/security/$ISA/pam_unix.so.1
login auth required /usr/lib/security/$ISA/pam_ldap.so.1 try_first_pass
...
other password sufficient /usr/lib/security/$ISA/pam_unix.so.1
other password required /usr/lib/security/$ISA/pam_ldap.so.1

```

vi /etc/nsswitch.conf

```

passwd:      files ldap
group:       files ldap

```

/etc/init.d/ldap.client start

/etc/init.d/nscd start

การแก้ไขค่าของ Software Sudo

ทำการกำหนดค่าต่างๆ โดยเรียก File /opt/sudo_166/sbin/visudo
 โดยทำการเพิ่ม ค่าเหล่านี้เข้าไป

```

nobody ALL=NOPASSWD: /usr/bin/mkdir -p *, \
/usr/bin/rm -r *, \
/usr/bin/chown -R *, \
/usr/bin/chmod *, \
/usr/bin/mv *

```

ภาคผนวก จ.

Source ของโปรแกรม Import Unix Account to LDIF

```

#!/opt/php_4.3.1/bin/php -q
<?
define(SUFFIX, "dc=mydomain, dc=com");
error_reporting(4);
if ($argc < 3)
    exit("usage: $argv[0] passwd-file shadow-file\n");

if ( is_readable($argv[1])){
    $f = fopen($argv[1], "r");}
else
    exit("Coudln't open $argv[1] for read\n");

if ( is_readable($argv[2])){
    $f1 = fopen($argv[2], "r");}
else
    exit("Coudln't open $argv[2] for read\n");

while (! feof($f))
{
    $line = chop(fgets($f, 10240));
    $line1 = chop(fgets($f1, 10240));
    if (feof($f))
        break;
    $pwent = explode(":", $line);
    $pwent1 = explode(":", $line1);
    if (($pwent[2] < 100)||($pwent[2] > 60000))
        continue;
    $e = 0;
    $ldifent[$e++] = "dn: uid=$pwent[0], ou=people, " . SUFFIX . "\n";

```

```

$ldifent[$e++] = "objectClass: top\n";
$ldifent[$e++] = "objectClass: account\n";
$ldifent[$e++] = "objectClass: posixAccount\n";
$ldifent[$e++] = "objectClass: shadowAccount\n";
$ldifent[$e++] = "cn: $pwent[0]\n";
$ldifent[$e++] = "uid: $pwent[0]\n";
$ldifent[$e++] = "userPassword: {crypt}$pwent1[1]\n";
$ldifent[$e++] = "uidNumber: $pwent[2]\n";
$ldifent[$e++] = "gidNumber: $pwent[3]\n";
if ($pwent[4]) $ldifent[$e++] = "gecos: $pwent[4]\n";
else $ldifent[$e++] = "gecos: -1\n";
$ldifent[$e++] = "homeDirectory: $pwent[5]\n";
$ldifent[$e++] = "loginShell: $pwent[6]\n";
$ldifent[$e++] = "shadowLastchange: $pwent1[2]\n";

if ($pwent1[3]) $ldifent[$e++] = "shadowMin: $pwent1[3]\n";
else $ldifent[$e++] = "shadowMin: -1\n";
if ($pwent1[4]) $ldifent[$e++] = "shadowMax: $pwent1[4]\n";
else $ldifent[$e++] = "shadowMax: -1\n";
if ($pwent1[5]) $ldifent[$e++] = "shadowWarning: $pwent1[5]\n";
else $ldifent[$e++] = "shadowWarning: -1\n";
if ($pwent1[6]) $ldifent[$e++] = "shadowInactive: $pwent1[6]\n";
else $ldifent[$e++] = "shadowInactive: -1\n";
if ($pwent1[7]) $ldifent[$e++] = "shadowExpire: $pwent1[7]\n";
else $ldifent[$e++] = "shadowExpire: -1\n";
if ($pwent1[8]) $ldifent[$e++] = "shadowFlag: $pwent1[8]\n";
else $ldifent[$e++] = "shadowFlag: -1\n";

for ($ctr = 0; $ctr < count($ldifent); $ctr++)
{

```

```
if ($ldifent[$ctr])
    echo $ldifent[$ctr];
}
unset($ldifent);
unset($pwent);
unset($pwent1);
}
?>
```



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ฉ.

Source ของโปรแกรม Import Unix Group to LDIF

```

#!/opt/php_4.3.1/bin/php -q
<?

define(SUFFIX, "dc=mydomain, dc=com");
error_reporting(4);
if ($argc < 2)
    exit("usage: $argv[0] group-file\n");
if ( ! is_readable($argv[1])){
    $f = fopen($argv[1], "r");}
else    exit("Couldn't open $argv[1] for read\n");
while ( ! feof($f))
{
    $line = chop(fgets($f, 10240));
    if (feof($f))
        break;
    $gpent = explode(":", $line);
    $e = 0;
    $ldifent[$e++] = "dn: cn=$gpent[0], ou=group, " . SUFFIX . "\n";
    $ldifent[$e++] = "objectClass: top\n";
    $ldifent[$e++] = "objectClass: posixGroup\n";
    $ldifent[$e++] = "cn: $gpent[0]\n";
    $ldifent[$e++] = "gidNumber: $gpent[2]\n";
    for ($ctr = 0; $ctr < count($ldifent); $ctr++)
    {
        if ($ldifent[$ctr])
            echo $ldifent[$ctr];
    }
    if($gpent[3]){
        $gpid = explode("",$gpent[3]);

```

```

        for ($i=0;$i < count($gpuid);$i++)
        echo "memberUid: $gpuid[$i]\n";
    }
    echo "\n";
    unset($ldifent);
    unset($gpent);
}
?>

```



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ข.

Source ของโปรแกรมที่ใช้ Start/Stop Openldap

```
#!/sbin/sh

#

# Copyright (c) 1999 by Sun Microsystems, Inc.
# All rights reserved.
#

#ident  "@(#)slpd      1.1      99/04/02 SMI"

LD_LIBRARY_PATH=/opt/db_4.1.25/lib
export LD_LIBRARY_PATH

case "$1" in
'start')
    /opt/openldap_2.1.12/libexec/slapd
    ;;

'stop')
    kill -INT `cat /opt/openldap_2.1.12/var/slapd.pid`
    ;;

*)
    echo "Usage: $0 { start | stop }"
    exit 1
    ;;

esac

exit 0
```

ประวัติผู้เขียน

ชื่อผู้เขียน	นายคทาวุธ ตรีเทพชาญชัย
วันเกิด	19 พฤษภาคม 2517
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษาระดับปริญญาตรี	วิศวกรรมศาสตรบัณฑิต (คอมพิวเตอร์)
สถานที่สำเร็จการศึกษา	คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง
ปีการศึกษาที่สำเร็จการศึกษา	2539

