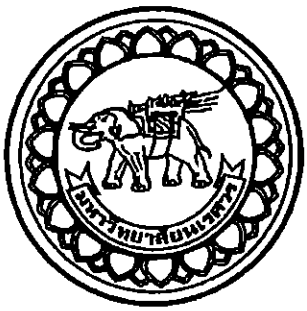


การใช้สมาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้

AUTHENTICATING SECURELY VIA UNTRUSTED COMPUTER BY USING SMARTPHONE

นางสาวจารุวรรณ งามสอาด รหัส 52371207

นายศรัณย์ ภู่นพคุณ รหัส 52371504

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร

ปีการศึกษา 2555

ใบรับรองปริญญานิพนธ์

ชื่อหัวข้อโครงงาน การใช้สมาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้

ผู้ดำเนินโครงงาน นางสาวจารุวรรณ งามสอาด รหัส 52371207

นายศรัณย์ ภู่นพคุณ รหัส 52371504

ที่ปรึกษาโครงงาน อาจารย์ภาณุพงศ์ สอนคม

สาขาวิชา วิศวกรรมคอมพิวเตอร์

ภาควิชา วิศวกรรมไฟฟ้าและคอมพิวเตอร์

ปีการศึกษา 2555

.....

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนเรศวร อนุมัติให้ปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์

.....ที่ปรึกษาโครงงาน
(อาจารย์ภาณุพงศ์ สอนคม)

.....กรรมการ
(ดร. วรลักษณ์ คงเด่นฟ้า)

.....กรรมการ
(ดร. พงศ์พันธ์ กิจสนาโยธิน)

.....กรรมการ
(อาจารย์เศรษฐา ตั้งค้าวานิช)

ชื่อหัวข้อโครงงาน	**การใช้สมาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้**	
ผู้ดำเนินโครงงาน	**นางสาวจารุวรรณ งามสอาด**	**รหัส 52371207**
	นายศรัณย์ ภู่นพคุณ	**รหัส 52371504**
ที่ปรึกษาโครงงาน	**อาจารย์ภาณุพงศ์ สอนคม**	
สาขาวิชา	**วิศวกรรมคอมพิวเตอร์**	
ภาควิชา	**วิศวกรรมไฟฟ้าและคอมพิวเตอร์**	
ปีการศึกษา	**2555**	

บทคัดย่อ

การใช้งานคอมพิวเตอร์สาธารณะหรือคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ (Untrusted Computer) อาจจะไม่ปลอดภัยเมื่อต้องใส่รหัสผ่านเพื่อยืนยันตัวตนบนเว็บไซต์ต่าง ๆ เพราะอาจมีโปรแกรมประเภท Key logger หรือ Trojan ทำการดักจับรหัสผ่านไว้ ผู้จัดทำจึงจัดทำโครงงานการใช้สมาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ขึ้น เพื่อป้องกันความเสียหายจากการถูกดักจับรหัสผ่าน

โดยการนำสมาร์ทโฟนมาเป็นตัวช่วยในการสร้างรหัสผ่านที่ใช้เพียงครั้งเดียวขึ้น ซึ่งผู้ใช้สามารถใส่รหัสผ่านที่ได้จากการสมัครใช้งานและตัวเลขสุ่มที่ได้จากเซิร์ฟเวอร์ลงในสมาร์ทโฟนที่เชื่อถือได้ จากนั้นแอพพลิเคชั่นบนสมาร์ทโฟนระบบแอนดรอยด์จะทำการนำข้อมูลที่ได้เข้ากระบวนการ Hash Function เพื่อสร้างรหัสผ่านที่ใช้เพียงครั้งเดียว เนื่องจากตัวเลขสุ่มที่ได้จากเซิร์ฟเวอร์จะเปลี่ยนไปทุก ๆ ครั้งที่ทำการรันโปรโตคอล

ผลที่ได้ คือ ระบบการยืนยันตัวตนมีความปลอดภัยสูงขึ้นกว่าระบบการยืนยันตัวตนที่ใช้โดยทั่วไป นอกจากนี้ทางผู้ให้บริการระบบสามารถประหยัดค่าใช้จ่ายได้เนื่องจากไม่จำเป็นต้องใช้การส่งข้อความทางโทรศัพท์มือถือเหมือนวิธีการแบบ Two-Step Verification และสามารถนำแอพพลิเคชั่นไปใช้ร่วมกับอุปกรณ์อัจฉริยะ (Smart Device) ประเภทอื่น ๆ ได้โดยไม่ยึดติดว่าจะต้องใช้กับสมาร์ทโฟนเพียงอย่างเดียวเท่านั้น

Project title	Authenticating Securely Via Untrusted Computer By Using Smartphone	
Name	Miss. Jaruwan Ngamsaard	ID. 52371207
	Mr. Saran Phunoppakhun	ID. 52371504
Project advisor	Mr. Panupong Sornkhom	
Major	Computer Engineering	
Department	Electrical and Computer Engineering	
Academic year	2555	

Abstract

Using a public computer or an untrusted computer may not be secure when we must log in with our password to identify ourselves on websites because they may have programs such as key logger or trojan to steal passwords. Therefore, We will do a project about using smart phones to identify ourselves on untrusted computers for protecting the web application against password theft.

We will use a smart phone to create a one time password so that users can enter the password which is recieved when they apply for and enter the random number from the server to the trusted smart phone. Then, the androind application on the smart phone will access the data to hash function the process to create a one time password, because the random number from the server will change everytime when the protocal runs.

The result is an authenticaltion system which is more secure than the current system normally used. Furthermore, service providers can save their costs because there is no need to send sms via mobile phone as a two-step verification method, and the application can be used with the other smart devices, not only with smart phones.

กิตติกรรมประกาศ

โครงงาน "การใช้สาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้" จะไม่สามารถสำเร็จได้ถ้าไม่ได้รับความช่วยเหลือจาก อาจารย์ภาณุพงศ์ สอนคม อาจารย์ที่ปรึกษาโครงงานนี้ ที่ให้ความกรุณาแนะนำวิธีในการทำงานให้เข้าใจถึงการศึกษาอย่างเป็นระบบขั้นตอน อีกทั้งสละเวลาเพื่อตรวจสอบการทำงานและชี้แนะแนวทางแก้ไขในทุกขั้นตอนตลอดการทำงานโครงงาน และสุดท้ายนี้ขอขอบพระคุณอาจารย์ทุกท่านและเพื่อนๆ ทุกคนที่ไม่ได้เอ่ยนามที่คอยให้ความช่วยเหลือและคำแนะนำต่างๆ จนได้โครงงานนี้สำเร็จได้ด้วยดี

คณะผู้ดำเนินโครงงานวิศวกรรม
นางสาวจารุวรรณ งามสอาด
นายศรัณย์ ภู่นพคุณ
มีนาคม 2555

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป(ต่อ)

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของโครงงาน

เว็บไซต์ในปัจบันมีการใช้งานในหลายรูปแบบ ทั้งเว็บไซต์ที่ใช้เพื่อหาความรู้ เว็บไซต์ที่ใช้เพื่อความบันเทิง เป็นต้น แต่อย่างไรก็ตามการเข้าใช้งานเว็บไซต์ต่าง ๆ จำเป็นต้องทำการล็อคอิน เพื่อเป็นการขอเข้าใช้งานเว็บไซต์

ในบางครั้งมีความจำเป็นที่จะต้องใช้งานบนคอมพิวเตอร์สาธารณะ หรือคอมพิวเตอร์ที่เชื่อถือไม่ได้ (Untrusted Computer) อาจเกิดความไม่ปลอดภัยในการใช้งานต่าง ๆ ได้ เพราะผู้ใช้ไม่สามารถรู้ได้ว่ามีภัยรูปแบบไหนอยู่บ้าง อาทิ เช่น การโดนดักจับ Password ในรูปแบบต่าง ๆ รวมถึงโปรแกรม Key Logger ที่อาจถูกติดตั้งอยู่ในเครื่องคอมพิวเตอร์ที่เชื่อถือไม่ได้ (untrusted computer) จึงทำให้กลุ่มผู้จัดทำมีแนวคิดในการทำระบบที่มีความปลอดภัยมากยิ่งขึ้นให้แก่ผู้ใช้

เนื่องจากแนวคิดการจัดทำโครงงานเกิดขึ้นเพื่อเพิ่มประสิทธิภาพการล็อคอิน ให้มีความปลอดภัยให้กับผู้ใช้งานมากยิ่งขึ้นกว่าระบบการล็อคอิน ที่มีอยู่ในปัจจุบัน และทางกลุ่มผู้จัดทำได้เล็งเห็นว่าปัจจุบันคนส่วนใหญ่มีโทรศัพท์มือถือสมาร์ทโฟนอยู่แล้ว จึงมีแนวคิดที่จะนำโทรศัพท์มือถือสมาร์ทโฟนมาใช้เพื่อมาเป็นตัวช่วยในการล็อคอิน เพื่อเพิ่มประสิทธิภาพความปลอดภัยให้กับผู้ใช้และระบบการล็อคอิน ให้มีมากยิ่งขึ้น

วัตถุประสงค์ของโครงงาน

1. เพื่อพัฒนาระบบการยืนยันตัวตนบนเว็บไซต์โดยใช้สมาร์ทโฟนแอนดรอยด์ เข้ามาช่วยในการยืนยันตัวตน เมื่อต้องใช้งานผ่านคอมพิวเตอร์สาธารณะ
2. เพื่อพัฒนาระบบล็อคอิน ให้มีความปลอดภัยกับผู้ใช้มากขึ้น เมื่อต้องเข้าใช้งานกับเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้

1.2 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถใช้สมาร์ทโฟนแอนดรอยด์ ยืนยันตัวตนบนเว็บไซต์ได้
2. สามารถล็อคอินผ่านคอมพิวเตอร์สาธารณะได้ปลอดภัยมากยิ่งขึ้น
3. การล็อคอินมีความปลอดภัยมากยิ่งขึ้นมากกว่าที่ใช้อยู่ในปัจจุบัน

1.3 ขอบเขตการทำโครงงาน

1. พัฒนาเว็บไซต์ต้นแบบสำหรับทดสอบระบบการยืนยันตัวตน
2. พัฒนาแอพพลิเคชั่นบนสมาร์ทโฟนในระบบแอนดรอยด์ที่สามารถรับรหัสผ่านจากผู้ใช้เพื่อไปคำนวณรหัสผ่านชั่วคราวสำหรับกาล็อคอินบนเว็บผ่านคอมพิวเตอร์สาธารณะได้

1.4 ขั้นตอนการดำเนินงาน

1. ศึกษาข้อมูลเกี่ยวกับหลักการและทฤษฎีต่างๆ
   1.1 ระบบการทำงานของล็อคอิน
   1.2 ขั้นตอนการเขียนและหลักการทำแอนดรอยด์ SDK
   1.3 ขั้นตอนการเขียน PHP และ My SQL
   1.4 ศึกษาการเข้ารหัสข้อมูลและการยืนยันตัวตน
2. ออกแบบและพัฒนาระบบ
3. ทดสอบระบบและแก้ไข
4. วิเคราะห์ข้อมูลและสรุปผลการทำงานทั้งหมด
5. จัดทำรูปเล่มรายงาน

1.5 แผนการดำเนินงาน

ตารางที่ 1.1 : ขั้นตอนการดำเนินงาน

กิจกรรม	ปี 2555							ปี 2556		
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1. เลือกหัวข้อโครงงานและอาจารย์ที่ปรึกษาโครงงาน	↔									
2. ศึกษาข้อมูลเกี่ยวกับหัวข้อโครงงาน	↔									
3. ศึกษาเรื่องการเข้ารหัส (Cryptography) และ เรื่อง การยืนยันตัวตน (Authentication)	↔	↔								
4. ศึกษาและรวบรวมข้อมูลเกี่ยวกับโปรแกรมแอนดรอยด์ SDK และ โปรแกรม PHP + My SQL	↔	↔								
5. ศึกษาการเขียนภาษา PHP และการเขียนแอพพลิเคชั่นแอนดรอยด์	↔	↔	↔							
6. ออกแบบหน้าเว็บไซต์ สำหรับล็อคอิน			↔	↔						
7. ออกแบบรูปแบบแอพพลิเคชั่น บนสมาร์ทโฟนแอนดรอยด์			↔	↔						
8. ทำการเขียน Code โปรแกรมในส่วนของเว็บล็อคอิน และแอพพลิเคชั่นแอนดรอยด์					↔	↔	↔			
9. ทดสอบโปรแกรมการทำงาน							↔	↔	↔	
10. แก้ไขข้อบกพร่องต่างๆที่เกิดจากการทดสอบโปรแกรม								↔	↔	

กิจกรรม	ปี 2555							ปี 2556		
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
11. จัดทำรูปแบบวิทยานิพนธ์	←	—	—	—	—	—	—	—	—	→
12. รวบรวมข้อมูลวิทยานิพนธ์ให้อาจารย์ที่ปรึกษาทำการตรวจสอบและพิจารณาแก้ไขข้อผิดพลาด								←	—	→
13. ตรวจสอบเล่มวิทยานิพนธ์อีกครั้งเพื่อความเป็นระเบียบ									←	→
14. จัดทำรูปเล่มวิทยานิพนธ์เล่มแดง										↔

1.6 รายละเอียดงบประมาณ

1. ค่าถ่ายเอกสาร 800 บาท
2. ค่าวัสดุอุปกรณ์ 500 บาท
3. ค่าเข้าเล่มวิทยานิพนธ์ 700 บาท

รวมเป็นเงิน 2,000 บาท **(สองพันบาทถ้วน)**

หมายเหตุ ถัวเฉลี่ยทุกรายการ

บทที่ 2
หลักการและทฤษฎีเบื้องต้น

2.1 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตนเป็นขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่จะบอกได้ว่าเป็นบุคคลที่กล่าวอ้างจริงหรือไม่ ซึ่งจะแบ่งได้ 2 ขั้นตอน คือ การระบุตัวตน (Identification) ซึ่งการการระบุตัวตนเป็นขั้นตอนที่ใช้ในการแสดงหลักฐานว่าผู้ใช้เป็นใคร เช่น ชื่อผู้ใช้ (Username) อีเมล์ (Email) เป็นต้น และการพิสูจน์ตัวตน (Authentication) เป็นขั้นตอนที่ใช้ตรวจสอบหลักฐานที่จะใช้บ่งบอกว่าเป็นบุคคลที่กล่าวอ้างจริง ซึ่งกลไกลการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้อีกเป็น 3 คุณลักษณะ คือ

1. สิ่งที่คุณมี (Possession factor) เช่น กุญแจ เครดิตการ์ด ชื่อผู้ใช้ เป็นต้น
2. สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (passwords) เบอร์โทรศัพท์ หรือใช้พิน (PINs) เป็นต้น
3. สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ เรตินาหรือม่านตา (retinal patterns) หรือรูปแบบเสียง (voice patterns) เป็นต้น

2.1.1 ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ประเภทของการพิสูจน์ตัวตนในปัจจุบันสามารแบ่งได้เป็น 9 วิธี ดังนี้

1. ไม่มีการพิสูจน์ตัวตน (No Authentication) ซึ่งใช้กับข้อมูลที่ไม่จำเป็นต้องมีการพิสูจน์ตัวตน เช่น ข้อมูลที่เป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนใช้บริการและสามารถเปลี่ยนแปลงได้ หรือข้อมูลข่าวสารหรือแหล่งข้อมูลนั้นสามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น
2. การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords) ซึ่งเป็นวิธีที่นิยมใช้กันอย่างแพร่หลายเป็นเวลานาน และรหัสผ่านควรถูกเก็บรักษาไว้เป็นความลับสำหรับผู้มีสิทธิ์เท่านั้น แต่ในปัจจุบันการใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความปลอดภัยของระบบคอมพิวเตอร์ ทั้งนี้อาจเกิดจากการตั้งรหัสผ่านที่ง่ายเกินไป และองค์ความรู้ต่าง ๆ ที่ก้าวหน้า จึงอาจถูกขโมยรหัสผ่านระหว่างการสื่อสารผ่านเครือข่ายได้
3. การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN) ซึ่ง PIN เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ และ PIN ถูกใช้กันอย่างแพร่หลายโดยเฉพาะการทำธุรกรรมต่าง ๆ เช่น ธุรกรรมทางด้านธนาคาร โดยการใช้บัตร ATM และเครดิตการ์ดต่างๆ และ PIN ช่วยให้การสื่อสารข้ามระบบเครือข่ายสาธารณะมีความปลอดภัยในมากขึ้น เพราะ PIN ถูกเข้ารหัสไว้และ

จำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

4. การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens (Authentication by Password Authenticators or Tokens) เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านที่สามารถเปลี่ยนแปลงได้ (dynamic password)" ในขณะที่กำลังเข้าสู่ระบบเครือข่าย สามารถแบ่งได้เป็น 2 วิธี คือ ซิงโครนัส และ อะซิงโครนัส ซึ่งการพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกได้เป็น 2 ประเภท ตามลักษณะของการใช้งาน คือ การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication) และการพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication) อีกวิธีนึงคือการพิสูจน์ตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่างหนึ่งว่า "challenge-response" ซึ่งถือว่าเป็นการป้องกันที่ปลอดภัยที่สุด

5. การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits) เป็นการนำอวัยวะส่วนต่าง ๆ ของร่างกายหรือลักษณะเฉพาะของบุคคลมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยในการยืนยันตัวตนเข้าสู่ระบบ เช่น การใช้การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคลร่วมกับการใช้รหัสผ่านในการยืนยันตัวตน เป็นต้น

6. การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP) ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาของการใช้รหัสผ่านอย่างเดียวซ้ำๆ ซึ่งการใช้ OTP จะทำให้ระบบมีความปลอดภัยเพิ่มมากขึ้น เพราะมีการเปลี่ยนรหัสผ่านทุกครั้งที่ผู้ใช้จะเข้าสู่ระบบ

7. การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography) เป็นการยืนยันตัวตนเพื่อรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายที่นิยมใช้ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจจะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าเป็นวิธีที่เหมาะสมที่สุดในการเข้ารหัส ซึ่งความเหมาะสมในการเข้ารหัสจะขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

8. การพิสูจน์ตัวตนโดยการใช้ลายเซ็นดิจิตอล (Digital Signature) เป็นการนำหลักการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ซึ่งสามารถแบ่งเป็นขั้นตอนได้ดังนี้

8.1 เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลจะที่ส่งถูกนำไปเข้าฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" แล้วจะได้เมสเซสไดเจสต์ (Message Digest) เป็นเอาต์พุตออกมา

8.2 การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล ซึ่งก็คือผู้ส่งได้ลงลายเซ็นดิจิตอล ที่จะยินยอมให้ผู้รับ ทำการตรวจสอบด้วยกุญแจสาธารณะของตัวผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

8.3 การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยนำข้อมูลไปผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นดิจิตอลด้วยกุญแจสาธารณะของผู้ส่ง ถ้าถอดได้ถูกต้อง จะสามารถยืนยันได้ว่าเป็นข้อมูลที่ส่งจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากับค่าเมสเซจไดเจสต์ที่คำนวณได้ในตอนแรก จะถือว่าข้อมูลนั้นเป็นข้อมูลที่ถูกต้อง

9. การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ (zero-knowledge proofs) เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม - ตอบ การพิสูจน์ตัวตนด้วยวิธีนี้ ซึ่งในการนำวิธีนี้มาใช้จำเป็นต้องใช้ความรู้ขั้นสูง เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ ซึ่งอาจเรียกระบบนี้ว่าเป็นการนำความรู้ด้าน AI (Artificial Intelligence) มาใช้ในการพิสูจน์ตัวตนนั่งเอง

2.1.2 Two – Factor Authentication

Two-Factor Authentication เป็นกระบวนการ "การแสดงตัวตน" โดยการใช้อุปกรณ์เสริมเพิ่มเติมซึ่งอาจอยู่ในรูปแบบ Hardware , บัตร ATM , RAS Token , Access Caerd , และ Swipe card เป็นต้น

การตรวจสอบผู้ใช้ระบบโดยใช้ Smart card เข้ามาช่วยในการตรวจสอบตัวตนของผู้ใช้งานระบบจะมีส่วนคล้ายคลึงกับระบบบัตร ATM ของธนาคาร ว่าเป็นของผู้ใช้คนนั้นหรือไม่ เพราะด้วยบัตร ATM จะมีผู้ใช้เพียงคนเดียวเท่านั้นและเป็นผู้ใช้คนเดียวที่จะสามารถล่วงรู้รหัสของตนเองได้ ถึงแม้บัตรสูญหายไปแล้วผู้อื่นก็ไม่สามารถล่วงรู้รหัสที่อยู่ในบัตรได้ จึงทำให้ยากต่อการเจาะเข้าสู่ระบบอีกขั้นหนึ่งได้

การใช้งาน Smart card นั้นต้องมีการใช้งานร่วมกับระบบ PKI หรือ "Public-key Infrastructures" ซึ่งผู้ใช้แต่ละคนจะได้รับ "Digital Certificate" ที่ได้รับรองจาก CA หรือ Certificate Authority เพื่อนำไปแสดงว่าผู้ใช้มีตัวตนจริง ทั้งนี้ใน Smart card จะเก็บ "Private key" ของผู้ใช้ไว้ และยังมีการเข้ารหัสเพื่อป้องกันไม่ให้แฮกเกอร์สามารถนำ Private key ไปใช้งานได้ง่ายๆ ระบบ Smart card ยังเหมาะที่ใช้เก็บ Private key เพื่อไม่ให้ผู้ไม่ประสงค์ดีเข้ามาถึงข้อมูลใน Smart card ได้ เพราะระบบมีการป้องกันหลายชั้นที่ค่อนข้างซับซ้อนหลายประการพอสมควร

2.2 การเข้ารหัสลับ (Cryptography)

การเข้ารหัสลับ (Cryptography) คือ การเข้ารหัสลับเป็นวิธีการเพิ่มความปลอดภัยให้ข้อมูล โดยทำการแปลงเนื้อหาเพื่อให้เฉพาะบุคคลที่มีคีย์การเข้ารหัสลับหรือบุคคลที่ได้รับอนุญาตที่จะสามารถเข้าใจข้อมูลได้

2.2.1 จุดประสงค์หลักของระบบการเข้ารหัสลับ

1. ทำให้ข้อมูลเป็นความลับ (Cryptography) เพื่อป้องกันให้ผู้ที่ไม่เกี่ยวข้อง ไม่มีสิทธิในการเข้าถึงข้อมูล

2. ทำให้สามารถตรวจสอบความสมบูรณ์ของข้อมูลได้ เพื่อป้องกันข้อมูลให้อยู่ในสภาพสมบูรณ์อย่างเดิม กล่าวคือ ในกระบวนการการสื่อสาร เมื่อผู้รับสารได้รับข้อมูลตามที่ผู้ส่ง ส่งมา ข้อมูลที่ถูกต้องดังกล่าวจะต้องไม่มีการสูญหายหรือถูกเปลี่ยนแปลงแก้ไขใดๆ

3. สามารถยืนยันตัวตนของผู้ส่งข้อมูลได้(Authentication) เพื่อให้สามารถตรวจสอบได้ว่าบุคคลใดเป็นผู้ส่งข้อมูลนั้นๆ เพื่อป้องกันการแอบอ้างจากบุคคลอื่น

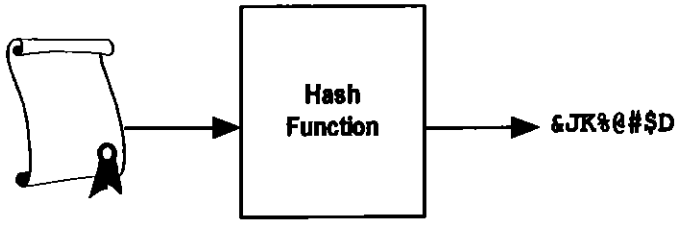
2.2.2 ระบบการเข้ารหัสข้อมูล

ระบบเข้ารหัสโดยพื้นฐานแล้วจะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความที่ต้องการส่งไปถึงผู้รับ ข้อมูลจะถูกเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้ ซึ่งในโครงงานนี้จะพูดถึงรูปแบบของการเข้ารหัสแบบแฮช (Hash)

2.2.3 รูปแบบของระบบเข้ารหัส

2.2.3.1 แฮช (Hash)

แฮช (Hash) เป็นความรู้พื้นฐานที่ใช้ในการสร้างลายเซ็นดิจิตอล แฮช(Hash) ในทางคอมพิวเตอร์นั้นหมายถึง การนำเอาตัวเลขหรือข้อความมาผ่านกระบวนการหรือวิธีการอย่างใดอย่างหนึ่ง แล้วได้ผลลัพธ์ออกมาเป็นตัวเลขชุด



รูปที่ 2.1 : แสดงการทำงานของแฮช

กรรมวิธีการแฮชที่ว่านี้โดยส่วนใหญ่จะเป็นฟังก์ชันทางคณิตศาสตร์ โดยฟังก์ชันแฮชที่ดี จะต้องมีคุณสมบัติการกระจายที่ดี คือ ข้อความเดียวกันเมื่อผ่านแฮชฟังก์ชันแล้ว จะต้องได้ผลลัพธ์เหมือนเดิมเสมอ และข้อความที่ต่างกันเพียงเล็กน้อยผ่านแฮชฟังก์ชัน ควรจะต้องได้ผลลัพธ์

ที่ต่างกันมาก ที่สำคัญก็คือ ไม่ควรมีข้อความใด ๆ ตั้งแต่ 2 ข้อความขึ้นไป ที่ผ่านแฮชฟังก์ชันแล้ว จะได้ผลลัพธ์ที่เหมือนกัน

2.2.3.2 ฟังก์ชันแฮชที่ดีควรมีคุณสมบัติดังต่อไปนี้

1. ฟังก์ชันแฮชควรจะสามารถใช้งานกับข้อมูลที่มีความยาวเท่าไรก็ได้
2. ฟังก์ชันแฮชจะต้องสามารถสร้างผลลัพธ์ที่มีความยาวเท่ากันหมด
3. ฟังก์ชันแฮชควรเป็นฟังก์ชันที่ไม่ซับซ้อน สามารถสร้างโดยฮาร์ดแวร์และซอฟต์แวร์ได้ง่าย
4. ฟังก์ชันแฮชไม่ควรเป็นฟังก์ชันที่ย้อนกลับได้หรือเป็นการเข้ารหัสทางเดียว คือ เมื่อทราบผลลัพธ์แล้วไม่มีทางทราบข้อมูลเลย

ในโลกผู้ค้นคิดฟังก์ชันแฮชมากมาย แต่ฟังก์ชันแฮชที่ใช้ในการทำลายเซ็นดิจิตอล ซึ่งเป็นที่ยอมรับว่าเป็นมาตรฐานนั้น มีอยู่ 2 ฟังก์ชัน ฟังก์ชันแรกมีชื่อว่า SHA โดย SHA ได้รับการพัฒนาโดย NIST (National Institute of Standard and Technology) ซึ่งเป็นหน่วยงานที่ทำหน้าที่กำหนดมาตรฐานทางเทคโนโลยีของสหรัฐอเมริกา โดยได้รับการประกาศเป็นมาตรฐานที่ FIPS PUB 180 ในปี 1993 โดยหลังจากนั้นมีการปรับปรุงเป็น SHA-1 ในปี 1995 โดยประกาศเป็นมาตรฐานที่ FIPS PUB 180-1

2.2.4 SHA-1

SHA-1 เป็นอัลกอริทึม Hash คำว่า SHA ก็มาจากคำเต็มตรงตัวว่า Secure Hash Algorithm ออกแบบโดย NSA (National Security Agency) หรือสำนักงานความมั่นคงแห่งชาติของสหรัฐ SHA-1 ถูกใช้ในเข้ารหัสข้อมูลหรือลายเซ็นดิจิตอล นอกจากนี้ SHA-1 ยังเป็นฟังชันแฮชทางเดียวอีกด้วย

2.2.4.1 ฟังก์ชันแฮชทางเดียว

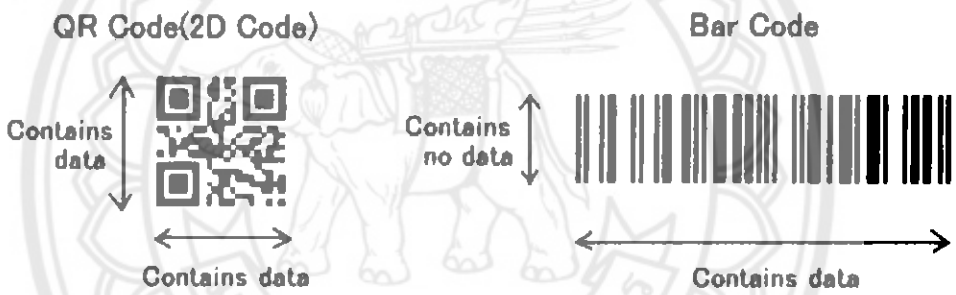
ฟังก์ชันทางเดียว (One-way Function) คือฟังก์ชันใดๆ ที่ง่ายในการคำนวณหาคำตอบไปในทิศทางเดียว แต่จะมีความยากมากๆ ในการคำนวณหาคำตอบในย้อนกลับ ซึ่งต้องใช้เวลานานและทรัพยากรจำนวนมากในการคำนวณหาคำตอบ จากลักษณะของฟังก์ชันทางเดียวที่กล่าวมาข้างต้น จึงได้มีการนำเอาแนวคิดของฟังก์ชันทางเดียวมาประยุกต์ใช้ในระบบการเข้ารหัสลับกุญแจสาธารณะ คือ ถ้ากำหนดกุญแจสาธารณะมาให้ จะสามารถทำการเข้ารหัสลับข้อความต้นฉบับได้อย่างง่ายดาย แต่ถ้ามีการกำหนดข้อความมาให้เป็นรหัส จะยากมากๆ ที่จะคำนวณหาข้อความต้นฉบับหรือกุญแจส่วนตัวเพื่อใช้ในการถอดรหัสลับ เช่น SHA-1 MD5 เป็นต้น

2.3 คิวอาร์โค้ด (QR Code : Quick Response Code)

คิวอาร์โค้ด เป็นรหัสที่ถูกพัฒนาขึ้นโดยบริษัท Denso – Wave ซึ่งเกิดจากแนวคิด "Code read easily for reader" ซึ่งเป็นการแปลงรหัสโค้ดให้อยู่ในรูปของข้อมูลได้อย่างรวดเร็ว ซึ่งคิวอาร์โค้ดเป็นบาร์โค้ด 2 มิติ ซึ่งมีประสิทธิภาพในการเก็บข้อมูลและใช้งานมากกว่าบาร์โค้ด 1 มิติ นอกจากนี้ยังสามารถใช้ได้กับการเก็บข้อมูลหลากหลายรูปแบบ อาธิ เช่น การนำคิวอาร์โค้ดไปใช้ในการเก็บข้อมูลสินค้า หรือการดาวน์โหลดไฟล์ต่าง ๆ เป็นต้น

2.3.1 การเปรียบเทียบการทำงานของบาร์โค้ด 1 มิติและ 2 มิติ

การทำงานของบาร์โค้ด 1 มิติ ต่างจาก บาร์โค้ด 2 มิติ ในลักษณะของการเก็บข้อมูล คือ บาร์โค้ด 1 มิติ จะมีการเก็บข้อมูลในแนวนอนเท่านั้น แต่บาร์โค้ด 2 มิติ สามารถเก็บข้อมูลได้ทั้งแนวตั้งและแนวนอน จึงทำให้สามารถเก็บข้อมูลที่มีปริมาณมากกว่าบาร์โค้ด 1 มิติ ดังรูปที่ 2.2



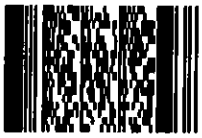
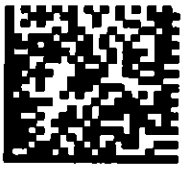
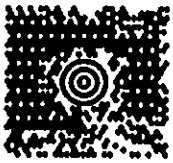
รูปที่ 2.2 : การเปรียบเทียบลักษณะบาร์โค้ดแบบ 2 มิติ และ 1 มิติ

ที่มา : http://www.denso-wave.com/qrcode/aboutar-e.html

บาร์โค้ด 1 มิติ มีลักษณะเป็นเส้นสีขาวสลับดำ ใช้แทนรหัสอักษรหรือตัวเลข ซึ่งปริมาณตัวอักษรที่สามารถเก็บได้คือ 20 ตัวอักษร และในการแปลงข้อมูลกลับจำเป็นต้องใช้อุปกรณ์เฉพาะหรือเครื่องมืออ่านบาร์โค้ด เช่น ซุปเปอร์มาร์เก็ต ร้านสะดวกซื้อ หรือ เคาเตอร์ให้บริการชำระเงินต่างๆ เป็นต้น

นอกจากนี้ยังมีการนำบาร์โค้ด 1 มิติ มาพัฒนาต่อยอดเป็นบาร์โค้ดแบบ 2 มิติ โดยมีการพัฒนาให้สามารถเก็บข้อมูลได้ทั้งแนวตั้งและแนวนอน จึงสามารถบรรจุข้อมูลได้มากกว่าบาร์โค้ด 1 มิติ ที่สามารถเก็บข้อมูลได้เพียงแนวนอนอย่างเดียวเท่านั้น ประมาณ 200 เท่า หรือ ประมาณ 4,000 ตัวอักษร และมีขนาดเล็กลงกว่าเดิม นอกจากนี้บาร์โค้ดแบบ 2 มิติ ยังมีการทำงานได้หลายภาษา เนื่องจากมีผู้พัฒนาจากหลายๆ ประเทศ ดังตารางที่ 2.3

ตารางที่ 2.1 : แสดงการเปรียบเทียบบาร์โค้ดแบบ 2 มิติ

หัวข้อ		ประเภทของบาร์โค้ดแบบ 2 มิติ			
		QR Code	PDF417	Data Matrix	Maxi Code
รูปแบบของบาร์โค้ด					
ประเทศผู้พัฒนา		DENSO (ญี่ปุ่น)	Symbol Technologies (สหรัฐอเมริกา)	RVSI Acuity CiMatrix (สหรัฐอเมริกา)	UPS (สหรัฐอเมริกา)
ประเภทของบาร์โค้ด		Matrix	Stacked Bar Code	Matrix	Matrix
ข้อมูลที่บรรจุ (ตัวอักษร)	ตัวเลข	7,089	2,710	3,116	138
	ตัวอักษร	4,296	1,850	2,355	93
	ตัวเลขฐานสอง	2,953	1,018	1,556	-
	ตัวคันจิ (อักษีญี่ปุ่น)	1,817	554	778	-
ลักษณะเด่น		* เก็บข้อมูลได้ปริมาณมาก * มีขนาดเล็ก * มีความเร็วในการอ่านสูง	* เก็บข้อมูลได้ในปริมาณที่มาก	* มีขนาดเล็ก	* มีความเร็วในการอ่านสูง
รองรับมาตรฐาน		* AIM * International * JIS * ISO	* AIM * ISO * International	* AIM * ISO * International	* AIM * ISO * International

ที่มา : http://www.bu.ac.th/knowledgecenter/executive_journal/oct_dec_10/pdf/aw5.pdf

ที่มา : http://www.denso-wave.com/qrcode/aboutar-e.html

2.3.2 รูปแบบของบาร์โค้ดแบบ 2 มิติ

บาร์โค้ด 2 มิติ สามารถแบ่งได้เป็น 2 ประเภท ดังนี้

2.3.2.1 บาร์โค้ดแบบสแต็ก (Stacked Barcode)

บาร์โค้ดแบบสแต็กมีลักษณะคล้ายกับการนำบาร์โค้ดแบบ 1 มิติ มาวางซ้อนกันหลายๆแถว มีการทำงานโดยอ่านภาพถ่ายบาร์โค้ดแล้วปรับความกว้างของบาร์โค้ดก่อนทำการถอดรหัส ซึ่งการปรับความกว้างนี้ทำให้สามารถถอดรหัสจากภาพที่เสียหายบางส่วนได้ โดยส่วนที่เสียหายนั้นจะต้องไม่เสียหายเกินขีดจำกัดหนึ่งที่กำหนดไว้ การอ่านบาร์โค้ดแบบสแต็กสามารถอ่านได้ทิศทางเดียว เช่น อ่านจากซ้ายไปขวา หรือ ขวาไปซ้าย และ อ่านจากบนลงล่างหรือจากล่างขึ้นบน เป็นต้น ตัวอย่างบาร์โค้ดแบบสแต็ก เช่น

1. บาร์โค้ด PDF417 (Portable Data File) เป็นบาร์โค้ดแบบ 2 มิติ ถูกพัฒนาขึ้นในปี 2535 โดยบริษัท Symbol Technologies ประเทศสหรัฐอเมริกาบาร์โค้ดแบบ PDF417 มีความสอดคล้องกับมาตรฐาน ISO/IEC 15438 และ AIM USS-PDF417 ลักษณะของบาร์โค้ดเป็นรูปสี่เหลี่ยมผืนผ้า มีส่วนแทนรหัสข้อมูลหรือที่เรียกว่าโมดูลข้อมูล (Data Module) เป็นแถบสีดำและสีขาวเรียงกันหลายๆ แถว แถวแนวตั้งและแนวนอน (ดังรูปที่ 2.3) ประกอบไปด้วย 3 ถึง 90 แถว และ 1 ถึง 30 คอลัมน์ ซึ่งสามารถบรรจุข้อมูลได้มากถึง 2,710 ตัวเลข 1,850 ตัวอักษร 1,018 ไบนารี หรือคันจิ 554 ตัวอักษร "คำว่า PDF ย่อมาจาก Portable Data File ประกอบไปด้วย 4 แถบ และ 4 ช่องว่างใน 17 โมดุล จึงทำให้ได้หมายเลข 417"

รูปที่ 2.3 : แสดงบาร์โค้ด 2 มิติแบบ PDF417

2.3.2.2 บาร์โค้ดแบบเมตริกซ์ (Matrix Barcode)

บาร์โค้ดแบบเมตริกซ์มีลักษณะหลากหลายและมีความเป็นสองมิติมากกว่าบาร์โค้ดแบบสเต็ก ลักษณะสำคัญของบาร์โค้ดแบบเมตริกซ์ คือ มีรูปแบบค้นหา (Finder Pattern) ทำหน้าที่เป็นตัวอ้างอิงตำแหน่งในการอ่านและถอดรหัสข้อมูล ช่วยให้อ่านข้อมูลได้รวดเร็วและสามารถอ่านบาร์โค้ดได้แม้บาร์โค้ดเอียง หมุน หรือ กลับหัว ตัวอย่างบาร์โค้ดแบบเมตริกซ์ เช่น

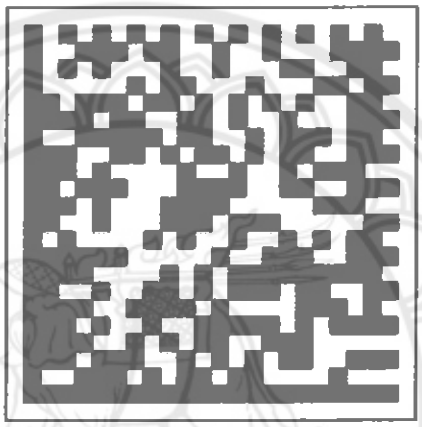
1. บาร์โค้ดแบบ QR Code (Quick Response Code)

QR Code เป็นบาร์โค้ดแบบ 2 มิติ แบบเมตริกซ์ที่ถูกพัฒนาขึ้นโดยบริษัท Nippon Denso ประเทศญี่ปุ่นในปี 2537 มีความสอดคล้องกับมาตรฐาน ISO/IEC 18004 , JIS X 0510 , JEIDA-55 และ AIM ITS/97/001 ISS-QR Code ลักษณะของบาร์ดค้ดเป็นรูปสี่เหลี่ยมจัตุรัส มีโมดูล 21x21 ถึง 177 x 177 โมดูล สามารถบรรจุข้อมูลได้ถึง 7,089 ตัวเลขหรือ 4,296 ตัวอักษร ข้อมูลเลขฐานสอง 2,953 ไบต์ มีตัวอักษรญี่ปุ่น 1,817 ตัวอักษร รูปแบบการทำงานของ QR Code อยู่ที่มุมทั้งสามของบาร์โค้ด คือ มุมซ้ายล่าง และ มุมขวาบน ดังรูปที่ 2.4

รูปที่ 2.4 : แสดงบาร์โค้ด 2 มิติแบบ QR Code

ที่มา : http://www.qrstuff.com/images/sample.png

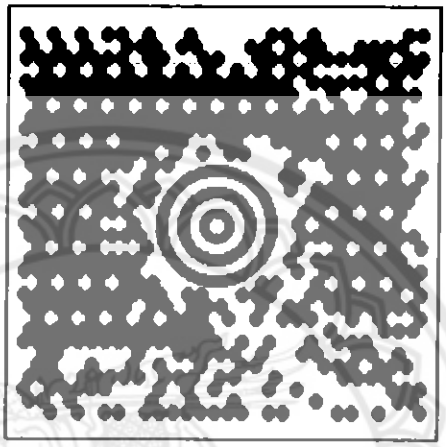
2. บาร์โค้ดแบบ Data Matrix ถูกพัฒนาโดยบริษัท RVSI Acuity CiMatrix ประเทศสหรัฐอเมริกา มีความสอดคล้องกับมาตรฐาน ISO/IEC 16022 และ ANSI/AIM BC-11-ISS-Data Matrix มีลักษณะบาร์โค้ดรูปสี่เหลี่ยมจตุรัสและสี่เหลี่ยมผืนผ้าสำหรับบาร์โค้ดสี่เหลี่ยมจัตรัสมีโมดูล 10 x 10 ถึง 144 x 144 รูปสี่เหลี่ยมผืนผ้ามี 8 x 8 ถึง 16 x 48 โมดูล Data Matrix สมารถบรรจุข้อมูลได้มากถึง 3,116 ตัวเลข หรือ 2,355 ตัวอักษร ข้อมูลประเภทอื่นได้แก่ เลขฐานสองบรรจุได้ 1,556 ไบต์ และตัวอักษรภาษาญี่ปุ่นบรรจุได้ 778 ตัวอักษร รูปแบบของบาร์โค้ด Data Matrix อยู่ที่ตำแหน่งขอบซ้ายและด้านล่างของบาร์โค้ดตามรูปที่ 2.4 บาร์โค้ด Data Matrix ส่วนใหญ่ใช้งานที่มีพื้นที่จำกัดและต้องการบาร์โค้ดที่มีขนาดเล็กลง



รูปที่ 2.5 : แสดงบาร์โค้ด 2 มิติแบบ Data Matrix

ที่มา : http://upload.wikimedia.org/wikipedia/commons/thumb/e/e8/Datamatrix.svg/220px-Datamatrix.svg.png

3. บาร์โค้ดแบบ MaxiCode เป็นบาร์โค้ดแบบ 2 มิติ พัฒนาโดยบริษัท Oniplanar นำไปใช้โดยบริษัทขนส่ง UPS (United Parcel Service) ประเทศสหรัฐอเมริกาในปี 2530 Maxi สอดคล้องกับมาตรฐาน ISO/IES 16023 และ ANSI/AIM BC10-ISS-MaxiCode ลักษณะบาร์โค้ดเป็นรูปสี่เหลี่ยมขนาด 1.11 x 1.054 นิ้ว แทนรหัสข้อมูลมีลักษณะเป็นรูปหกเหลี่ยมทั้งหมด 866 โมดูล เรียงตัวกันใน 33 แถวรอบรูปแบบค้นหา ซึ่งการค้นหาของ MaxiCode มีลักษณะเป็นวงกลมซ้อนกันสามวงอยู่กลางบาร์โค้ดดังรูปที่ 2.5



รูปที่ 2.6 : แสดงบาร์โค้ด 2 มิติแบบ MaxiCode

ที่มา : http://www.registrodedatos.com/UserFiles/Image/Maxicode_IVAN_250.jpg

2.4 ฐานข้อมูล (Database)

ฐานข้อมูล (Database) เป็นกลุ่มของข้อมูลที่มีความสัมพันธ์กัน และนำมาเก็บรวมไว้ด้วยกันอย่างเป็นระบบและข้อมูลที่นำมาเก็บรวมกันไว้เป็นฐานข้อมูล ต้องตรงตามวัตถุประสงค์การใช้งานขององค์กรหรือบุคคล เช่น สำนักงานก็รวบรวมข้อมูลต่าง ๆ ตั้งแต่หมายเลขโทรศัพท์ของพนักงานจนถึงเอกสารทุกอย่างของสำนักงานนั้น ๆ ซึ่งข้อมูลส่วนนี้จะมีส่วนที่สัมพันธ์กันและสะดวกต่อการเรียกข้อมูลเหล่านี้ออกมาใช้ในภายหลัง ข้อมูลอาจเกี่ยวกับบุคคล สิ่งของ สถานที่ หรือเหตุการณ์ ที่เราสนใจก็ได้ และจากการเก็บข้อมูลจะเก็บข้อมูลที่มีความสัมพันธ์กันอย่างเป็นระบบจึงทำให้ไม่เกิดความซับซ้อนของข้อมูล ซึ่งช่วยให้ข้อมูลมีความถูกต้อง และเป็นมาตรฐานเดียวกัน

2.4.1 ประโยชน์ของระบบฐานข้อมูล

ฐานข้อมูลเป็นการจัดเก็บข้อมูลอย่างเป็นระบบ จึงช่วยให้การจัดเก็บข้อมูลขององค์กรเป็นระเบียบ และจะมีการแยกตามแต่ละประเภท ทำให้มูลประเภทเดียวกันจัดเก็บไว้ด้วยกันเป็นหมวดหมู่ ง่ายต่อการค้นหาและนำข้อมูลไปใช้งานในด้านต่างๆ ซึ่งจะขึ้นอยู่กับการนำข้อมูลไปใช้ประโยชน์ของแต่ละหน่วยงาน

2.4.2 ประโยชน์ของฐานข้อมูลเชิงสัมพันธ์

1. ลดความซ้ำซ้อนของข้อมูล
2. ใช้ข้อมูลร่วมกันและได้รับข้อมูลตรงกัน เนื่องจากข้อมูลนำมาจากแหล่งเดียวกัน
3. ง่ายต่อการเปลี่ยนแปลงแก้ไขข้อมูล
4. กำหนดสิทธิ์ในการเข้าถึงข้อมูลได้

2.4.3 โครงสร้างฐานข้อมูล

1. อักขระ (Character) คือ เครื่องหมายหรือสัญลักษณ์ ตัวอักษร และตัวเลข
2. เขตข้อมูล (Field) คือ อักษรที่มากกว่า 1 ตัว ที่เป็นรายละเอียดของสิ่งใดสิ่งหนึ่ง เช่น ชื่อ ที่อยู่ อายุ เพศ เป็นต้น
3. ระเบียน (Record) คือ ระเบียน หรือ รายการข้อมูล
4. ตาราง (Table) คือ ตารางหรือแฟ้มข้อมูลที่ประกอบด้วยระเบียนต่างๆ
5. ฐานข้อมูล (Database) คือ ฐานข้อมูลประกอบไปด้วยตารางและแฟ้มข้อมูลที่เกี่ยวข้อง

2.4.4 องค์ประกอบของฐานข้อมูล

ระบบฐานข้อมูลโดยส่วนใหญ่เป็นระบบที่มีการนำเอาคอมพิวเตอร์มาช่วยในการจัดเก็บ ค้นหา และประมวลผลข้อมูล เพื่อให้ได้สารสนเทศที่ต้องการเพื่อที่จะนำไปใช้ในการปฏิบัติงาน และบริหารงานของผู้บริหาร โดยอาศัยโปรแกรมเข้ามาช่วยในการจัดการข้อมูล

ระบบฐานข้อมูลมีกระบวนการ 5 ประเภท คือ

1. ฮาร์ดแวร์ (Hardware) คือ อุปกรณ์ต่างๆ ที่นำมาใช้ในการอำนวยความสะดวกในการบริหารงานฐานข้อมูลอย่างมีประสิทธิภาพ

2. โปรแกรม (Program หรือ Software) มีหน้าที่ควบคุมดูแลการสร้างฐานข้อมูล การเรียกใช้ และการจัดทำรายงาน เรียกว่า โปรแกรมระบบจัดการฐานข้อมูล (Database Management System : DBMS)

3. ข้อมูล (Data) คือ สารสนเทศที่นำมาเก็บรวบรวมไว้

4. บุคลากร (People ware) หมายถึง ผู้ใช้งาน (User) พนักงานปฏิบัติการ (Operator) นักวิเคราะห์และออกแบบระบบ (System Analyst) ผู้เขียนโปรแกรมประยุกต์ใช้งาน (Programmer) และผู้บริหารฐานข้อมูล (Database Administrator : DBA)

5. ขั้นตอนการปฏิบัติงาน (Procedure) คือ ขั้นตอนวิธีและวิธีการต่างๆ ในการปฏิบัติการ เพื่อให้สามารถทำงานได้อย่างถูกต้องเป็นขั้นตอนที่กำหนดไว้

2.4.5 ความสัมพันธ์ระหว่างแฟ้มข้อมูล

1. ความสัมพันธ์แบบหนึ่งต่อหนึ่ง (One-to-one Relationships) เป็นการแสดงความสัมพันธ์ของข้อมูลในแฟ้มข้อมูลหนึ่งที่มีความสัมพันธ์กับข้อมูลในอีกแฟ้มข้อมูลหนึ่ง ในลักษณะหนึ่งต่อหนึ่ง (1 : 1)

2. ความสัมพันธ์แบบหนึ่งต่อกลุ่ม (One-to-many Relationships) เป็น การแสดงความสัมพันธ์ของข้อมูลในแฟ้มข้อมูลหนึ่ง ที่มีความสัมพันธ์กับข้อมูลหลาย ๆ ข้อมูลในอีกแฟ้มข้อมูลหนึ่ง ในลักษณะ (1 : m) ตัวอย่างเช่น

3. ความสัมพันธ์แบบกลุ่มต่อกลุ่ม (Many-to-many Relationships) เป็นการแสดงความสัมพันธ์ของข้อมูลสองแฟ้มข้อมูลในลักษณะกลุ่มต่อกลุ่ม (m : n)

2.4.6 คำศัพท์พื้นฐานในระบบฐานข้อมูล

คำศัพท์เฉพาะที่ควรรู้และทำความเข้าใจให้ชัดเจนก่อนที่จะนำไปใช้ในการออกแบบฐานข้อมูล มีดังต่อไปนี้

1. เอนทิตี้ (Entity) หมายถึง ชื่อของกลุ่มข้อมูลที่จะนำมาเก็บในฐานข้อมูล เช่น คน สัตว์ ความชำนาญ

2. แอตทริบิวต์ (Attribute) หมายถึง สิ่งที่ใช้แสดงลักษณะ คุณสมบัติ และบอกข้อมูลของเอนทิตี้ เช่น เพศ อายุ น้ำหนัก ส่วนสูง เป็นต้น

3. รีเลชั่น (Relation) หมายถึง ตารางข้อมูล (Table) ซึ่งใช้เรียกแทนข้อมูลเรื่องใดเรื่องหนึ่งในระบบฐานข้อมูล

4. ความสัมพันธ์ (Relationship) หมายถึง สิ่งที่แสดงถึงความสัมพันธ์ระหว่าง Entity ซึ่งมีระดับความสัมพันธ์ 3 ระดับ

4.1 ความสัมพันธ์แบบ One – to – One (1 : 1)

4.2 ความสัมพันธ์แบบ One – to – Many (1 : n)

4.3 ความสัมพันธ์แบบ Many – to – Many (m : n)

5. ทูเพิล (Tuple) หมายถึง แถว (Row) ข้อมูลในตาราง (Table) โดยในแต่ละแถวของข้อมูลจะประกอบด้วยหลาย Attribute ซึ่งทูเพิล (Tuple) ใช้เรียกแทนแต่ละแถว (Row) ของ Relation

6. คาร์ดินาลลิตี้ (Cardinality) คือ จะนวนแถวของข้อมูลในแต่ละ Relation

7. คีย์หลัก (Primary key) คือ แอตทริบิวต์ที่มีค่าที่เป็นเอกลักษณ์ ไม่สามารถจะมีข้อมูลซ้ำกันได้

8. คีย์นอก (Foreign key) คือ แอตทริบิวต์ที่ใช้เชื่อมความสัมพันธ์ระหว่าง Table ที่มีความสัมพันธ์เกี่ยวข้องกัน

9. โดเมน (Domain) คือ ขอบเขตค่าของข้อมูลในฐานข้อมูล

2.5 เครื่องมือที่ใช้ในการพัฒนาเว็บไซต์

2.5.1 ภาษา HTML

HTML ย่อมาจาก Hyper Text Makeup Language เป็นภาษาคอมพิวเตอร์รูปแบบหนึ่งโดยเป็นภาษาพื้นฐานในการเขียนเว็บเพจ ภาษา HTML เป็นภาษาที่มีลักษณะของข้อมูลที่เป็นตัวอักษรในมาตรฐานของรหัสแอสกี (ASCII Code) โดยเขียนอยู่ในรูปของเอกสารข้อความ (Text Document) จึงกำหนดรูปแบบและโครงสร้างได้ง่าย ภาษา HTML ได้ถูกพัฒนาขึ้นอย่างต่อเนื่องตั้งแต่ HTML Level 1 (รุ่นดั้งเดิม) , HTML 2.0 , HTML 3.0 , HTML 3.2 , และ HTML 4.0 วึ่งเป็นรุ่นที่นิยมเขียนกันในปัจจุบัน (ขณะนี้ W3C ได้พัฒนา HTML 4.01 ออกมาแล้ว เพื่อรองรับมาตรฐาน ภาษา XML) จึงทำให้ภาษา HTML ในปัจจุบันสามารถแสดงผลกราฟฟิคและระบบเสียงได้เพื่อตอบสนองในการทำงานในปัจจุบัน

2.5.2 ภาษา SQL

SQL ย่อมาจาก Structured Query Language เป็นภาษาทางด้านฐานข้อมูล ที่สามารถสร้างและปฏิบัติการกับฐานข้อมูลแบบสัมพันธ์ (Relational database) โดยเฉพาะ ภาษา SQL ถูกพัฒนาขึ้นจากแนวคิดของ Relational calculus และ Relational algebra เป็นหลัก เริ่มพัฒนาครั้งแรกโดย Almaden Research Center ของบริษัทไอบีเอ็มโดยมีชื่อเริ่มแรกว่า "ซีเควล" (Sequel) ซึ่งต่อมาได้เป็นเป็นชื่อ "เอสคิวแอล" (SQL) หลังจากนั้นได้ถูกนำมาพัฒนาโดยผู้ผลิตซอฟแวร์ด้านระบบจัดการฐานข้อมูลเชิงสัมพันธ์จนเป็นที่นิยมกันอย่างมากในปัจจุบัน โดยที่ผู้ผลิตแต่ละรายก็พยายามที่จะพัฒนาระบบจัดการฐานข้อมูลของตนให้มีลักษณะเด่นเฉพาะขึ้นมา ทำให้รูปแบบการใช้คำสั่ง SQL มีรูปแบบที่แตกต่างกันออกไป ในปี ค.ศ. 1986

2.5.3 ภาษา PHP

PHP ย่อมาจาก Hypertext Preprocessor หรือ Personal Home Page ถูกคิดค้นขึ้นในปี ค.ศ. 1994 โดย Rasmus Lerdorf เพื่อใช้ตรวจสอบสถิติการเข้าชมเว็บของตนเอง ต่อมาได้พัฒนาให้มีประสิทธิภาพและเปลี่ยนเป็นชื่อเป็น Professional Home Page โดยเป็นภาษาคอมพิวเตอร์ประเภท Open Source ที่ใช้กันอย่างแพร่หลาย ซึ่งใช้ในการจัดทำเว็บไซร์และสามารถประมวลผลออกมาในรูปแบบ HTML โดยทีโครงสร้างคำสั่งมาจากภาษา C , Java และ Perl

PHP ได้พัฒนาและออกแบบมาเพื่อใช้ในการสร้างเอกสาร HTML โดยสามารถแทรกคำสั่ง PHP ได้ตามที่ต้องการลงในเอกสาร HTML ดังนั้น PHP จึงเป็นภาษาที่เรียกว่า Sever Side หรือ HTML Embedded Scripting Language เป็นภาษาที่สำคัญ ที่ช่วยให้สามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพ ซึ่งภาษา PHP ง่ายต่อการเรียนรู้และเป็น Database Enabled Web Page ทำให้เอกสารของ HTML สามารถมที่จะเชื่อมต่อกับระบบฐานข้อมูล (Database) ได้อย่างมีประสิทธิภาพจึงทำให้ PHP เป็นภาษาที่ได้รับความนิยมเป็นอย่างมากในการเขียนเว็บไซร์ที่มีการติดต่อกับฐานข้อมูล

2.5.4 AppServ

AppServ คือ โปรแกรมที่รวบรวม Packages ต่างๆ ได้แก่

1. Apache Web Sever คือ โปรแกรมที่ทำหน้าที่เป็น Web Sever
2. MySQL Database คือ โปรแกรมที่ทำหน้าที่เป็น Database Sever
3. PHP Interpreter คือ ตัวแปรภาษา PHP ที่เอาไว้เขียนโปรแกรม
4. PHP MyAdmin คือ ตัวควบคุมจัดการ MySQL Database ผ่านเว็บไซร์

โปรแกรม AppServ สามารถติดตั้ง Apache , PHP , MySQL โดยขั้นตอนที่ไม่ยุ่งยากและพร้อมใช้งานโดยทันที ซึ่งสามารถที่จะเขียน PHP ให้สามารถทำงานร่วมกับ MySQL Database ภายในเครื่องได้ทันที โดยเครื่องคอมพิวเตอร์ก็เปรียบเสมือน Web Server

2.6 JAVA

ภาษาจาวา เป็นภาษาโปรแกรมเชิงวัตถุที่พัฒนาขึ้นโดย "เจมส์ กอสลิง" และทีมวิศวกร ซึ่งบริษัท Sun Microsystems ต้องการนำภาษาจาวามาใช้แทนภาษา C++ ชื่อของ "JAVA" มาจากชื่อกาแฟที่ทีมวิศวกรของ Sun Microsystems ดื่มตอนที่ร่วมกันพัฒนาภาษา Java ขึ้นมา ซึ่งจุดเด่นของภาษา Java อยู่ที่ผู้เขียนโปรแกรมสามารถใช้หลักการของ Object - Oriented Programming มาพัฒนาโปรแกรมของตน ภาษาจาวาเริ่มเป็นที่นิยมแพร่หลายในปี ค.ศ. 1995 ภาษาจาวาเป็นภาษาที่ไม่ขึ้นกับแพลตฟอร์ม (platform independent) JDK 1.0 ประกาศใช้เมื่อปี 1996 JDK

2.6.1. รุ่นต่างๆ ของภาษา JAVA

- 1.0 ค.ศ. 1996 ออกครั้งแรกสุด
- ค.ศ. 1997 ปรับปรุงครั้งใหญ่ โดยเพิ่ม inner class
- 1.2 4 ธันวาคม, ค.ศ. 1998 รหัส Playground ด้านจาวาแพลตฟอร์มได้รับการเปลี่ยนแปลงครั้งใหญ่ใน API และ JVM (API สำคัญที่เพิ่มมาคือ Java Collections Framework และ Swing; ส่วนใน JVM เพิ่ม JIT compiler) แต่ตัวภาษาจาวานั้นเปลี่ยนแปลงเพียงเล็กน้อย (เพิ่มคีย์เวิร์ด strictfp) และทั้งหมดถูกเรียกชื่อใหม่ว่า "จาวา 2" แต่ระบบเลขรุ่นยังไม่เปลี่ยนแปลง
- 1.3 8 พฤษภาคม, ค.ศ. 2000 รหัส Kestrel แก้ไขเล็กน้อย
- 1.4 13 กุมภาพันธ์, ค.ศ. 2002 รหัส Merlin เป็นรุ่นที่ถูกใช้งานมากที่สุดในปัจจุบัน (ขณะที่เขียน ค.ศ. 2005)
- 5.0 29 กันยายน, ค.ศ. 2004 รหัส Tiger (เดิมทีนับเป็น 1.5) เพิ่มคุณสมบัติใหม่ในภาษาจาวา เช่น Annotations ซึ่งเป็นที่ถกเถียงกันว่านำมาจากภาษา C# ของบริษัทไมโครซอฟท์, Enumerations, Varargs, Enhanced for loop, Autoboxing, และที่สำคัญคือ Generics
- 6.0 11 ธันวาคม, ค.ศ. 2006 รหัส Mustang เป็นรุ่นในการพัฒนาของ Java SDK 6.0 ที่ออกมาให้ทดลองใช้ในเดือนพฤศจิกายน ค.ศ. 2004
- 7.0 กำลังพัฒนา กำหนดออก ค.ศ. 2008 รหัส Dolphin กำลังพัฒนา

2.6.2. ข้อดีข้อเสียของภาษา JAVA

ข้อดีของภาษา JAVA

- โปรแกรม JAVA ที่เขียนขึ้นสามารถทำงานได้หลาย Platform โดยไม่จำเป็นต้องแก้ไขหรือ Compile ใหม่ ทำให้ช่วยลดค่าใช้จ่ายและเวลาที่ต้องเสียไปในการ Port หรือทำให้โปรแกรมใช้งานได้หลาย Platform
- ภาษา JAVA เป็นภาษาเชิงวัตถุ ซึ่งเหมาะสำหรับพัฒนาระบบที่มีความซับซ้อน การพัฒนาโปรแกรมแบบวัตถุจะช่วยให้สามารถใช้คำหรือชื่อ ต่าง ๆ ที่มีอยู่ในระบบงานนั้นมาใช้ในการออกแบบโปรแกรมได้ ทำให้เข้าใจได้ง่ายขึ้น
- ภาษา JAVA มีความซับซ้อนน้อยกว่าภาษา C++ ทำให้ใช้งานได้ง่ายกว่าและลดความผิดพลาดได้มากขึ้น
- ภาษา JAVA มีการตรวจสอบข้อผิดพลาดทั้งตอน Compile time และ Runtime ทำให้ลดข้อผิดพลาดที่อาจเกิดขึ้นในโปรแกรม และช่วยให้ Debug โปรแกรมได้ง่าย
- ภาษา JAVA ถูกออกแบบมาให้มีความปลอดภัยสูงตั้งแต่แรก ทำให้โปรแกรมที่เขียนขึ้นด้วย JAVA มีความปลอดภัยมากกว่าโปรแกรมที่เขียนขึ้นด้วยภาษาอื่นๆ
- ภาษา JAVA มี IDE, application server, และ Library ต่าง ๆ มากมายสำหรับ JAVA สามารถใช้งานได้โดยไม่ต้องเสียค่าใช้จ่าย ทำให้สามารถลดค่าใช้จ่ายที่ต้องเสียไปกับการซื้อ Tool และ s/w ต่าง ๆ

ข้อเสียของภาษา JAVA

- ทำงานได้ช้ากว่า Native Code (โปรแกรมที่ Compile ให้อยู่ในรูปของภาษาเครื่อง) หรือโปรแกรมที่เขียนขึ้นด้วยภาษาอื่น อย่างเช่น C หรือ C++ ทั้งนี้ก็เพราะว่าโปรแกรมที่เขียนขึ้นด้วยภาษา JAVA จะถูกแปลงเป็นภาษากลางก่อน แล้วเมื่อโปรแกรมทำงานคำสั่งของภาษากลางนี้จะถูกเปลี่ยนเป็นภาษาเครื่องอีกทีหนึ่ง ทีละคำสั่ง (หรือกลุ่มของคำสั่ง) ณ Runtime ทำให้ทำงานช้ากว่า Native code ซึ่งอยู่ในรูปของภาษาเครื่องแล้วตั้งแต่ compile โปรแกรมที่ต้องการความเร็วในการทำงานจึงไม่นิยมเขียนด้วยภาษา JAVA
- Tool ที่มีในการใช้พัฒนาโปรแกรม JAVA มักไม่ค่อยอำนวย ทำให้หลาย ๆ อย่าง โปรแกรมเมอร์จะต้องเป็นทำขึ้นเอง ทำให้ต้องเสียเวลาทำงานในส่วนที่ Tool ทำไม่ได้ ถ้าดู Tool ของ MS จะใช้งานได้ง่ายกว่า และพัฒนาได้เร็วกว่า (แต่ต้องซื้อ Tool ของ MS และก็ต้องรันบน platform ของ MS

2.7 แอนดรอยด์

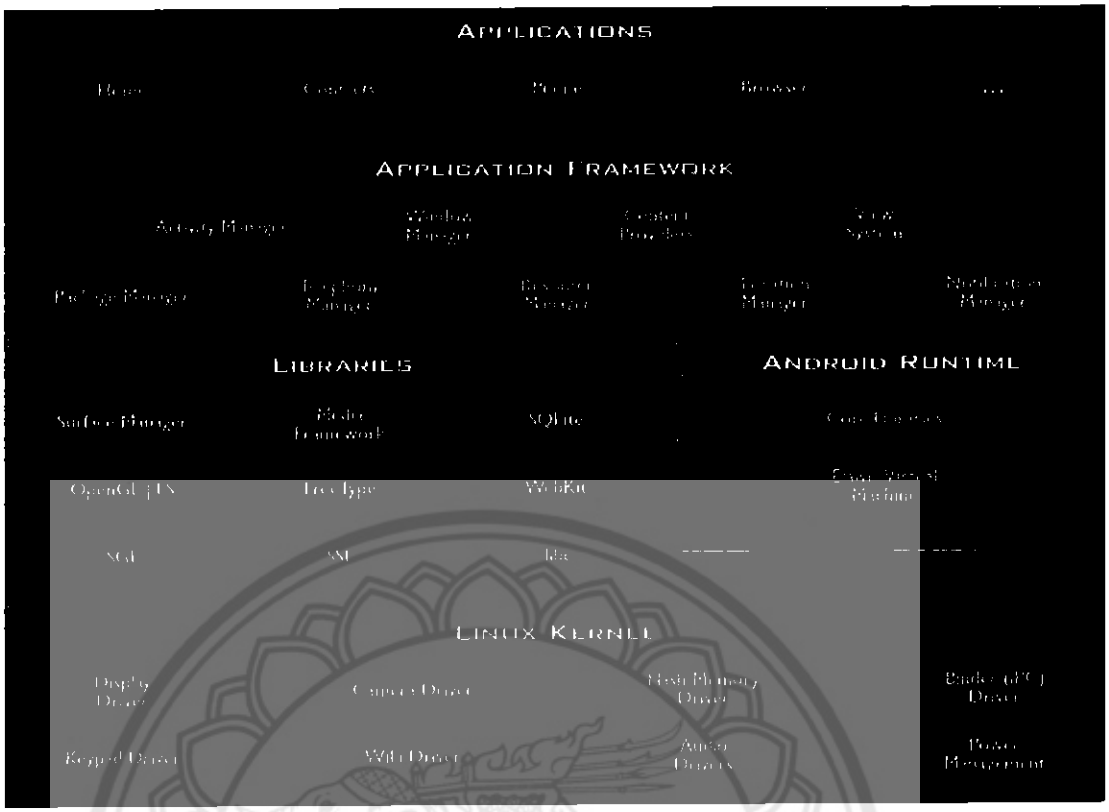
เริ่มต้นระบบปฏิบัติการแอนดรอยด์ ถูกพัฒนามาจากบริษัทแอนดรอยด์ (Android Inc.) เมื่อปี พ.ศ. 2546 โดยมีนาย แอนดี้ รูบิน (Andy Rubin) ผู้ให้กำเนิดระบบปฏิบัติการนี้ และถูกบริษัท Google ซื้อกิจการเมื่อ เดือนสิงหาคม ปี พ.ศ. 2548 โดยบริษัท Android ได้กลายเป็นบริษัทลูก ของบริษัท Google และยังมีนาย แอนดี้ รูบิน ดำเนินงานอยู่ในทีมพัฒนาระบบปฏิบัติการต่อไป

ระบบปฏิบัติการแอนดรอยด์ เป็นระบบปฏิบัติการที่พัฒนามาจากการนำเอา แกนกลางของระบบปฏิบัติการลินุกซ์ Linux Kernel ซึ่งเป็นระบบปฏิบัติการที่ออกแบบมาเพื่อทำงานเป็นเครื่องให้บริการ Server มาพัฒนาต่อ เพื่อให้กลายเป็นระบบปฏิบัติการบนอุปกรณ์พกพา Mobile Operating System

ต่อมาเมื่อเดือน พฤศจิกายน ปี พ.ศ 2550 บริษัทกูเกิ้ล ได้ทำการก่อตั้งสมาคม OHA (Open Handset Alliance, http://www.openhandsetalliance.com) เพื่อเป็นหน่วยงานกลางในการกำหนดมาตรฐานกลาง ของอุปกรณ์พกพาและระบบปฏิบัติการแอนดรอยด์ โดยมีสมาชิกในช่วงก่อนตั้งจำนวน 34 รายเข้าร่วม ซึ่งประกอบไปด้วยบริษัทชั้นนำที่ดำเนินธุรกิจด้านการสื่อสาร เช่น โรงงานผลิตอุปกรณ์พกพา, บริษัทพัฒนาโปรแกรม, ผู้ให้บริการสื่อสาร และผู้ผลิตอะไหล่อุปกรณ์ด้านสื่อสาร

2.7.1 โครงสร้างของแอนดรอยด์

การทำความเข้าใจโครงสร้างของระบบปฏิบัติการแอนดรอยด์ ถือว่าเป็นสิ่งสำคัญเพราะถ้านักพัฒนาโปรแกรมสามารถมองภาพโดยรวมของระบบได้ทั้งหมดจะให้สามารถเข้าใจถึงกระบวนการทำงานได้ดียิ่งขึ้น และสามารถนำไปช่วยในการออกแบบโปรแกรมที่ต้องการพัฒนาเพื่อให้เกิดประสิทธิภาพในการทำงาน



รูปที่ 2.7 : โครงสร้างของแอนดรอยด์

ที่มา : http://www.sourcecode.in.th/articles.php?id=71

จากโครงสร้างของระบบปฏิบัติการแอนดรอยด์ จะเห็นได้ว่า มีการแบ่งออกมาเป็นส่วนๆ ที่มีความเกี่ยวเนื่องกัน โดยส่วนบนสุดจะเป็นส่วนที่ผู้ใช้งานทำการติดต่อโดยตรงซึ่งก็คือ ส่วนของแอพพลิเคชั่น จากนั้นก็จะลำดับลงมาเป็นองค์ประกอบอื่นๆ ตามลำดับ และสุดท้ายจะเป็นส่วนที่ติดต่อกับอุปกรณ์โดยผ่านทาง Linux Kernel โครงสร้างของแอนดรอยด์ สามารถอธิบายเป็นส่วนๆ ได้ดังนี้

แอพพลิเคชั่น ส่วน แอพพลิเคชั่น หรือส่วนของโปรแกรมที่มีมากับระบบปฏิบัติการ หรือเป็นกลุ่มของโปรแกรมที่ผู้ใช้งานได้ทำการติดตั้งไว้ โดยผู้ใช้งานสามารถเรียกใช้โปรแกรมต่างๆได้โดยตรง ซึ่งการทำงานของแต่ละโปรแกรมจะเป็นไปตามที่ผู้พัฒนาโปรแกรมได้ออกแบบและเขียนโค้ดโปรแกรมเอาไว้

แอพพลิเคชั่นเฟรมเวิร์ค เป็นส่วนที่มีการพัฒนาขึ้นเพื่อให้นักพัฒนาสามารถพัฒนาโปรแกรมได้สะดวก และมีประสิทธิภาพมากยิ่งขึ้น โดยนักพัฒนาไม่จำเป็นต้องพัฒนาในส่วนที่มีความยุ่งยากมาก เพียงแค่ทำการศึกษาถึงวิธีการเรียกใช้งานแอพพลิเคชั่นเฟรมเวิร์ค ในส่วนที่ต้องการใช้งาน แล้วนำมาใช้งาน ซึ่งมีหลายกลุ่มด้วยกัน ตัวอย่างเช่น

- **Activities Manager** เป็นกลุ่มของชุดคำสั่งที่จัดการเกี่ยวกับวงจรการทำงานของหน้าต่างโปรแกรม(Activity)
- **Content Providers** เป็นกลุ่มของชุดคำสั่ง ที่ใช้ในการเข้าถึงข้อมูลของโปรแกรมอื่น และสามารถแบ่งปันข้อมูลให้โปรแกรมอื่นเข้าถึงได้
- **View System** เป็นกลุ่มของชุดคำสั่งที่เกี่ยวกับการจัดการโครงสร้างของหน้าจอที่แสดงผลในส่วนที่ติดต่อกับผู้ใช้งาน (User Interface)
- **Telephony Manager** เป็นกลุ่มของชุดคำสั่งที่ใช้ในการเข้าถึงข้อมูลด้านโทรศัพท์ เช่นหมายเลขโทรศัพท์ เป็นต้น
- **Resource Manager** เป็นกลุ่มของชุดคำสั่งในการเข้าถึงข้อมูลที่เป็น ข้อความ, รูปภาพ
- **Location Manager** เป็นกลุ่มของชุดคำสั่งที่เกี่ยวกับตำแหน่งทางภูมิศาตร์ ที่ระบบปฏิบัติการได้รับค่าจากอุปกรณ์
- **Notification Manager** เป็นกลุ่มของชุดคำสั่งที่จะถูกเรียกใช้เมื่อโปรแกรมต้องการแสดงผลให้กับผู้ใช้งาน ผ่านทางแถบสถานะ(Status Bar) ของหน้าจอ

Libraries เป็นส่วนของชุดคำสั่งที่พัฒนาด้วย C/C++ โดยแบ่งชุดคำสั่งออกเป็นกลุ่มตามวัตถุประสงค์ของการใช้งาน เช่น Surface Manage จัดการเกี่ยวกับการแสดงผล, Media Framework จัดการเกี่ยวกับการการแสดงภาพและเสียง, Open GL | ES และ SGL จัดการเกี่ยวกับภาพ 3มิติ และ 2มิติ, SQL lite จัดการเกี่ยวกับระบบฐานข้อมูล เป็นต้น

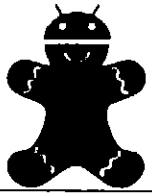
แอนดรอยด์ **Runtime** จะมี Darvik Virtual Machine ที่ถูกออกแบบมาเพื่อให้ทำงานบนอุปกรณ์ที่มี หน่วยความจำ (Memmory) , หน่วยประมวลผลกลาง(CPU) และพลังงาน(Battery)ที่จำกัด ซึ่งการทำงานของ Darvik Virtual Machine จะทำการแปลงไฟล์ที่ต้องการทำงาน ไปเป็นไฟล์ .DEX ก่อนการทำงาน เหตุผลก็เพื่อให้มีประสิทธิภาพเพิ่มขึ้นเมื่อใช้งานกับ หน่วยประมวลผลกลางที่มีความเร็วไม่มาก ส่วนต่อมาคือ Core Libraries ที่เป็นส่วนรวบรวมคำสั่งและชุดคำสั่งสำคัญ โดยถูกเขียนด้วยภาษาจาวา (Java Language)

Linux Kernel เป็นส่วนที่ทำหน้าที่หัวใจสำคัญ ในจัดการกับบริการหลักของระบบปฏิบัติการ เช่น เรื่องหน่วยความจำ พลังงาน ติดต่อกับอุปกรณ์ต่างๆ ความปลอดภัย เครือข่าย โดย Android ได้นำเอาส่วนนี้มาจากระบบปฏิบัติการลินุกซ์ รุ่น 2.6 (Linux 26. Kernel) ซึ่งได้มีการออกแบบมาเป็นอย่างดี

2.7.2 แอนดรอยด์เวอร์ชั่น

รุ่นพัฒนาของแอนดรอยด์จะใช้รหัสชื่อเป็นชื่อขนมหวาน โดยมีอักษรขึ้นต้นเรียงลำดับกัน

ตารางที่ 2.2 : แอนดรอยด์เวอร์ชั่น

เวอร์ชั่น	ชื่อ / Logo	ลินุกซ์ เคอร์เนล	วันที่เปิดตัว
1.0	-	-	23 กันยายน 2551
1.5	V1.5 Cupcake 	2.6.27	30 เมษายน 2552
1.6	V1.6 Donut 	2.6.29	15 กันยายน 2552
2.0	V2.0 Eclari 	2.6.29	26 ตุลาคม 2553
2.2	V2.2 Froyo 	2.6.32	20 พฤษภาคม 2553
2.3	V2.3 Gingerbread 	-	6 ธันวาคม 2553
3.0	V3.0 Gingerbread 	-	22 กุมภาพันธ์ 2554

2.7.3 แอนดรอยด์ SDK (Android Software Development Kit)

คือ ชุดโปรแกรมที่ทาง Google ได้พัฒนาออกมาเพื่อแจกจ่ายให้นักพัฒนาแอพพลิเคชั่นหรือผู้สนใจทั่วไปดาวน์โหลดไปใช้กันโดยไม่มีค่าใช้จ่าย ซึ่งก็เป็นหนึ่งในปัจจัยที่ทำให้แอพพลิเคชั่นบนแอนดรอยด์ นั้นเพิ่มขึ้น อย่างรวดเร็ว ซึ่งในชุด SDK นั้นจะมีโปรแกรมและไลบรารี่ต่างๆ ที่จำเป็นต่อการพัฒนาแอพพลิเคชั่นบนแอนดรอยด์ อย่างเช่น Emulator ซึ่งทำให้ผู้ใช้สามารถสร้างแอพพลิเคชั่นและนำมาทดลองรันบน Emulator โดยมีสภาวะแวดล้อมเหมือนมือถือที่รันระบบปฏิบัติการแอนดรอยด์ จริง

รูปที่ 2.8 : แอนดรอยด์ SDK เมื่อทำการ Run Program

ที่มา : ได้จากการรันโปรแกรม

บทที่ 3
วิธีดำเนินโครงงาน

3.1 การวิเคราะห์

การเก็บรวบรวมและวิเคราะห์ความต้องการของระบบ (System Requirement and Analysis) เป็นขั้นตอนที่ทำให้ทราบถึงความต้องการในระบบของของผู้ใช้บริการ

3.1.1 ความต้องการของระบบ (System Requirement)

ในการศึกษาความต้องการของระบบในโครงงานจึงได้เก็บรวบรวมข้อมูลต่างๆ จากเว็บไซต์ ศึกษาหนังสือและเอกสารที่เกี่ยวข้อง จึงสามารถสรุปความต้องการของระบบได้ดังนี้

3.1.1.1 ความต้องการของผู้พัฒนาระบบ ล็อคอิน

ความต้องการของผู้พัฒนาระบบล็อคอินสามารถแบ่งได้ดังนี้

1. ต้องการเพิ่มความปลอดภัยในการใช้คอมพิวเตอร์สาธารณะของผู้ใช้
2. ต้องการประยุกต์ใช้มือถือสมาร์ทโฟนเข้ามาช่วยในการ ล็อคอิน เพื่อเพิ่มความปลอดภัยให้กับผู้ใช้

3.1.1.2 ความต้องการที่ใช้การเข้ารหัสแบบ SHA1

เนื่องจากทางผู้จัดทำได้นำเทคนิคการเข้ารหัสมาใช้กับโทรศัพท์สมาร์ทโฟน ซึ่งเป็นที่ทราบกันโดยทั่วไปว่าโทรศัพท์สมาร์ทโฟนมีหน่วยการประมวลผลที่น้อยกว่าคอมพิวเตอร์ ซึ่งการเข้ารหัสแบบ Hash function มีความเร็วในการคำนวณประมวลผลที่เร็วกว่าการเข้ารหัสแบบ Encryption ดังนั้นผู้พัฒนาจึงเลือกใช้การเข้ารหัสแบบ Hash Function โดยเลือกใช้เป็นชนิด SHA1 ในการพัฒนาระบบ

3.2 การออกแบบ

3.2.1 การออกแบบโปรโตคอล

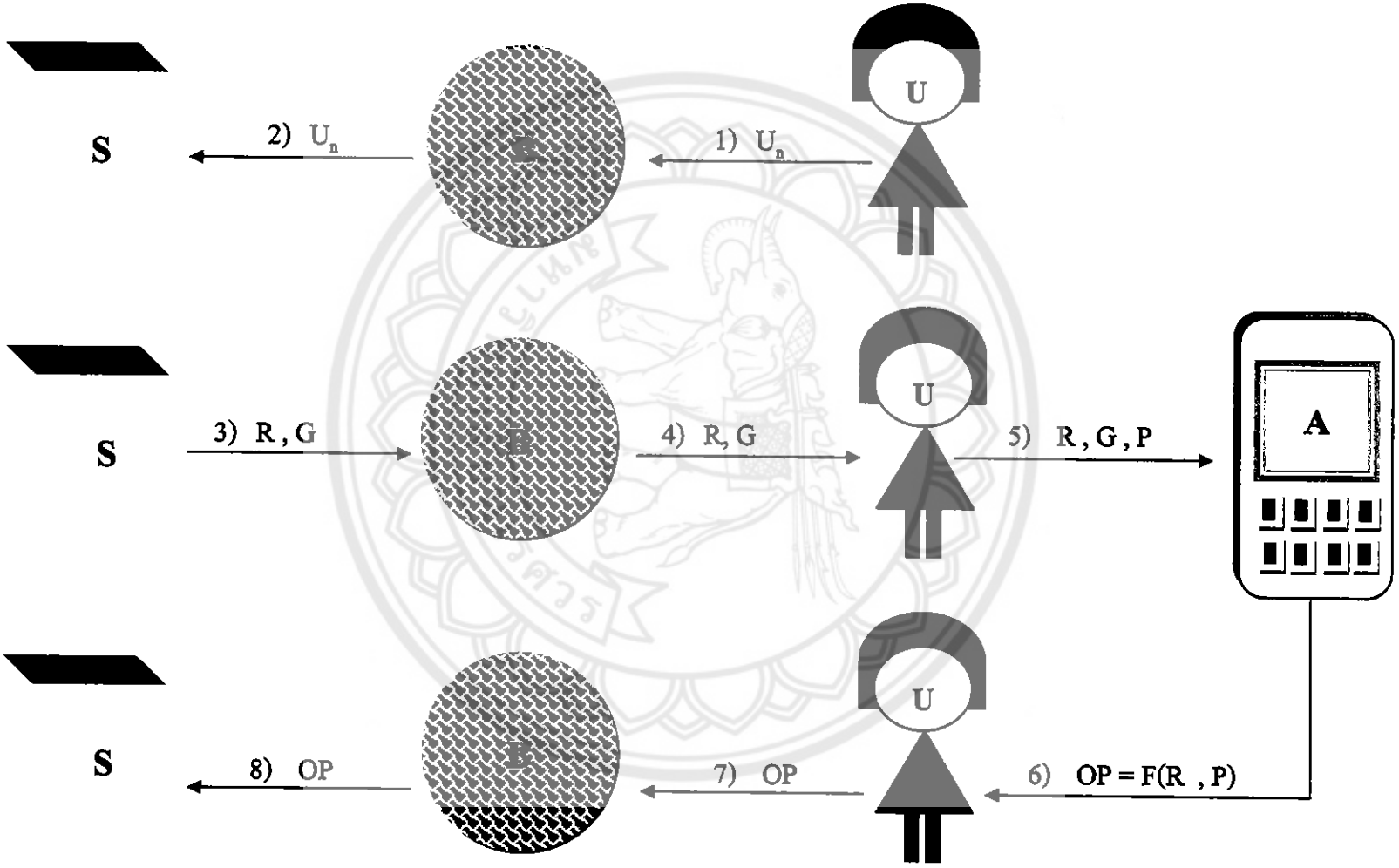
จากการวิเคราะห์องค์ประกอบของระบบ การใช้สมาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ จึงได้มีการออกแบบโปรโตคอล ดังขั้นตอนต่อไปนี้

โดยที่

S	คือ	เซิร์ฟเวอร์
U	คือ	ผู้ใช้งานระบบ
A	คือ	แอพพลิเคชั่น
B	คือ	เบราว์เซอร์
U_n	คือ	ชื่อผู้ใช้
R	คือ	ชุดข้อความสุ่มตัวเลขและตัวอักษร 10 หลัก
G	คือ	ค่าสุ่มตำแหน่ง 4 ตำแหน่ง*
P	คือ	รหัสผ่านของผู้ใช้
F	คือ	ค่าที่ได้จาก R และ G ที่ทำการเข้ารหัสแบบ SHA1
OP	คือ	รหัส 4 หลักที่ได้จากการเข้ารหัสในแอพพลิเคชันแอนดรอยด์

หมายเหตุ :

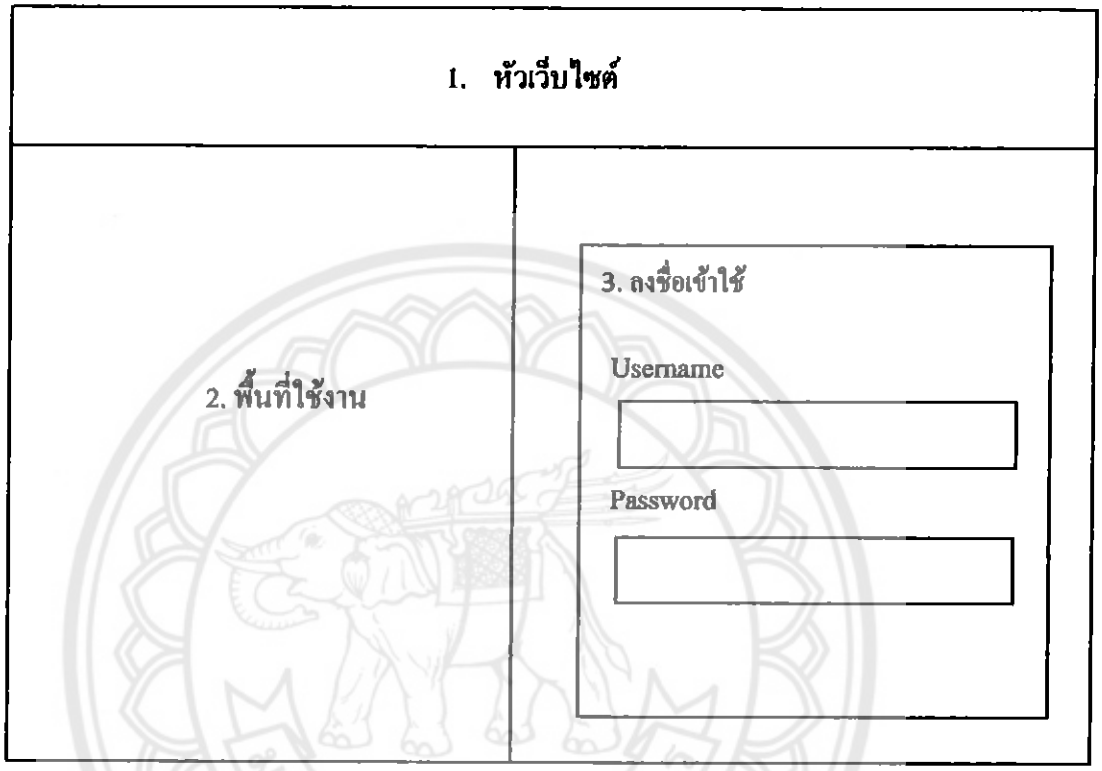
* ค่าสุ่มตำแหน่ง หมายถึง ค่าตำแหน่ง 4 ตำแหน่งที่ได้จากการสุ่ม จาก 40 ตำแหน่ง ของรหัส 40 ตัวที่ได้จากการเข้ารหัส SHA1



รูปที่ 3.1 การออกแบบโปรโตคอล

3.2.3 การออกแบบหน้าเว็บไซต์

ในหน้าของเว็บไซต์ที่ทำหน้าที่เป็นตัวหลักการเข้าระบบล็อคอิน ได้มีการแบ่งหน้าเว็บไซต์ออกเป็นดังนี้



รูปที่ 3.2 : การออกแบบหน้าเว็บไซต์

ส่วนหน้าเว็บไซต์จะแบ่งเป็น 3 ส่วน ดังนี้

1. หัวเว็บไซต์ : แสดงรูปภาพ
2. พื้นที่ใช้งาน : ส่วนของพื้นที่ที่ให้ทำรายการต่าง ๆ
3. ลงชื่อเข้าใช้ : ส่วนของพื้นที่ที่ให้ทำรายการต่าง ๆ

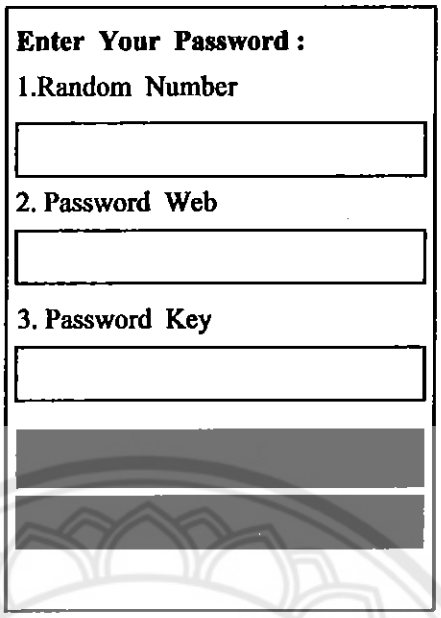
3.2.4 การออกแบบหน้าแอพพลิเคชั่นแอนดรอยด์

การออกแบบหน้าแอพพลิเคชั่นแอนดรอยด์ ได้แบ่งออกเป็น 2 หน้าการออกแบบโดยหน้าแรกของแอพพลิเคชั่น ดังรูปที่ 3.5 และหน้าที่สองดังรูปที่ 3.6 ตามลำดับ

รูปที่ 3.3 : การออกแบบหน้าแรกแอพพลิเคชั่นแอนดรอยด์

ส่วนหน้าแอพพลิเคชั่นแอนดรอยด์ จะแบ่งเป็น 3 ส่วน ดังนี้

1. พื้นที่ใช้งาน : ส่วนของพื้นที่ที่ให้ทำรายการต่าง ๆ
2. Manual : ปุ่มกดเข้าฟังก์ชั่นการใช้งาน
3. Scan : ปุ่มกดเข้าฟังก์ชั่น Scan Bar code

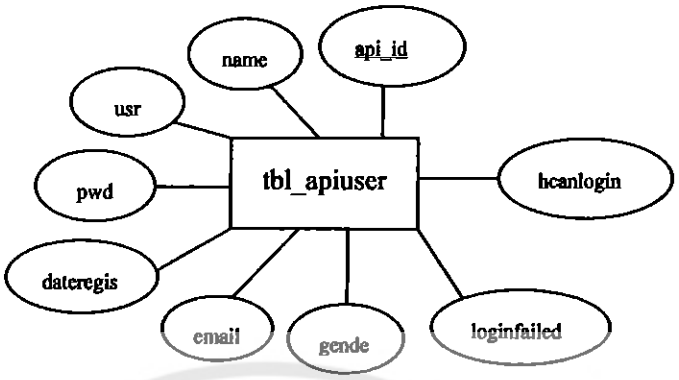


รูปที่ 3.4 : ส่วนที่สองของการออกแบบหน้าแอพพลิเคชั่นแอนดรอยด์

ส่วนหน้าที่สองแอพพลิเคชั่นแอนดรอยด์ จะแบ่งเป็น 5 ส่วน ดังนี้

1. Random Number : ช่องกรอกเลข Random ที่ได้จากการ Scan barcode หรือที่มีให้จากหน้าเว็บไซต์
2. Password Web : ช่องกรอก Password ที่ได้จากการสมัครการใช้งานในครั้งแรก
3. Password Key : ช่องที่ได้จากการ Submit แล้วนำ Password Key ที่ได้ไปกรอกที่หน้าเว็บไซต์อีกครั้ง
4. QR-Code : ปุ่มกด QR-code เป็นช่องที่ผู้ใช้สามารถกดเพื่อไปหน้า Scan barcode อีกครั้งได้
5. Submit : ปุ่มกด Submit ใช้ในกรณีที่ผู้ใช้กรอกรหัส Random Number และ Password web เสร็จสิ้นแล้ว

3.2.5 การออกแบบดาต้าเบส

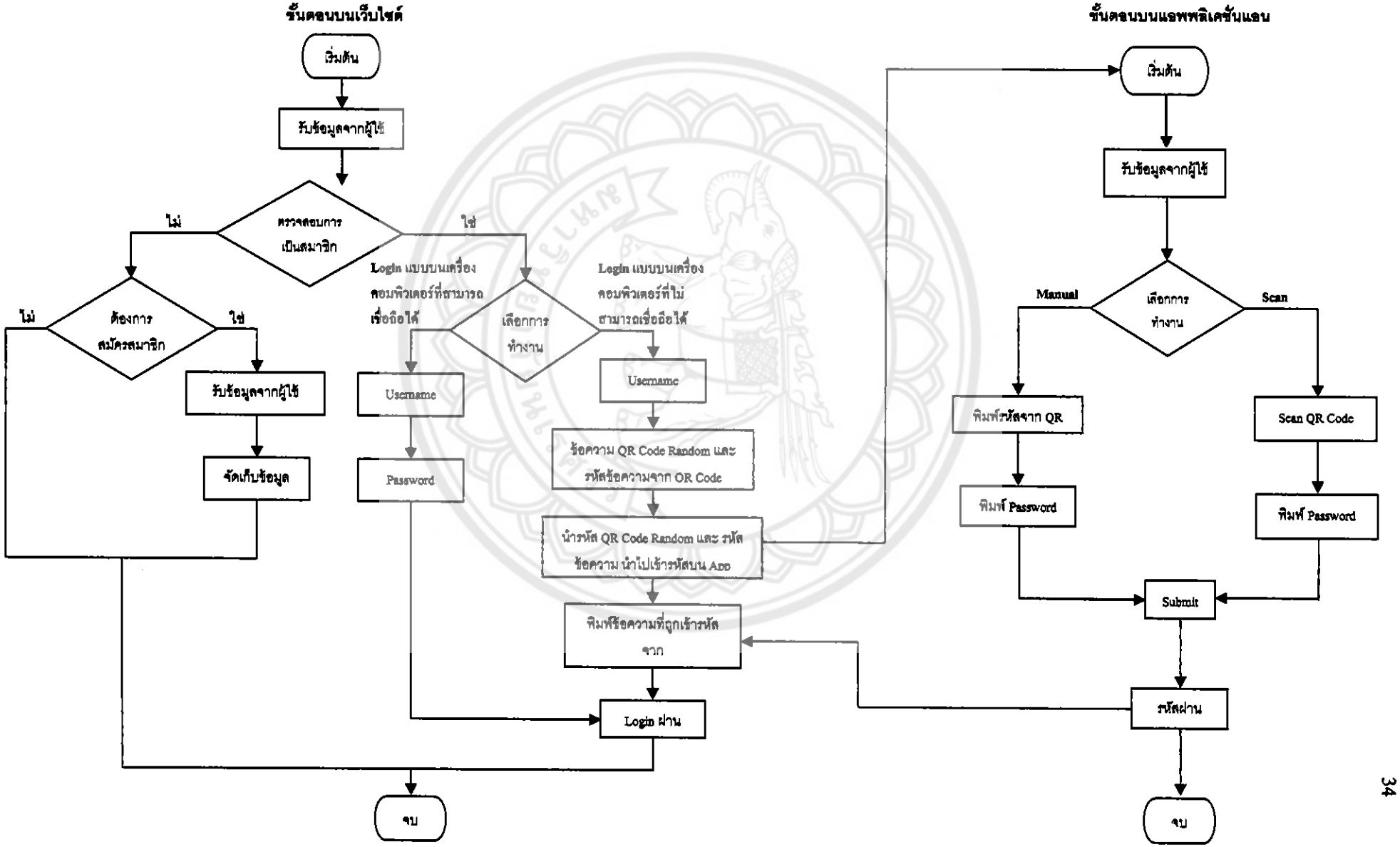


รูปที่ 3.5 : ER – Diagram

ตารางที่ 3.1 : ตาราง tbl_apiuser

ฟิลด์	ชนิด	ไพรมารี	รายละเอียด
api_id	int (s)	PK	หมายเลขการทำรายการ
name	varchar (50)	-	ชื่อ
usr	varchar (50)	-	ชื่อผู้ใช้
pwd	varchar (50)	-	รหัสผ่าน
dateregis	detetime	-	วันที่
email	varchar (50)	-	อีเมลล์
gender	char (6)	-	เพศ
login failed	varchar (1)	-	ตัวนับจำนวนครั้งที่กรอกรหัสผิด
hcan login	varchar (1)	-	เวลาที่ถูกบล็อก

3.2.5 ขั้นตอนการทำงานของระบบล็อคอิน



รูปที่ 3.6 ระบบการทำงานของระบบล็อคอิน

บทที่ 4
ผลการทดสอบและการใช้งานจริงของระบบ

เมื่อพัฒนาโปรแกรมล็อคอินเสร็จสมบูรณ์ ผู้จัดทำจะทำการทดสอบโปรแกรม ว่าเป็นไปตามเงื่อนไขที่กำหนดไว้หรือไม่ โดยการทดลองโปรแกรมนั้นแบ่งออกเป็น 5 ส่วนใหญ่ดังนี้

4.1 หน้าแรกของระบบและส่วนประกอบต่างๆ ของระบบ

4.2 การสมัครสมาชิก

4.3 ขั้นตอนการล็อคอินบนเว็บไซต์

4.3.1 แบบบนเครื่องคอมพิวเตอร์ที่สามารถเชื่อถือได้

4.3.2 แบบบนเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ (โดยการนำมือถือสมาร์ทโฟนเข้ามาช่วยในการล็อคอิน)

4.4 ขั้นตอนการใช้งานบนมือถือแอพพลิเคชั่นแอนดรอยด์

4.4.1 รูปแบบแอพพลิเคชั่นแอนดรอยด์

4.4.2 ขั้นตอนการใช้งาน แบบ Manual

4.4.3 ขั้นตอนการใช้งาน แบบ Scan

4.4.4 ขั้นตอนการดาวน์โหลดแอพพลิเคชั่นแอนดรอยด์

4.5 การทดลองและวิเคราะห์ความปลอดภัยของระบบ

4.1 หน้าแรกของระบบและส่วนประกอบต่างๆ ของระบบ

4.1.1 หน้าแรกของระบบ เป็นการสร้างหน้าเว็บไซต์ทั่วไปในการใช้งาน ในหน้าแรกของเว็บไซต์จะบังคับเลือกว่าจะล็อคอินเข้าสู่ระบบในรูปแบบใด ดังในรูปที่ 4.2

รูปที่ 4.1 : หน้าแรกของเว็บไซต์

4.1.2 รูปแบบการเลือกใช้งาน ในส่วนนี้จะอยู่ในหน้าแรกของระบบซึ่งจะมีรูปแบบให้เลือกดังนี้

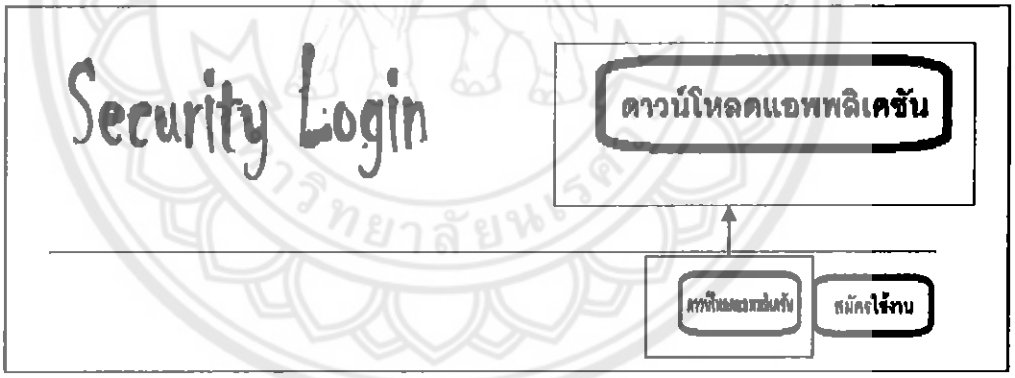
1. รูปแบบล็อคอิน แบบบนเครื่องคอมพิวเตอร์ที่สามารถเชื่อถือได้
2. รูปแบบล็อคอิน แบบบนเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ (โดยการนำมือถือสมาร์ทโฟนเข้ามาช่วยในการล็อคอิน)

รูปที่ 4.2 : เลือกรูปแบบการล็อคอิน

4.1.3 ปุ่มสมัครเข้าใช้งาน ในส่วนนี้จะอยู่หน้าแรกของระบบล็อคอินเพื่อไว้รองรับผู้ใช้ที่ยังไม่ได้สมัครสมาชิกก่อนเข้าสู่ระบบ

รูปที่ 4.3 : รูปปุ่มสมัครใช้งาน

4.1.4 ปุ่มดาวน์โหลดแอพพลิเคชั่น ในส่วนนี้จะอยู่หน้าแรกของระบบล็อคอิน เพื่อไว้รองรับกรณีที่ผู้ใช้เปลี่ยนมือถือ และอยากดาวน์โหลด แอพพลิเคชั่นใหม่อีกครั้ง



รูปที่ 4.4 : รูปปุ่มดาวน์โหลดแอพพลิเคชั่น

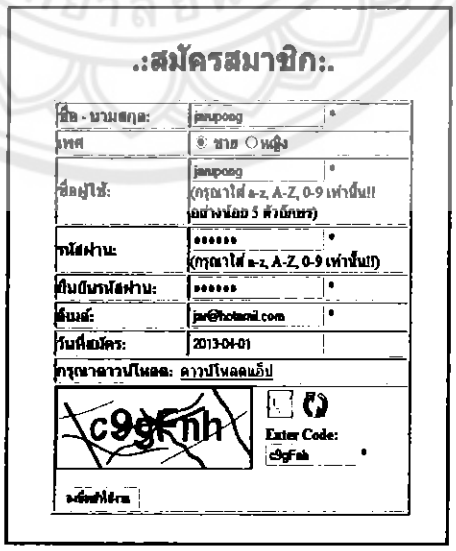
4.2 การสมัครสมาชิก

การสมัครสมาชิก ก่อนที่ผู้ใช้ระบบจะมีสิทธิ์ใช้ระบบนั้น จะต้องมีการสมัครสมาชิกเพื่อลงทะเบียนเข้าสู่ระบบก่อน โดยสามารถทำตามขั้นตอนดังนี้

1. เลือกที่ปุ่ม "สมัครใช้งาน" ในหน้าแรกของเว็บ จากนั้นระบบจะเข้ามายังหน้าสำหรับใส่ข้อมูลส่วนตัวดังรูปที่ 4.5

รูปที่ 4.5 : หน้าสำหรับใส่ข้อมูลส่วนตัวในหน้าสมัครสมาชิก

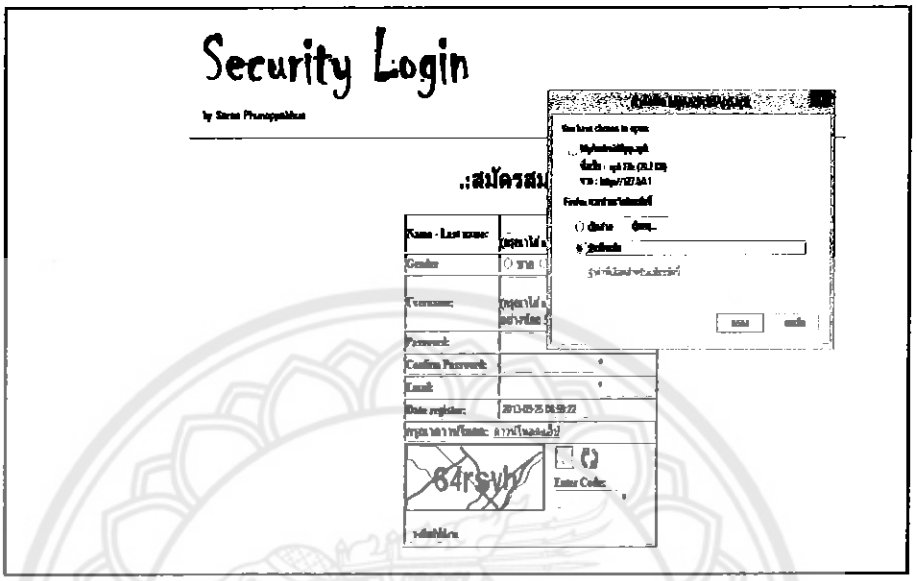
2. ให้ทำการกรอกข้อมูลของผู้ที่ต้องการสมัครลงไปดังรูปที่ 4.6 และเลือก "กรุณาดาวน์โหลด" ดังรูปที่ 4.7



รูปที่ 4.6 : การกรอกข้อมูลลงในส่วนใส่ข้อมูลส่วนตัวในหน้าสมัครสมาชิก

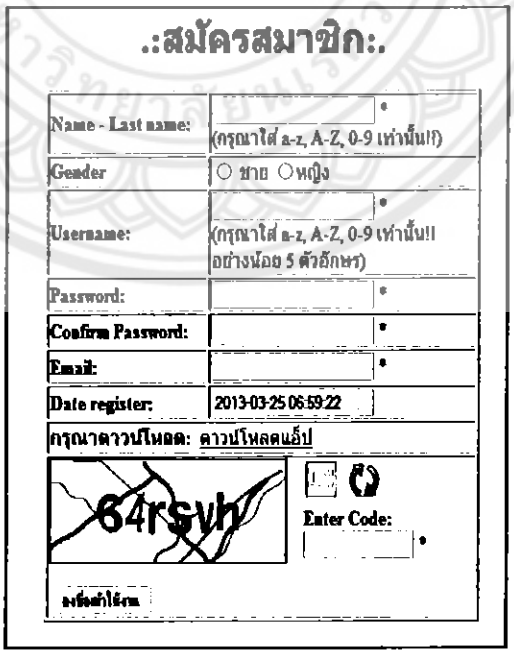
3. ระบบจะเข้ามายังหน้าสำหรับการดาวน์โหลดแอพพลิเคชั่นแอนดรอยด์ ดังรูปที่ 4.6

**หมายเหตุ รูปแบบการดาวน์โหลดแล้วแต่ Browser ที่ผู้ใช้ ใช้งาน



รูปที่ 4.7 : หน้าการดาวน์โหลดแอพพลิเคชั่นแอนดรอยด์

4. ทำการดาวน์โหลดแอพพลิเคชั่นแอนดรอยด์ และใส่รหัส Captcha ดังรูปที่ 4.8 ให้เสร็จสิ้นแล้วกดปุ่มลงชื่อเข้าใช้งานเรียบร้อยแล้วจะเข้าสู่หน้าล็อคอิน ดังรูปที่ 4.9



รูปที่ 4.8 : แสดงการกรอกรหัส Captcha

4.3 ขั้นตอนการล็อคอินบนเว็บไซต์

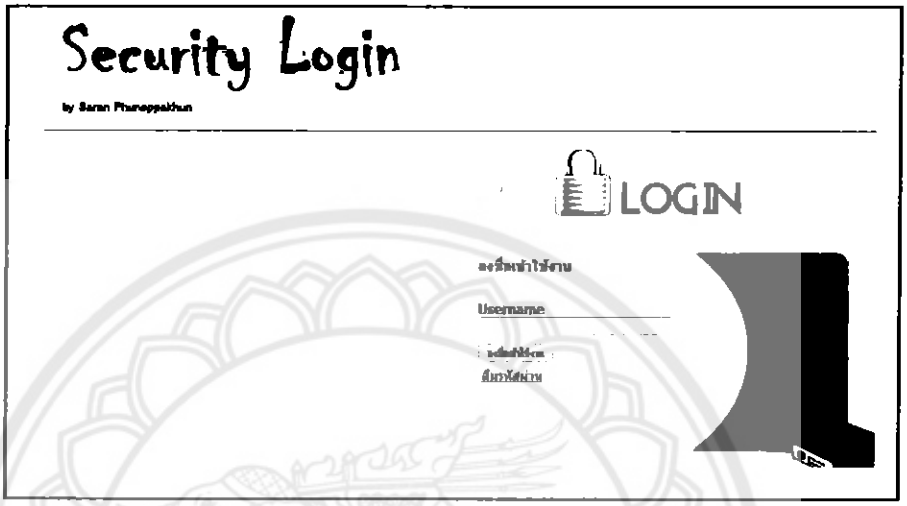
เมื่อผู้ใช้ทำการสมัครสมาชิกเป็นที่เรียบร้อยแล้ว ผู้ใช้จะสามารถทำการเข้าสู่ระบบเพื่อใช้ระบบได้ โดยการเข้าสู่ระบบล็อคอินนั้นสามารถทำได้ดังนี้

4.3.1 ขั้นตอนการล็อคอินบนเว็บไซต์ แบบบนเครื่องคอมพิวเตอร์ที่สามารถเชื่อถือได้ เป็นขั้นตอนการเข้าระบบที่ผู้ใช้งานมั่นใจว่าคอมพิวเตอร์มีความปลอดภัยในการใช้งานสูง อย่างเช่น คอมพิวเตอร์ส่วนตัวเป็นต้น ซึ่งในขั้นตอนการเข้าระบบมีต่อไปนี้

1. ผู้ใช้เปิดหน้าแรกของการล็อคอิน โดยเลือกรูปแบบการล็อคอินแบบบนเครื่องคอมพิวเตอร์ที่สามารถเชื่อถือได้ดังรูปที่ 4.10

รูปที่ 4.10 : การเลือกรูปแบบการล็อคอินแบบบนเครื่องคอมพิวเตอร์ที่สามารถเชื่อถือได้

2. เมื่อผู้ใช้เลือกรูปแบบแล้วนั้นจะปรากฏหน้าล็อคอิน โดยผู้ใช้สามารถป้อนชื่อผู้ใช้และรหัสผ่านที่ได้สมัครสมาชิกไว้ ลงในช่องว่าง ดังรูปที่ 4.11 และกดปุ่ม “ลงชื่อเข้าใช้งาน”



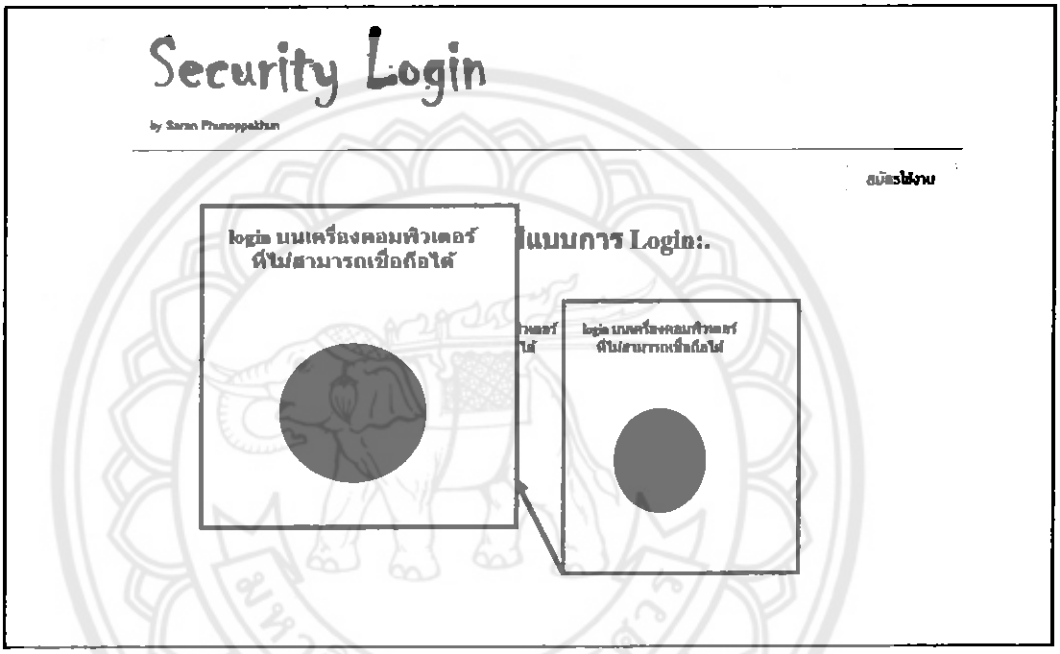
รูปที่ 4.11 : การกรอกข้อมูลในหน้าลงทะเบียนเข้าสู่ระบบ

3. เมื่อผู้ใช้ ล็อคอินเข้าสู่ระบบแล้ว จะนำไปสู่หน้า “ยินดีต้อนรับเข้าสู่ระบบ” ดังรูปที่ 4.12

รูปที่ 4.12 : แสดงสถานะเมื่อมีการล็อคอินผ่าน

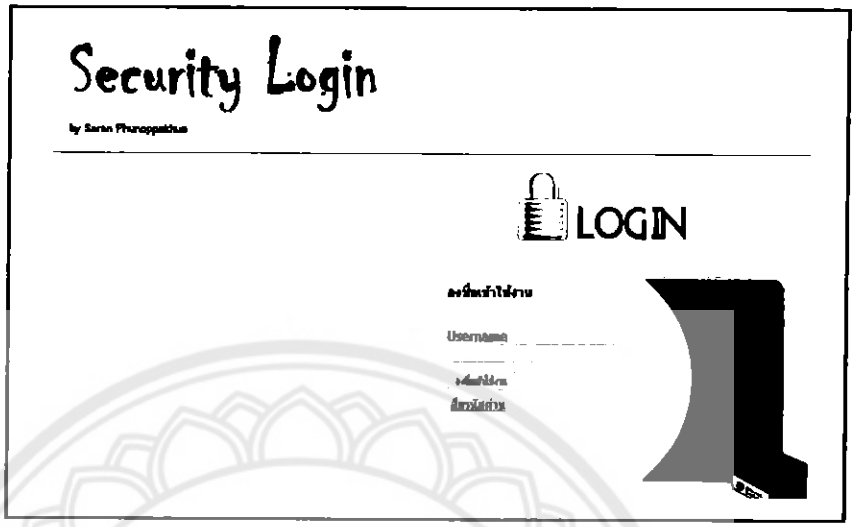
4.3.2 ขั้นตอนการ Login บนเว็บไซต์ แบบบนเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ (โดยการนำมือถือสมาร์ทโฟนเข้ามาช่วยในการล็อคอิน) ขั้นตอนการล็อคอินบนเว็บไซต์แบบปลอดภัย (โดยการนำมือถือสมาร์ทโฟนเข้ามาช่วยในการล็อคอิน) เป็นขั้นตอนการเข้าระบบที่ผู้ใช้ไม่สามารถใช้งานผ่านคอมพิวเตอร์สาธารณะได้ เช่น เครื่องคอมพิวเตอร์ร้านอินเตอร์เน็ตเป็นต้น ซึ่งในขั้นตอนการเข้าระบบมีต่อไปนี้

1. ผู้ใช้เปิดหน้าแรกของการล็อคอิน โดยเลือกรูปแบบการล็อคอิน แบบบนเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ดังรูปที่ 4.13



รูปที่ 4.13 : การเลือกรูปแบบการล็อคอินแบบบนเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้

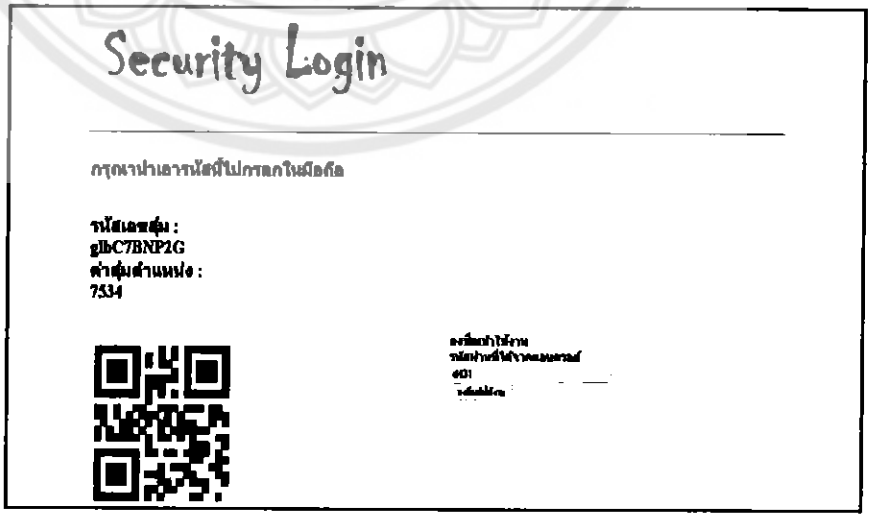
2. เมื่อผู้ใช้เลือกรูปแบบแล้วนั้นจะปรากฏหน้าล็อคอิน โดยผู้ใช้สามารถป้อนชื่อผู้ใช้งานที่ได้สมัครสมาชิกไว้ ลงในช่องว่าง และทำการกดปุ่ม "ลงชื่อเข้าใช้งาน" ดังรูปที่ 4.14



รูปที่ 4.14 : การกรอกข้อมูลในหน้าลงทะเบียนเข้าสู่ระบบ

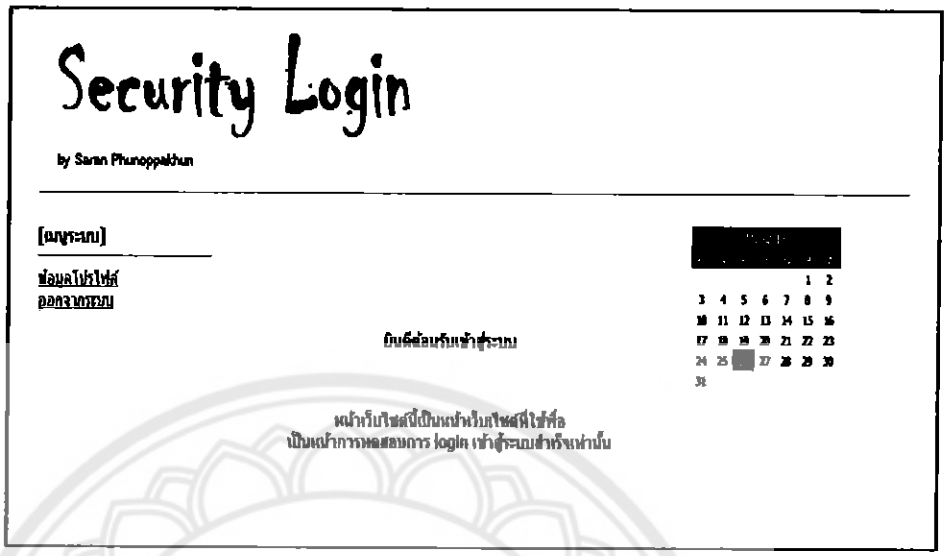
3. เมื่อผู้ใช้เข้าสู่ระบบโดยการกรอกชื่อผู้ใช้งานแล้วนั้นจะปรากฏ หน้าล็อคอินอีกหนึ่งชั้นเพื่อให้ผู้ใช้นำมือถือสมาร์ทโฟนที่มีแอพพลิเคชั่นแอนดรอยด์ของระบบที่ได้ดาวน์โหลดไว้บนมือถือครั้งเมื่อสมัครเข้าใช้งานนำมา Scan barcode หรือ ป้อนรหัสสุ่มที่ได้จากหน้าเว็บ นำมากรอกลงในช่องว่าง ดังรูปที่ 4.15

**หมายเหตุ (ขั้นตอนการใช้งานบนมือถือแอพพลิเคชั่นแอนดรอยด์จะพูดถึงในหัวข้อที่ 4.5 ต่อไป)



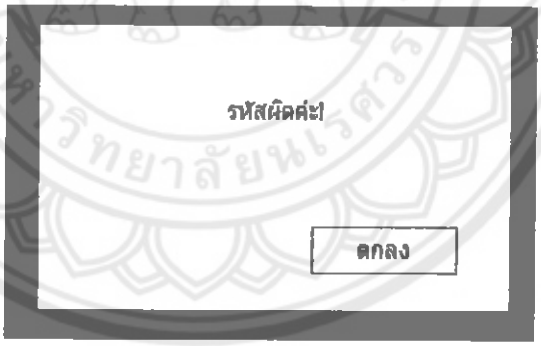
รูปที่ 4.15 : การกรอกข้อมูลโดยการนำมือถือสมาร์ทโฟนเข้ามาช่วยในการล็อคอิน

4. เมื่อผู้ใช้ ล็อคอิน เข้าสู่ระบบแล้ว จะนำไปสู่หน้า "ยินดีต้อนรับเข้าสู่ระบบ" ดังรูปที่ 4.16

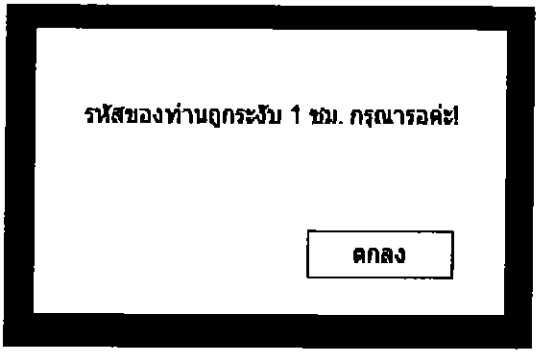


รูปที่ 4.16 : เมื่อทำการล็อคอินผ่าน

5. กรณีที่ผู้ใช้ใส่รหัสผิดที่ได้จากแอพพลิเคชั่นแอนดรอยด์ทางระบบแบบปลอดภัย จะทำการแจ้งเตือนดังรูปที่ 4.17 และเมื่อผู้ใช้กรอกรหัสผิดพลาดเกิน 3 ครั้งทางระบบจะแจ้งเตือนการถูกระงับใช้รหัสผ่าน ดังรูปที่ 4.18



รูปที่ 4.17 : การแจ้งเตือนเมื่อกรอกรหัสผิด

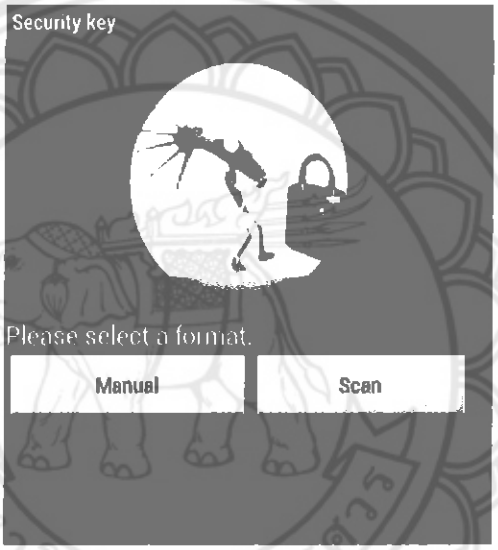


รูปที่ 4.18 : การแจ้งเตือนเมื่อกรอกรหัสผิดเกิน 3 ครั้ง

4.4 ขั้นตอนการใช้งานบนมือถือแอพพลิเคชั่นแอนดรอยด์

มือถือสมาร์ทโฟนที่เข้ามาช่วยในการล็อคอินเป็นโปรแกรมแอพพลิเคชั่นทำงานแบบออฟไลน์ซึ่งโปรแกรมนี้จะช่วยในการสร้าง Authorization Code เพื่อเป็น Key ในการเข้าสู่ระบบจึงทำให้ระบบมีความปลอดภัยมากยิ่งขึ้น โดยมีขั้นตอนและรูปแบบการใช้งานดังนี้

4.4.1 รูปแบบแอพพลิเคชั่นแอนดรอยด์ เป็นการสร้างหน้าแอพพลิเคชั่นทั่วไปในการใช้งานโดยให้ชื่อแอพพลิเคชั่น ว่า "Security Key" ซึ่งในหน้าแรกของแอพพลิเคชั่นจะบังคับเลือกว่าจะต้องการ Authorization เพื่อเป็น Key ในการเข้าสู่ระบบล็อคอินบนเว็บไซต์ในรูปแบบใด ดังรูปที่ 4.18



รูปที่ 4.19 : หน้าแรกของแอพพลิเคชั่นแอนดรอยด์

4.4.2 ขั้นตอนการใช้งานแบบ Manual

ขั้นตอนนี้เป็นขั้นตอนที่ผู้ใช้งานจะต้อง Key Password หรือรหัสเลขสุ่ม ที่ได้จากหน้าเว็บไซต์นำมากรอกในแอพพลิเคชั่น โดยผู้ใช้เอง มีขั้นตอนดังนี้

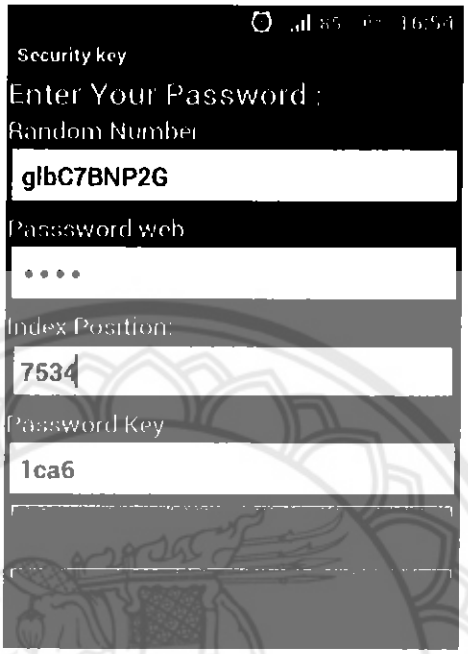
1. ผู้ใช้เปิดหน้าแรกของการแอพพลิเคชั่นแอนดรอยด์ โดยเลือกรูปแบบการ Authorization แบบ Manual ดังรูปที่ 4.20

รูปที่ 4.20 : การเลือกรูปแบบ Authorization แบบ Manual

2. เมื่อผู้ใช้ทำการเลือกรูปแบบแล้ว ผู้ใช้งานจะต้องนำ Key Password หรือรหัสเลขสุ่มที่ได้จากหน้าเว็บไซต์นำมากรอกในแอพพลิเคชั่น ในช่องว่างที่ชื่อ "Random Number" , "Password web" และกรอก "Index Position" ดังรูปที่ 4.21

รูปที่ 4.21 : แสดงการกรอกรหัส "Random Number" , "Index Position" และ "Password web"

3. เมื่อผู้ใช้ กรอกรหัส "Random Number" , "Password web" และ "Index Position" แล้วก็ทำการกดปุ่ม "Submit" ก็จะได้รหัส "Password Key" ดังรูปที่ 4.22 เพื่อนำไปกรอกที่หน้าเว็บไซต์ต่อไป

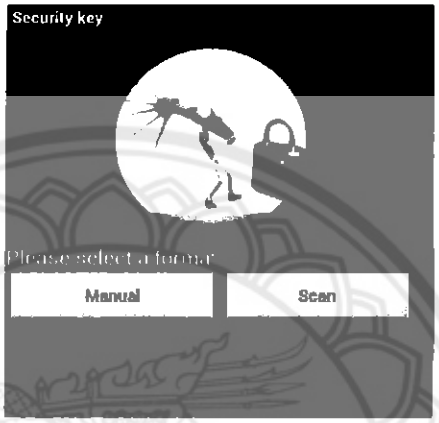


รูปที่ 4.22 : แสดงการกดปุ่ม Submit เมื่อทำการกรอกรหัสครบทุกช่อง

4.4.3 ขั้นตอนการใช้งานแบบ Scan

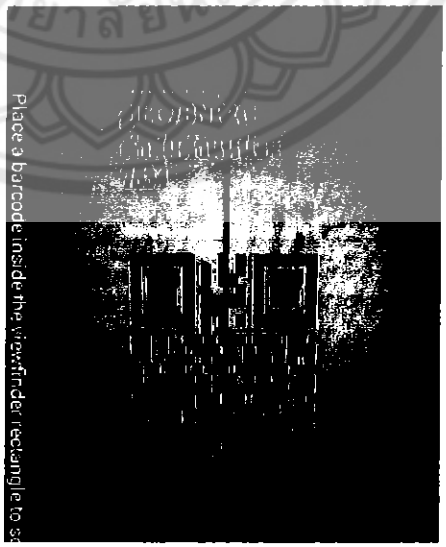
ขั้นตอนนี้เป็นขั้นตอนที่ช่วยอำนวยความสะดวกกับผู้ใช้ โดยที่ไม่ต้องกรอกรหัสในส่วนของ "Random Number" เองเพียงแต่กรอกในช่องของ "Password web" เท่านั้น โดยมีขั้นตอนการทำงานดังต่อไปนี้

1. ผู้ใช้เปิดหน้าแรกของการแอพพลิเคชั่นแอนดรอยด์ โดยเลือกรูปแบบการ Authorization แบบ Scan ดังรูปที่ 4.23



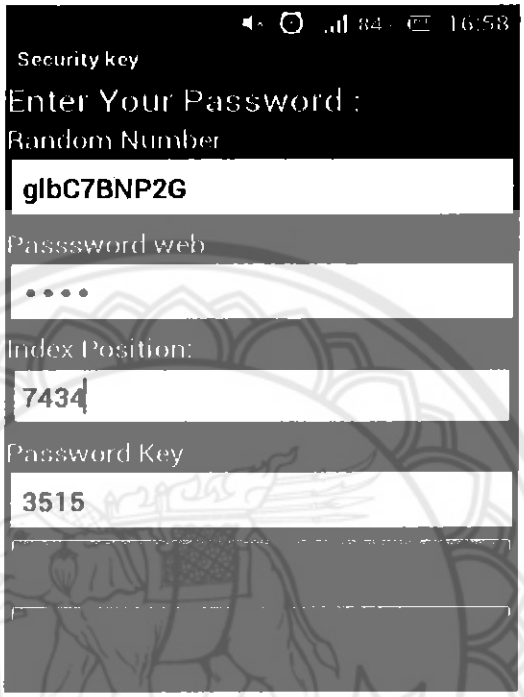
รูปที่ 4.23 : การเลือกรูปแบบ Authorization แบบ Scan

2. เมื่อผู้ใช้กดปุ่ม Scan ระบบจะเข้าสู่โหมด Scan barcode โดยผู้ใช้จะต้องนำมือถือไป Scan barcode ที่หน้าเว็บไซต์ ดังรูปที่ 4.24



รูปที่ 4.24 : การแสดง Scan barcode บนมือถือสมาร์ทโฟน

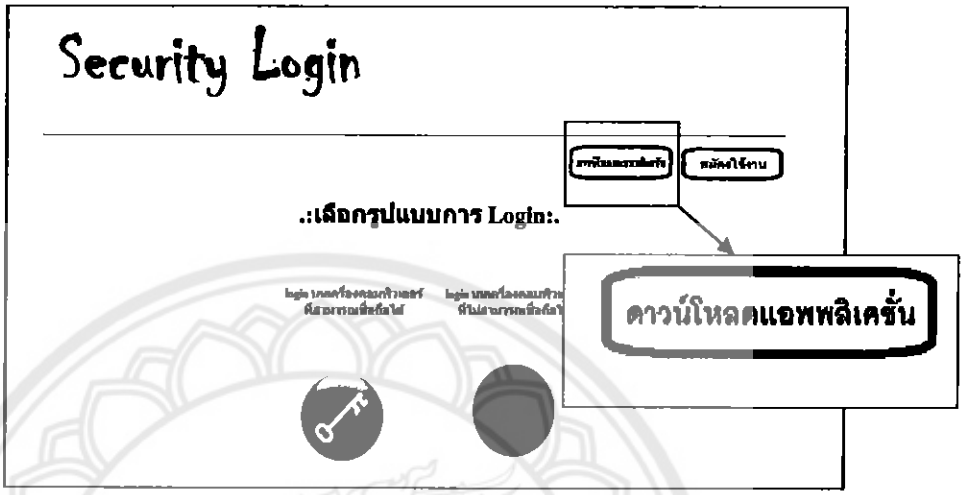
3. เมื่อทำการ Scan barcode แล้วนั้นผู้ใช้ก็ทำการกรอกรหัส "Password web" ที่ได้จากการสมัครเข้าใช้งานในครั้งแรก จากนั้นกรอกเลขสุ่มตำแหน่งที่ช่อง " Index Position" และทำการกดปุ่ม "Submit" เพื่อนำ "Password Key" ที่ได้ดังรูปที่ 4.25 เพื่อนำไปกรอกที่หน้าเว็บไซต์ต่อไป



รูปที่ 4.25 : แสดงการกรอก "Password web" และกดปุ่ม Submit

4.4.4 ขั้นตอนการดาวน์โหลดแอพพลิเคชั่นแอนดรอยด์

การดาวน์โหลดแอพพลิเคชั่นแอนดรอยด์ ทางผู้จัดทำได้อำนวยความสะดวกไว้ให้ผู้ผู้ใช้ไว้ที่หน้าแรกของเว็บไซต์ ดังรูปที่ 4.26



รูปที่ 4.26 : รูปปุ่มดาวน์โหลดแอพพลิเคชั่น

เมื่อทำการกดปุ่มดาวน์โหลดแอพพลิเคชั่นแล้วจะมีรูป QR Code ขึ้นมา ดังรูปที่ 4.27 นำมือถือสมาร์ทโฟนมาถ่ายรูป QR Code ก็จะสามารถติดตั้งแอพพลิเคชั่นลงมือถือได้อย่างสะดวก โดยที่ไม่ต้องเข้าไปโหลดใน Play สโตร์ ของระบบแอนดรอยด์

รูปที่ 4.27 : รูปแสดงการ Scan QR code เพื่อดาวน์โหลดแอพพลิเคชั่น

4.5 การทดลองและวิเคราะห์ความปลอดภัยของระบบ

ในส่วนการทดลองและวิเคราะห์ระบบความปลอดภัยของระบบ ทางผู้พัฒนาได้ทำการแบ่งการทดลองออกเป็นกรณีต่าง ๆ ดังนี้

4.5.1 กรณีที่ 1 Brute force attack

กรณี Brute orce attack เป็นกรณีที่ Attacker รู้ชื่อผู้ใช้ , รหัสผ่านและตัวเลขสุ่มที่ใช้เพียงครั้งเดียว ซึ่ง Attacker ต้องการนำมาถอดรหัสเพื่อให้ได้รหัสผ่านที่แท้จริง การที่ Attacker จะสามารถถอดรหัสผ่านที่แท้จริงได้นั้น โดยทำการคำนวณความน่าจะเป็น

อักษรภาษาอังกฤษตัวพิมพ์ใหญ่	26	ตัวอักษร
อักษรภาษาอังกฤษตัวพิมพ์เล็ก	26	ตัวอักษร
ตัวเลข 0-9	10	ตัวอักษร

ดังนั้นกรณีที่รหัสผ่าน 8 หลัก search space เท่ากับ $\frac{1}{62^8}$ หรือ $\frac{1}{218,340,105,584,896}$ และความน่าจะเป็นที่ Attacker จะสามารถถอดรหัสได้เป็น $\frac{1}{62^8 \div 2}$ หรือ $\frac{1}{109,170,052,792,448}$ กรณีซึ่ง การที่ Attacker จะสามารถถอดรหัสได้ ยาก-ง่าย เพียงใดนั้นยังขึ้นอยู่กับผู้ใช้ว่าตั้งรหัสผ่านอย่างไร

4.5.2 กรณีที่ 2 Replay attack

กรณีที่มีโปรแกรมดักจับรหัสผ่านถูกติดตั้งอยู่ในเครื่องทางผู้พัฒนาเองได้คำถึงความปลอดภัยในส่วนนี้ กล่าวคือ ได้มีการจัดทำแอพพลิเคชั่นเพื่อเป็นตัวช่วยในการสร้างรหัสที่ใช้ได้เพียงครั้งเดียว โดยการนำรหัสผ่านและรหัสที่ได้จากหน้าเว็บใส่ในแอพพลิเคชั่นเพื่อทำการสร้างรหัสผ่านขึ้น ทั้งนี้รหัสผ่านที่ได้นั้นจะมีการเปลี่ยนแปลงไปทุกครั้งของการใช้งาน

ดังนั้นในกรณีที่ถูกโปรแกรมดักจับรหัสผ่านไปได้นั้น จะมีการสุ่มตัวเลขที่มีมีจำนวน 10 หลัก ซึ่งความเป็นไปได้ในการนำรหัสนั้นกลับมาใช้อีกครั้งเท่ากับ

$\frac{1}{62^8}$ หรือ $\frac{1}{839,299,365,868,340,224}$

บทที่ 5
บทสรุปและข้อเสนอแนะ

โครงงานนี้พัฒนาขึ้นเพื่อให้สามารถใช้งานคอมพิวเตอร์สาธาณะหรือคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้ได้อย่างปลอดภัยมากยิ่งขึ้น โดยการนำเทคโนโลยีอุปกรณ์อัจริยะ เช่น โทรศัพท์สมาร์ทโฟนมาเป็นเป็นตัวช่วยในการสร้างรหัสผ่านที่ใช้เพียงครั้งเดียว ซึ่งในบทนี้เป็นการสรุปผลการดำเนินงาน และข้อเสนอแนะต่าง ๆ เพื่อเป็นแนวทางในการพัฒนาสำหรับผู้ที่สนใจต่อไป

5.1 วิเคราะห์ระบบและผลการทดลอง

เนื่องจากกลุ่มผู้พัฒนาระบบเล็งเห็นว่าการยืนยันตัวตนโดยการล็อคอินในปัจจุบันที่ใช้เฉพาะการใส่ยูสเซอร์เนมและพาสเวิร์ดเท่านั้น ยังไม่มีความปลอดภัยมากพอสำหรับการเก็บข้อมูลของผู้ใช้ เพราะถ้าใช้ในกรณีที่ใช้เครื่องคอมพิวเตอร์สาธารณะที่ไม่สามารถเชื่อถือได้ อาจมีโปรแกรมต่าง ๆ เช่น โปรแกรมคีย์ล็อคเกอร์ที่สามารถดักจับพาสเวิร์ดของผู้ใช้ โดยที่อาจถูกติดตั้งไว้โดยที่ผู้ใช้ไม่รู้และก่อให้เกิดความเสียหายต่อผู้ใช้ได้

ทางด้านผู้พัฒนาจึงทำการออกแบบระบบ ล็อคอิน ขึ้นมาใหม่ โดยเน้นให้มีความปลอดภัยแก่ผู้ใช้มากยิ่งขึ้น โดยการนำแอพพลิเคชันแอนดรอยด์ บนโทรศัพท์มือถือสมาร์ทโฟนมาเป็นตัวช่วยในการล็อคอินโดยให้ผู้ใช้สามารถใส่ พาสเวิร์ด ที่ได้จากการสมัครพร้อมกับเลขสุ่มที่ได้จากหน้าเว็บไซต์ ใส่ลงไปในแอพพลิเคชันแอนดรอยด์ แล้วทำการเข้ารหัสเพื่อหลีกเลี่ยงการใส่ พาสเวิร์ด ผ่านเครื่องคอมพิวเตอร์ที่ไม่น่าเชื่อถือโดยตรง และป้องกันการล่วงรู้ พาสเวิร์ด จากผู้ไม่พึงประสงค์ได้โดยง่าย

จากการทดลองระบบที่ใช้พัฒนาขึ้นมานั้นสามารถกล่าวได้ว่า ระบบล็อคอินที่พัฒนาขึ้นมานั้นช่วยให้ความปลอดภัยในการยืนยันตัวตนของผู้ใช้มีมากยิ่งขึ้น และสามารถนำความสามารถของมือถือสมาร์ทโฟนในปัจจุบันนำมาใช้งานในเรื่องของการยให้เกิดประโยชน์ได้สูงสุด

5.2 สรุปผลการทำงานของระบบ

โครงงานนี้เกิดขึ้นจากการที่คณะผู้จัดทำเล็งเห็นว่าระบบการยืนยันตัวตนโดยการล็อคอินแบบเดิมมีความปลอดภัยไม่มากพอจึงมีแนวคิดที่จะพัฒนาระบบการยืนยันตัวตนโดยการล็อคอินให้มีความปลอดภัยเพิ่มมากยิ่งขึ้น

การเข้าถึงข้อมูลที่สำคัญโดยการใช้ยูสเซอร์เนมและพาสเวิร์ดเพียงอย่างเดียว มีความปลอดภัยไม่มากพอสำหรับการรักษาความปลอดภัยของข้อมูลที่สำคัญ คณะผู้จัดทำจึงได้พัฒนารูปแบบของระบบการ ล็อคอิน ขึ้นมาใหม่เพื่อเพิ่มความปลอดภัยของผู้ใช้ให้มีประสิทธิภาพเพิ่มมากยิ่งขึ้น โดยการนำโทรศัพท์มือถือสมาร์ทโฟนระบบ แอนดรอยด์ มาเป็นตัวช่วยในการล็อคอิน ซึ่งมีวิธีการและขั้นตอนดังนี้ คือ เมื่อผู้ใช้มีต้องการเข้าถึงข้อมูล จะต้องทำการกรอกยูสเซอร์เนม เพื่อเป็นการตรวจสอบว่าได้เป็นสมาชิกอยู่หรือไม่ ถ้าตรวจสอบแล้วว่าเป็นสมาชิกจะสามารถเข้าไปยังส่วนถัดไป คือ นำรหัสที่ได้จากหน้าเว็บไซต์ไปกรอกบน แอพพลิเคชัน บนโทรศัพท์ พร้อมใส่ พาสเวิร์ดที่ได้จากการสมัครใช้งานเว็บไซต์ในครั้งแรก เพื่อให้แอพพลิเคชันนำค่าที่ได้ไปเข้ารหัสแบบ SHA1 แล้วนำรหัสที่ได้ไปกรอกในเว็บไซต์ ถ้ารหัสถูกต้องก็จะสามารถเข้าถึงข้อมูลได้ต่อไป

จากขั้นตอนของระบบที่คณะผู้จัดทำได้พัฒนาดังกล่าวมาแล้ว สามารถช่วยให้การเข้าถึงข้อมูลมีความปลอดภัยมากยิ่งขึ้น เนื่องด้วยการที่มีระบบความปลอดภัยที่ซับซ้อนมากยิ่งขึ้น และหลีกเลี่ยงการกรอกรหัสผ่านเข้าไปบนเว็บโดยตรง จึงทำให้รหัสผ่านปลอดภัยจากโปรแกรมที่ไม่ปลอดภัยที่เราไม่รู้ที่ถูกติดตั้งอยู่ในเครื่องคอมพิวเตอร์สาธารณะ เช่น โปรแกรมคีย์ล็อคเกอร์และช่วยให้ความปลอดภัยในการใช้ระบบของผู้ใช้มีความปลอดภัยมากยิ่งขึ้น

5.3 การเปรียบเทียบระบบล็อคอิน

การล็อกอินในปัจจุบันเป็นการล็อกอินที่มีความซับซ้อนในการล็อกอินข้อนข้างน้อย เนื่องจากเป็นเพียงการใช้ ยูสเซอร์เนมและพาสเวิร์ดในการล็อกอินเท่านั้น แต่ระบบที่ถูกพัฒนาขึ้นมานี้ได้มีการนำเทคโนโลยีโทรศัพท์สมาร์ทโฟนมาเป็นตัวช่วยในการล็อกอิน เพื่อเพิ่มความซับซ้อนและความปลอดภัยให้กับระบบอีกขั้นหนึ่ง เพราะผู้ใช้ที่ต้องการเข้าสู้ระบบนอกจะจะต้องรู้ พาสเวิร์ด ในขั้นตอนการสมัครแล้วยังจำเป็นต้องมีโทรศัพท์สมาร์ทโฟน เพื่อเป็นตัวช่วยในการสร้างรหัสที่ใช้งานเพียงครั้งเดียวที่จะนำไปใช้ในการล็อกอินแต่ละครั้ง ดังนั้น จะเห็นได้ว่าระบบที่ถูกพัฒนาขึ้นมีความปลอดภัยมากกว่าระบบการล็อกอินแบบเก่า โดยการใช้โทรศัพท์สมาร์ทโฟนเป็นตัวช่วย และการใช้รหัสที่ใช้งานเพียงครั้งเดียวที่จะมีการเปลี่ยนทุก ๆ ครั้งที่ผู้ใช้จะเข้าระบบ

ตารางที่ 5.1 : การเปรียบเทียบการทำงานของระบบล็อคอิน

หัวข้อ	Two-Step Verification	MP-Auth	KM-Auth*
ต้องมีการส่ง SMS จาก Sever	✓	×	×
แก้ปัญหา Key-logging	✓	✓	✓
แอพพลิเคชั่นมีการทำงานแบบออฟไลน์	×	×	✓
ต้องมีการเชื่อมต่อกับคอมพิวเตอร์	×	✓	×
ใช้งานบนอุปกรณ์อัจฉริยะอื่นได้	✓	×**	✓
สามารถแก้ปัญหา Phishing ได้	✓	✓	✓

หมายเหตุ :

* KM-Auth คือ ชื่อโครงงาน "การใช้งานสมาร์ทโฟนช่วยยืนยันตัวตนผ่านเครื่องคอมพิวเตอร์ที่ไม่สามารถเชื่อถือได้"

** ใช้งานบนอุปกรณ์อัจฉริยะอื่นได้ เนื่องจากวิธีการแบบ MP-Auth จำเป็นต้องใช้บลูทูธ (Bluetooth) ในการติดต่อกับคอมพิวเตอร์ จึงเป็นข้อจำกัดในการใช้งาน

5.4 ปัญหาและอุปสรรคที่พบ

1. ผู้พัฒนามีความรู้ในเรื่องการเขียนโปรแกรมภาษา PHP ไม่มากนัก จึงต้องใช้เวลาในการศึกษามากพอสมควร

2. เนื่องจากโครงงานเป็นเรื่องเกี่ยวกับความปลอดภัย ซึ่งมีความซับซ้อน จึงต้องใช้เวลาในการออกแบบรูปแบบระบบความปลอดภัยมากพอสมควร

5.5 ข้อเสนอแนะ

1. นำโปรโตคอล SSL มาใช้ เพื่อให้การรับส่งข้อมูลมีความปลอดภัยมากยิ่งขึ้น
2. พัฒนาให้ใช้ได้กับโทรศัพท์ระบบอื่นนอกจากระบบแอนดรอยด์
3. พัฒนาในส่วนการจัดการผู้ใช้ เช่น กรณีลืมพาสเวิร์ดให้ทำการรีเซ็ทพาสเวิร์ดผ่านทางอีเมล์
4. ประยุกต์ระบบให้กับอัลกอริทึมตัวใหม่ๆ เพื่อให้มีความปลอดภัยมากยิ่งขึ้น

5.6 ปัญหาและอุปสรรคที่พบ

1. ก่อนดำเนินงาน ควรศึกษาข้อมูลให้เข้าใจมากที่สุด เพื่อลดข้อผิดพลาดและระยะเวลาในการทำงาน

2. ควรศึกษาภาษาที่ใช้ในการพัฒนาโครงงานให้มีความรู้ความชำนาญในการใช้งาน เพื่อความรวดเร็วและง่ายต่อการทำงาน

เอกสารอ้างอิง

[1] สิริพร จิตต์เจริญธรรม , เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล. **"ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน"** [Online]. www.thaicert.org/paper/authen/authentication_guide.php 2547.

[2] **Code ฟังก์ชัน sha1** http://computer.todaygoods.com/php/sha1.html **(สืบค้นเมื่อเดือน มีนาคม พ.ศ. 2556)**

[3] ธำรงรัตน์ อมรรักษา. **"ความปลอดภัยของข้อมูลสำหรับการสื่อสารสื่อประสม: จากทฤษฎีสู่การปฏิบัติ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี"**. 27 เมษายน 2553 [สืบค้น 27 เมษายน 2555];
สืบค้นจาก : http://www.bcoms.net/system_analysis/index.aspoption=com_rokdownloads&view

[4] คำสั่งการสร้าง QR code สืบค้นเมื่อเดือน มีนาคม พ.ศ. 2556) :
http://qrserver.com/api/documentation/create-qr-code/#general_directive

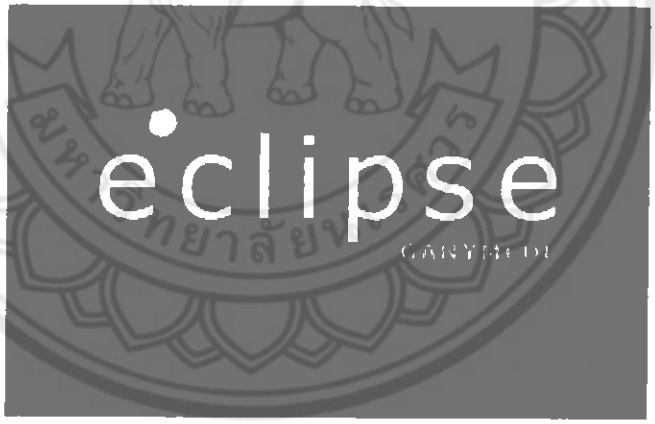
[5] ดร.จักรชัย โสอินทร์. พงษ์ศธร จันทร์ยอย. **Basic Android App Development. พิมพ์ครั้งที่ 1 . นนทบุรี. สำนักพิมพ์ไอดีซี. 2554**

[6] สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. แนะนำเทคโนโลยีบาร์โค้ด :
[สืบค้น 15 มีนาคม 2555]; สืบค้นจาก : http://www.nstda.or.th/nstda-knowledge/2866-2d-barcode

[7] ระบบTwo Factor Authentication
[สืบค้น 1 เมษายน 2556]; สืบค้นจาก :: http://en.wikipedia.org/wiki/Two-factor_authentication

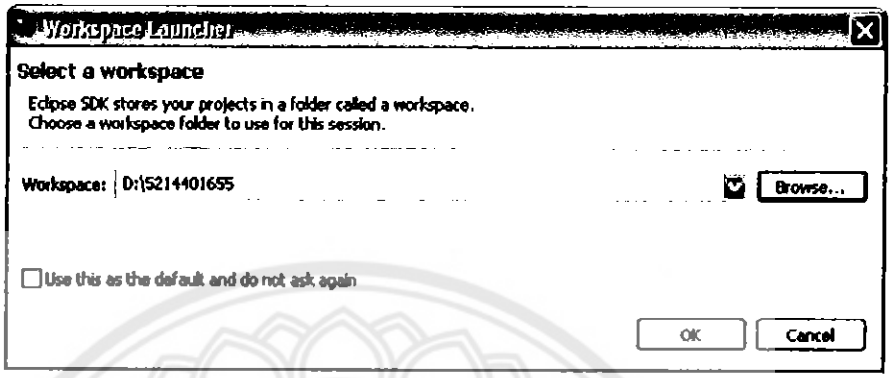
ภาคผนวก ก
การติดตั้งโปรแกรม Eclipse 3.4.2

1. Download และติดตั้ง Sun JDK หรือJRE1.5 หรือสูงกว่า
2. เข้าไปที่ Web Site ของ Eclipse เพื่อ Download Eclipse SDK สำหรับ Windows 32 หรือ 64 บิต เมื่อทำการ Download เสร็จสิ้นแล้ว จะได้ไฟล์ eclipse-SDK-3.4.2-win32.zip (152MB)
3. ทำการ Unzip ไฟล์ eclipse-SDK-3.4.2-win32.zip ลงใน Directory ที่ต้องการ เช่น D:\ เมื่อทำการแตกไฟล์เรียบร้อยแล้ว จะปรากฏ Directory ชื่อว่า eclipse สร้างขึ้นใน Directory ที่แตกไฟล์นั้น อย่างเช่น D:\ Directory ไฟล์ของโปรแกรม Eclipse จะถูกเก็บอยู่ใน Directory Eclipse
4. ทำการรันโปรแกรม Eclipse โดย Double Cilck ที่ไฟล์ eclipse.exe ซึ่งอยู่ใน Directory Eclipse ดังรูป ก-1



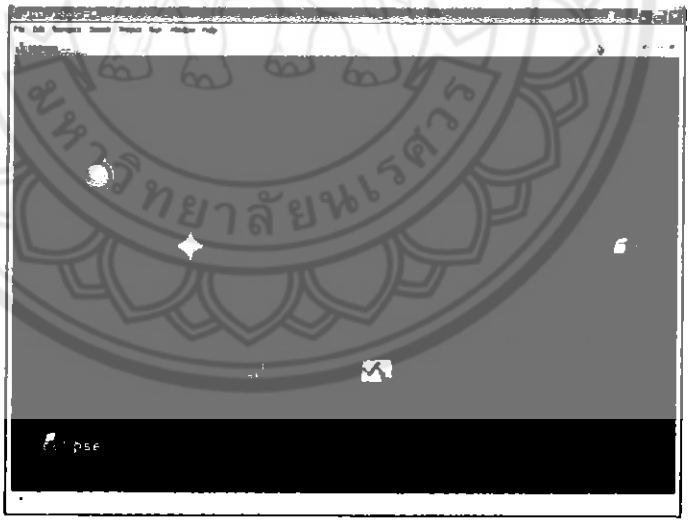
ดังรูป ก-1 แสดงการรันโปรแกรม Eclipse

5. เมื่อทำการรันโปรแกรม Eclipse ขึ้นมาใช้งาน โปรแกรมจะให้เลือก Path สำหรับเก็บ Workspace Project ต่างๆ ที่ใช้งาน โดยให้เลือก Path ตามที่ต้องการ อย่างเช่น d:\5214401655 ดังรูป ก-2



รูปที่ ก-2 การเลือก Path สำหรับเก็บ Workspace Project

6. จากนั้นโปรแกรมจะแสดงหน้าจอ Welcome เพื่อแนะนำการใช้งาน Eclipse พื้นฐานดังรูปที่ ก-3



รูปที่ ก-3 หน้าจอแรกของโปรแกรม Eclipse

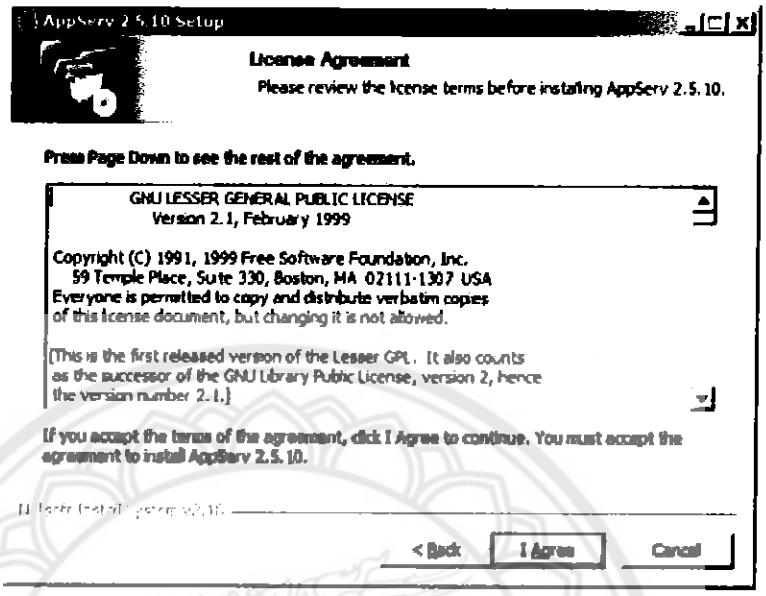
ภาคผนวก ข

การติดตั้งโปรแกรม Appserv 2.5.10 เพื่อจำลองเว็บเซิร์ฟเวอร์ (Web Server)

1. ทำการ Download โปรแกรม Appserv 2.5.10 แล้วทำการ Double Cilck ที่ไฟล์ติดตั้ง จะปรากฏดังรูปที่ ข-1

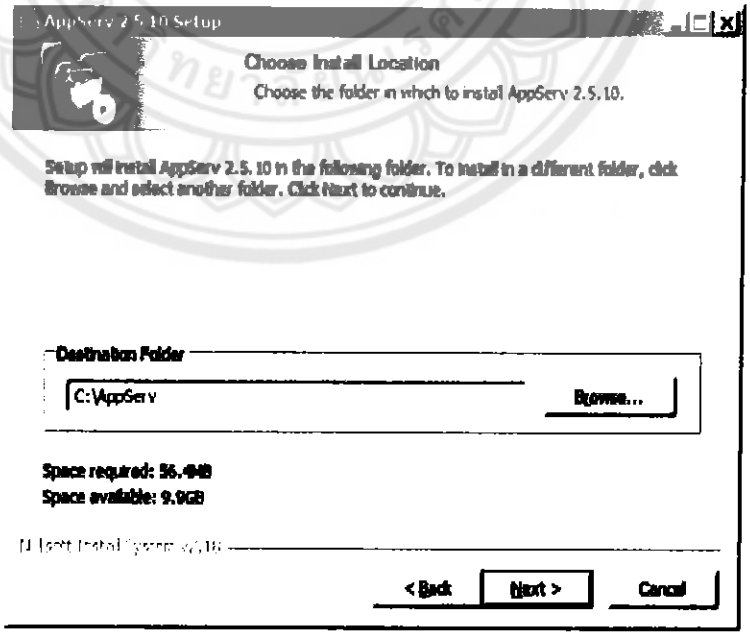
รูปที่ ข-1 เมื่อทำการติดตั้งจะมีหน้าจอต้อนรับของโปรแกรม

2. คลิก Next จะพบหน้าจอ ประกาศเรื่องลิขสิทธิ์ ซึ่งเป็นลิขสิทธิ์แบบ GNU/GPI L License ดังรูปที่ ข-2



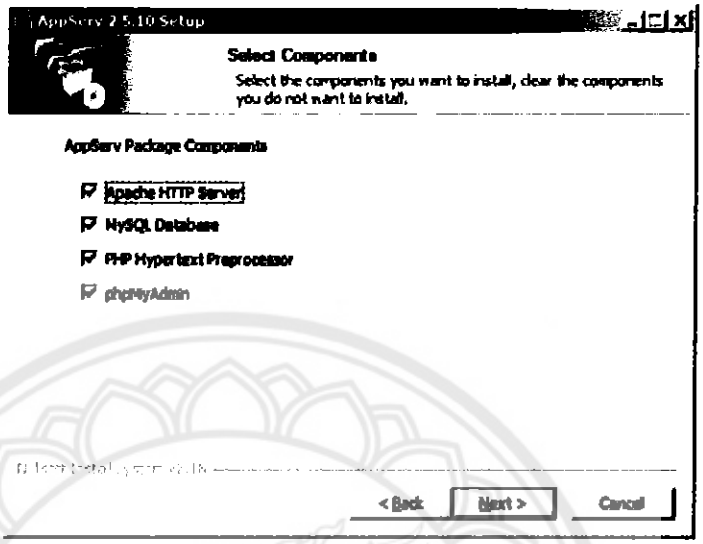
รูปที่ ข-2 แสดงหน้าประกาศลิขสิทธิ์ GNU/GPL License

3. ทำการคลิก I Agree เพื่อยอมรับสิทธิ์ในการใช้งาน จะทำให้เข้าสู่หน้าเลือกโฟลเดอร์ และไดร์ฟ ที่จะทำการติดตั้ง ในที่นี้เป็น C:\AppServ ดังรูปที่ ข-3



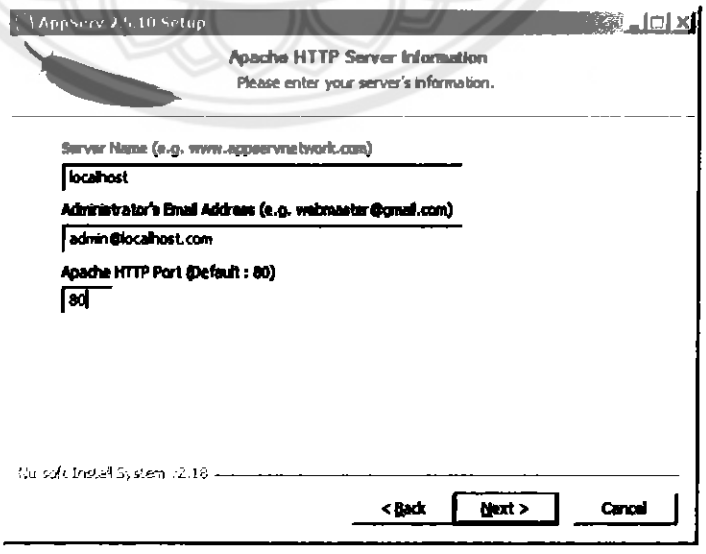
รูปที่ ข-3 เลือกโฟลเดอร์ที่จะทำการติดตั้ง

4. เมื่อทำการเลือกโฟลเดอร์ที่ติดตั้งแล้ว คลิ๊ก Next จะเข้าสู่หน้าเลือก Components แล้วคลิกเลือกให้หมดทุกตัว ดังรูปที่ ข-4



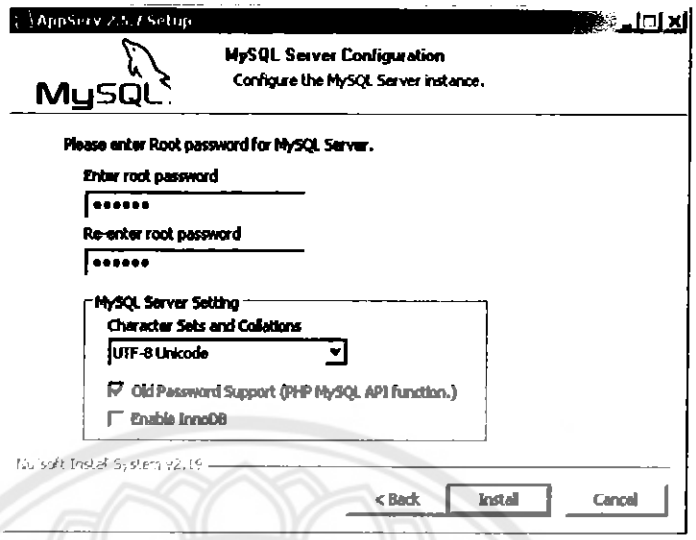
รูปที่ ข-4 ขั้นตอนการเลือก Components ที่จะทำการติดตั้ง

5. เมื่อทำการเลือก Components แล้วจะกด Next จะพบหน้า Sever Information กรอกข้อมูล ดังรูปที่ ข-5
   - ช่อง Server Name ให้ใส่ localhost
   - ช่อง Admin Email ให้ใส่ email ของผู้ใช้
   - ช่อง HTTP Post ให้ใส่หมายเลข Port ในที่นี้แนะนำเป็น 80



รูปที่ ข-5 Sever Information

6. ทำการตั้งค่า MySQL ดังรูปที่ ข-6

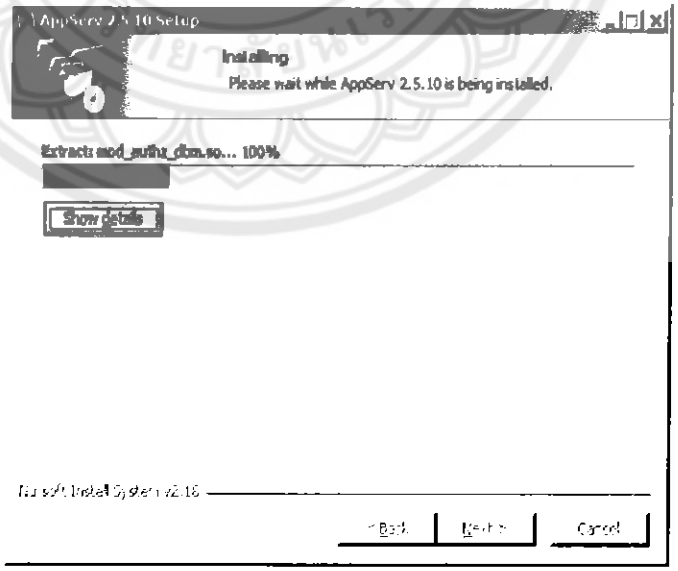


รูปที่ ข-6 การตั้งค่า MySQL

หมายเหตุ

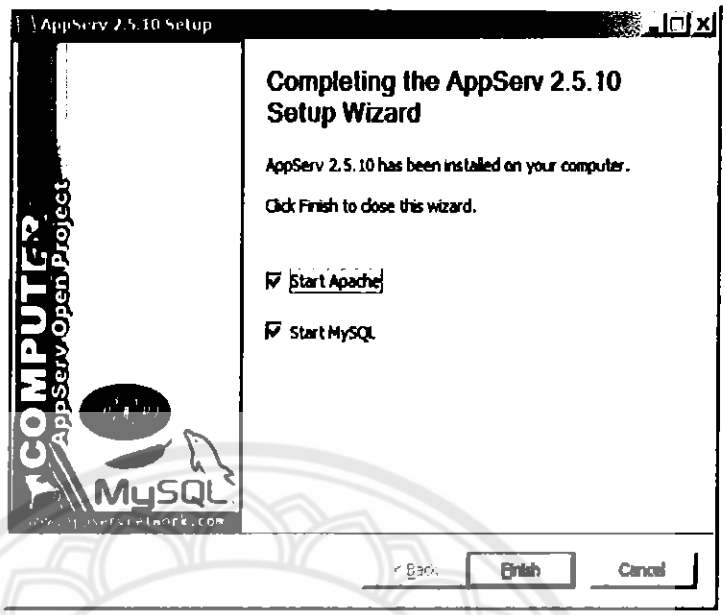
- ช่อง Enter Root Password ใส่รหัสผ่าน "root"
- ช่อง Re-Enter Root Password ใส่ "root" อีกครั้ง
- ช่อง Character Sets เลือกเป็น UTF-8

7. เมื่อทำการตั้งค่า MySQL เรียบร้อยแล้ว จากนั้นรอโปรแกรมติดตั้งจนเสร็จสิ้นดังรูปที่ ข-7



รูปที่ ข-7 ติดตั้งโปรแกรม

8. เมื่อทำการติดตั้งเรียบร้อยแล้วให้กดปุ่ม Finish ดังรูปที่ ข-8



รูปที่ ข-8 ขั้นตอนสุดท้ายของการติดตั้ง

ภาคผนวก ค

Source Code ของเว็บไซต์

ชุดโค้ดส่วนหนึ่งใน login_sec2.php

```
$pwd = $_SESSION['session_pwd'];
$rd_char = $_SESSION['rd_char'];
$tfPassword=$_POST['tfPassword'];
//นำ ตัวเลขสุ่ม 10 หลักและพาสเวิดที่ได้จากตอนสมัครเข้ารหัสด้วย sha1
$outpwd= sha1($rd_char.$pwd);
        $index1=rand(1,10);      //random ค่าตั้งแต่ตัวที่ 1-10
        $_SESSION['index1']=$index1;
        $index2=rand(11,20);     //random ค่าตั้งแต่ตัวที่ 11-20
        $_SESSION['index2']=$index2;
        $index3=rand(21,30);     //random ค่าตั้งแต่ตัวที่ 21-30
        $_SESSION['index3']=$index3;
        $index4=rand(31,40);     //random ค่าตั้งแต่ตัวที่ 31-40
        $_SESSION['index4']=$index4;
            // นำค่าที่ได้จากข้างต้นมาลบด้วยตัวเลขตั้งต้นเพื่อนำค่าที่ได้ไปกำหนดตำแหน่ง
        $index1b=$index1-1;
        $_SESSION['index1b']=$index1b;
        $index2b=$index2-11;
        $_SESSION['index2b']=$index2b;
        $index3b=$index3-21;
        $_SESSION['index3b']=$index3b;
        $index4b=$index4-31;
        $_SESSION['index4b']=$index4b;
            //แสดงตำแหน่งของรหัสผ่านเพื่อให้ผู้ใช้นำไปกรอกใส่มือถือ
        $outpwd1=$index1b.$index2b.$index3b.$index4b;
        echo "<br />";
        echo $outpwd1;
```

ชุดโค้ดส่วนหนึ่งใน checklogin2.php

```
$pwd = $_SESSION['session_pwd'];
 $api_id = $_SESSION['session_apiuser'];
 $rd_char = $_SESSION['rd_char'];
 $tfPassword=$_POST['tfPassword'];
 $outpwd=sha1($rd_char.$pwd);
$index1=$_SESSION['index1'];
$index2=$_SESSION['index2'];
$index3=$_SESSION['index3'];
$index4=$_SESSION['index4'];
$index1b=$_SESSION['index1b'];
$index2b=$_SESSION['index2b'];
$index3b=$_SESSION['index3b'];
$index4b=$_SESSION['index4b'];
// password ที่ใช้สำหรับการเช็คว่าตรงกับรหัสที่ผู้ใช้กรอกหรือไม่
$outpwd2=$outpwd[$index1b].$outpwd[$index2b].$outpwd[$index3b].$outpwd[$index4b];
// ถ้า password ที่ผู้ใช้กรอกตรงกับ password ของ sever จะสามารถ login ได้ และเข้าสู่หน้า
home.php
if($tfPassword==$outpwd2){
        require_once('config.php');
        mysql_connect($v_hostname,$v_username,$v_password);
        $sql = "UPDATE `db_ass`.`tbl_apiuser` SET loginfailed='0', hcanlogin='' WHERE
api_id='$api_id';";
        $result = mysql_db_query($v_database,$sql);
        echo "<script langquage='javascript'>";
        echo "window.location='home.php';";
        echo "</script>";
}else{  //ถ้าใส่รหัสผิดจะมีการแจ้งว่า "รหัสผิดครับ!" ถ้าผิดเกิน 3 ครั้งจะถูกระงับใช้งาน 1 ชม.
        require_once('config.php');
        mysql_connect($v_hostname,$v_username,$v_password);
        $sql = "SELECT  * FROM `db_ass`.`tbl_apiuser` WHERE api_id='$api_id';";
```

```
$result = mysql_db_query($v_database,$sql);
$numrows=mysql_num_rows($result);
if($numrows>0){
        $resultoutput = mysql_fetch_array($result);
                $loginfailed=$resultoutput['loginfailed'];
        if($loginfailed<"3")
        {
        $loginfailed=$loginfailed+1;
        $dt=date('h')+1;
        $sql2 = "UPDATE `db_ass`.`tbl_apiuser` SET loginfailed='$loginfailed',
hcanlogin='$dt' WHERE api_id='$api_id';";
        $result2 = mysql_db_query($v_database,$sql2);
        echo "<script langquage='javascript'>";
        echo "alert('รหัสผิดครับ!');";
        echo "</script>";
        echo "<script langquage='javascript'>";
        echo "window.location='login_sec2.php';";
        echo "</script>";
                }else{
        echo "<script langquage='javascript'>";
        echo "alert('รหัสผิดเกิน 3 ครั้ง คุณสามารถเข้าใช้งานได้อีก 3 ชมถัดไป!');";
                echo "</script>";
                echo "<script langquage='javascript'>";
                echo
"window.location='http://127.0.0.1/nuass.co.cc/';";
                echo "</script>";
        }
}
```

ภาคผนวก ง

Source Code Android

```
package com.mkyong.android;
import android.app.Activity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;
public class menu extends Activity
{

        private Button btManual;
        private Button btScan;
        private String          contents;       //ค่า fvRoomID ที่ได้จากการ ScanQR

        @Override
        public void onCreate(Bundle savedInstanceState) {
                super.onCreate(savedInstanceState);
                setContentView(R.layout.menu);

                btManual = (Button)findViewById(R.id.btManual);
                btManual.setOnClickListener(new OnClickListener() {
               public void onClick(View v) {
                        Intent goNext = new Intent(getApplicationContext(),
MyAndroidAppActivity.class);
                        //goNext.putExtra("contents", contents);
                        startActivity(goNext);
```

```
        }
        }

        btScan = (Button)findViewById(R.id.btScan);
        btScan.setOnClickListener(new OnClickListener() {
        public void onClick(View v) {
          // TODO Auto-generated method stub
          try {
            //กำหนด intent ในการเรียกใช้ Barcode Scanner
            Intent intent = new Intent("com.google.zxing.client.android.SCAN");
            //ส่ง Mode ในการ Scan ให้กับ โปรแกรม Barcode Scanner
            intent.putExtra("SCAN_MODE", "QR_CODE_MODE");
            //เริ่ม Activity จาก intent ที่กำหนด โดยกำหนด requestCode เป็น 0
            startActivityForResult(intent, 0);
          } catch (Exception e) {
            // TODO: handle exception
            //ถ้าไม่ได้ลงโปรแกรม Barcode Scanner ไว้จะแสดงข้อความ Please Install
Barcode Scanner
            Toast.makeText(getBaseContext(),"Please Install Barcode
Scanner",Toast.LENGTH_SHORT).show();
            }

        }
      });


    }
```

```
        @Override
    protected void onActivityResult(int requestCode, int resultCode, Intent intent) {
      // TODO Auto-generated method stub
      if (requestCode == 0) //ทำการตรวจสอบว่า requestCode ตรงกับที่ Barcode Scanner คืนค่ามา
หรือไม่
      {
        if (resultCode == RESULT_OK) //ถ้า Barcode Scanner ทำงานสมบูรณ์
        {
            //รับข้อมูลจาก Barcode Scanner ที่ได้จากการสแกน
            contents = intent.getStringExtra("SCAN_RESULT");
            //รับรูปแบบจาก Barcode Scanner ที่ได้จากการสแกน ว่าเป็นชนิดใด
            String format = intent.getStringExtra("SCAN_RESULT_FORMAT");
            //ทำการแสดงผลลัพธ์จากการแสกนใน classcheck
            //classCheck.setText("Check status at: " + contents);
          Intent goNext = new Intent(getApplicationContext(), MyAndroidAppActivity.class);
            goNext.putExtra("contents", contents);
            startActivityForResult(goNext,0);

        }
      }
    }
//End onActivityResult
}
```