ระบบควบคุมการใช้งานอุปกรณ์ ETOKEN ด้วยเทคโนโลยี GPS

CONTROL ETOKEN DEVICE USING SYSTEM WITH GPS

โดย

วัลลภ มั่นน้อย

WANLOP MUNNOI

อาจารย์ที่ปรึกษา

ดร.ปานวิทย์ ธุวะนุติ

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ 2
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 2 ปีการศึกษา 2556

CONTROL ETOKEN DEVICE USING SYSTEM WITH GPS

WANLOP MUNNOI

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE

REQUIREMENTS OF THE COURSE

INDEPENDENT STUDY 2

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT`S INSTITUTE OF TECHNOLOGY LADKRABANG

2 / 2013

ใบรับรองการศึกษาอิสระ 2 (Independent Study 2)

เรื่อง

ระบบควบคุมการใช้งานอุปกรณ์ ETOKEN ด้วยเทคโนโลยี GPS

CONTROL ETOKEN DEVICE USING SYSTEM WITH GPS

นายวัลลภ มั่นน้อย

รหัสประจำตัว 55661018

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาวิชาการศึกษาอิสระ

หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 2ปีการศึกษา 2556

..... อาจารย์ที่ปรึกษา

(ดร.ปานวิทย์ ธุวะนุติ)

..... กรรมการสอบ

(ผศ.ดร.กันต์พงษ์ วรรัตน์ปัญญา)

..... กรรมการสอบ

(ดร.นล เปรมัษเฐียร)

หัวข้อ	ระบบควบคุมการใช้อุปกรณ์ ETOKEN ด้วยเทคโนโลยี GPS
นักศึกษา	นายวัลลภ มั่นน้อย
รหัสนักศึกษา	55661018
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	เทคโนโลยีเครือข่ายและระบบ
ปีการศึกษา	2556
อาจารย์ที่ปรึกษา	ดร.ปานวิทย์ ธุวะนุติ

บทคัดย่อ

การใช้งานระบบเว็บแอพพลิเคชั่นในปัจจุบันนิยมใช้การยืนยันตัวบุคคลในการเข้าถึงข้อมูลในรูปแบบ 2 ระดับ (Two-Factor Authentication) ประกอบด้วย สิ่งที่คุณรู้ (Something you Know) และสิ่งที่คุณมี (Something you have) เพื่อเป็นการตรวจสอบ และเพิ่มความปลอดภัยในการเข้าใช้ระบบเว็บแอพพลิเคชั่น แต่ยังคงพบปัญหาที่ตามมา เนื่องจากสิ่งที่คุณมีนั้น ตัวอย่าง เช่น อุปกรณ์ eToken สามารถนำไปใช้งานที่ใดก็ได้ ทำให้ยากต่อการควบคุม และถูกปฏิเสธความรับผิดชอบจากผู้ใช้ ในงานวิจัยนี้ จึงวิเคราะห์จุดอ่อนดังกล่าว และได้ทำการออกแบบพร้อมพัฒนาระบบ เพื่อหาแนวทางการแก้ไขปัญหา โดยเพิ่มการยืนยันตัวตนในรูปแบบที่ 4 คือ พื้นที่ที่คุณอยู่ (Somewhere you are) เข้ามาใช้งานร่วมกับการยืนยันตัวตนแบบ 2 ระดับ ซึ่งจะอาศัยหลักการทำงานของเทคโนโลยี GPS ที่ติดตั้งมากับ Smart Phone ในการยืนยันพื้นที่ของผู้ใช้งานระบบเว็บแอพพลิเคชั่น ณ ปัจจุบัน ทำให้ขั้นตอนของการพิสูจน์ตัวตนมีความแข็งแรงมากขึ้น เพราะว่าสามารถระบุพื้นที่การใช้งานให้กับสิ่งที่คุณมีได้

Title	Control eToken device using system with GPS
Student	Mr.Wanlop Munnoi
Student ID	55661018
Degree	Master of Science
Program	Information Technology
Major	Network and System Technology
Academic Year	2013
Advisor	Dr. Panwit Tuwanut

ABSTRACT

The usage of web application nowadays often use two-factor authentication to access users information which are something you know and something you have, for verification and add more security into web application log in system. However, the problem could be found due to some information, for example eToken, can be used anywhere and makes it more difficult to control and have been denied from user responsibility. There for, this research's purpose is to analyses such weakness and implement the solution to solve the problem by adding the 4th person's verification which is somewhere you are into the system. The smartphone GPS technology will be introduced to verify the location of the users. This will strengthen the users verification system due to an ability to define the location of Something you have.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี ด้วยความกรุณาอย่างสูงจาก ดร.ปานวิทย์ ธุวะนุติ รับเป็นอาจารย์ที่ปรึกษาโครงงานการศึกษาอิสระ คอยให้คำปรึกษา แนะนำ ตลอดจนการแก้ไขข้อบกพร่องต่างๆ ด้วยความเอาใจใส่เป็นอย่างดี ผู้วิจัยรู้สึกซาบซึ้งในความกรุณาของอาจารย์ท่านนี้เป็นอย่างยิ่ง

ขอขอบคุณ นายกริส นาวานี กรรมการผู้จัดการ และพนักงาน บริษัท แบงคอคซิสเท็มแอนด์ซอฟแวร์ จำกัด ทุก ๆ ท่าน ที่ให้ความช่วยเหลือ ให้คำแนะนำ และเปิดโอกาศให้ได้ศึกษาเล่าเรียน

ขอขอบคุณช่วงเวลาที่ดีที่สุด ที่ได้มาศึกษา ณ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และได้พบมิตรภาพระหว่างรุ่นพี่ และรุ่นน้อง สิ่งที่ขาดไม่ได้คือเพื่อนร่วมชั้นเรียน ที่ร่วมทุก ร่วมสุขและคอยให้กำลังใจตลอดเสมอมา

ท้ายสุดขอกราบขอบพระคุณ คุณพ่อวิชาญ มั่นน้อย คุณแม่ผาสุข มั่นน้อยรวมถึงญาติสนิทมิตรสหายที่คอยช่วยเหลือและเป็นกำลังใจเสมอมา จนปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี และขอขอบคุณ ผู้มีพระคุณทุก ๆ ท่านเป็นอย่างสูงไว้ ณ โอกาสนี้

วัลลภ มั่นน้อย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

การพัฒนาระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS เป็นการพัฒนาระบบงานใหม่ เพื่อแก้ไขปัญหาที่เกิดจากการใช้งานอุปกรณ์ eToken ในปัจจุบันให้มีความปลอดภัยมากขึ้น ซึ่งสามารถแบ่งขั้นตอนการศึกษาเพื่อพัฒนาระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS โดยแบ่งหัวข้อต่าง ๆ ดังต่อไปนี้

1.1. ความเป็นมาและความสำคัญของปัญหา

1.2. วัตถุประสงค์ของโครงการ

1.3. ขอบเขตการศึกษาค้นคว้า

1.4. ผลที่คาดว่าจะได้รับ

1.1 ความเป็นมาและความสำคัญของปัญหา

eToken เป็นเทคโนโลยีสมาร์ทการ์ดที่สนับสนุนการยืนยันตัวตนแบบ 2 ระดับ โดยได้รับการรับรองมาตรฐานความปลอดภัยระดับสากล ทั้งในแบบการรักษาความปลอดภัย และการรักษาความเป็นส่วนบุคคล ซึ่ง สามารถจัดเก็บใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อนำไปใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งาน เช่น การยืนยันเข้าสู่คอมพิวเตอร์ผ่านระบบเครือข่าย (Network Logon) การลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signing) การเข้ารหัสถอดรหัสอีเมล์ (E-Mail Encryption) การยืนยันตัวตนเข้าสู่เว็บไซต์ (Secure web logon) และการยืนยันตัวตนเข้าสู่ระบบเครือข่ายเสมือน (Virtual Private Network) เป็นต้น

อุปกรณ์ eToken ไม่สามารถทำซ้ำหรือเลียนแบบได้ มีลักษณะภายนอกคล้ายกับอุปกรณ์จัดเก็บข้อมูล (Flash Drive) ซึ่งต่างจากอุปกรณ์ eToken ที่ไม่สามารถจัดเก็บข้อมูล แต่สามารถเก็บใบรับรองอิเล็กทรอนิกส์ได้ โดยใช้หลักการพิสูจน์ตัวตนคล้ายกับระบบธนาคารในการตรวจสอบผู้ใช้งานบัตร ATM ซึ่งปัจจุบันองค์กรทั้งภาครัฐและภาคเอกชนมีการนำอุปกรณ์ eToken เข้ามาใช้ในการพิสูจน์ตัวตน เพื่อเข้าใช้งานระบบต่าง ๆ แต่ระบบที่มีอยู่นั้นยังไม่ปลอดภัยเท่าที่ควร เนื่องจากระบบที่ใช้งานอยู่ในปัจจุบัน สามารถที่จะใช้งานผ่านระบบ จากภายในหรือภายนอกองค์กรก็ได้ ซึ่งทำให้เกิดปัญหาการควบคุมการใช้งานอุปกรณ์ eToken ภายนอกองค์กร ที่ไม่สามารถกำหนดพื้นที่การใช้งานได้ ทำให้เกิดความไม่ปลอดภัยของการใช้งานอุปกรณ์ eToken เพื่อเข้าระบบต่าง ๆ

ดังนั้นการติดตามจึงเป็นคำตอบของการแก้ไขปัญหานี้ ซึ่งสามารถทำการติดตามตรวจสอบตำแหน่งปัจจุบัน รวมถึงการกำหนดพื้นที่การใช้งานอุปกรณ์ eToken ได้ โดยใช้เทคโนโลยี GPS

(Global Positioning System) ร่วมกับระบบอินเตอร์เน็ต ทำให้ผู้ดูแลระบบสามารถควบคุมตำแหน่งปัจจุบันของอุปกรณ์ eToken ขณะเข้าใช้งานได้ทันที

1.2 วัตถุประสงค์ของโครงการ

วัตถุประสงค์ของโครงการศึกษาและพัฒนาระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS มีดังต่อไปนี้

1. เพื่อศึกษาหลักการทำงานและการใช้งานของระบบ GPS
2. เพื่อศึกษาการใช้งานและการประยุกต์ใช้งานวงจร GPS
3. เพื่อศึกษาการเขียน Application Android
4. เพื่อศึกษาวิธีการสื่อสารข้อมูลและการประมวลผลข้อมูล
5. เพื่อควบคุมการใช้งานอุปกรณ์ eToken ตามพื้นที่ ที่กำหนด
6. เพื่อเพิ่มความปลอดภัยการใช้งานอุปกรณ์ eToken

1.3 ขอบเขตการศึกษาค้นคว้า

การพัฒนาระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS มีเทคโนโลยีและเครื่องมือที่เกี่ยวข้อง คือ การประยุกต์ใช้งานอุปกรณ์ eToken กับเทคโนโลยี GPS การสื่อสารผ่านระบบดาวเทียม และการพัฒนาระบบสารสนเทศในลักษณะเว็บแอพพลิเคชั่น โดยมีขอบเขตการพัฒนาระบบ ดังต่อไปนี้

วิชาการศึกษาอิสระ 1

1. ศึกษารายละเอียดการเขียน Application Android และ GPS รวมถึงทฤษฎีที่เกี่ยวข้องกับการทำงาน
2. พัฒนาระบบการใช้งาน eToken โดยควบคุมด้วยตำแหน่ง GPS
3. พัฒนา Application Android ให้แสดงค่า GPS ออกทางหน้าจอของ Smartphone
4. พัฒนา Application Android ให้สามารถรับและส่งค่า GPS ไปยัง Server
5. พัฒนา Application Android ให้สามารถรับและส่งค่า Latitude, Longitude จาก Smartphone ผ่านเครือข่าย ไปยัง Server เพื่อเก็บลงฐานข้อมูล

วิชาการศึกษาอิสระ 2

1. พัฒนา Application Android ให้สามารถใช้ ชื่อและรหัสผ่านของผู้ใช้ในการยืนยันตัวตนผ่าน Application ที่ทำงานบน Smartphone
2. ศึกษาและพัฒนาฐานข้อมูลให้สามารถรองรับการเก็บข้อมูลจากเว็บแอพพลิเคชั่น

3. ศึกษาและพัฒนาเว็บแอพพลิเคชั่นสำหรับการจัดการกำหนดพื้นที่การใช้งานอุปกรณ์ eToken ด้วย GPS ตามขอบเขตของการศึกษาที่ได้ระบุไว้
4. ด้านการพัฒนาและการใช้งาน Android Application ประกอบด้วย 5 ส่วน
   - ระบบสามารถแสดงข้อมูลผู้ใช เช่น ชื่อ นามสกุล Device ของผู้ใช้งานเป็นต้น
   - ระบบสามารถแสดงพิกัดปัจจุบันของผู้ใช้งาน
   - ระบบสามารถส่งพิกัดไปยัง Server (กรณีที่หน้าเว็บรอการส่งพิกัด ผู้ใช้กำลังทำการยืนยันตัวตนผ่านหน้าเว็บ)
   - ระบบสามารถเปลี่ยนรหัสผ่านของผู้ใช้
   - ระบบสามารถส่ง E-Mail หรือ SMS เพื่อแจ้งพิกัดของตนไปยังผู้ดูแลระบบ
5. ด้านการพัฒนาและการใช้งาน Web Management (Back-Office) เป็นส่วนของผู้ดูแลระบบ
   - ผู้ดูแลระบบ มีเพียง 1 Role เท่านั้น
   - ระบบสามารถกำหนดพิกัด Default ได้
   - การตั้งค่าการใช้งานระบบ
     - ระบบสามารถกำหนดระยะในการรอการร้องขอพิกัดจาก Smartphone เช่น 1 นาที 2 นาที หรือมากกว่า
     - ระบบสามารถกำหนดรัศมีการยืนยันตัวตน เช่น 2 กิโลเมตร หรือ มากกว่า
     - ระบบสามารถลงทะเบียนการใช้งานอุปกรณ์ eToken โดยอาศัยข้อมูลที่สำคัญ ดังนี้ ข้อมูลผู้ใช้ และข้อมูล Device ID ของผู้ใช้
   - การจัดการข้อมูลผู้ใช้ เพิ่ม ลบ แก้ไข และสามารถจัดการข้อมูลต่าง ๆ ดังนี้
     - ระบบสามารถทำการ เพิ่ม ลบ และแก้ไข ข้อมูล Device ID
     - ระบบสามารถกำหนดพิกัดให้กับผู้ใช้นั้น ๆ (กรณีที่ผู้ใช้ไม่มีการกำหนดพิกัด ระบบจะนำค่าพิกัด Default มาใช้งานทันที)
     - ระบบสามารถตรวจสอบรายงานการยืนยันตัวตนของผู้ใช้ แบบรายวัน รายเดือน รายปี
6. ด้านการพัฒนาและการใช้งาน Web Service และ API (ส่วนที่ใช้ติดต่อระหว่าง Android กับ Server) ประกอบด้วย
   - Authentication API
   - Change Password API
   - API สำหรับการส่งพิกัด

7. ทำการปรับเปลี่ยนเพิ่มเติมหรือแก้ไขโครงงานตามความเหมาะสม เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ ซึ่งการเพิ่มเติมหรือการแก้ไขขึ้นอยู่ดุลพินิจของอาจารย์ที่ปรึกษา
8. ทำการทดสอบการใช้งานของระบบโดยรวม เพื่อหาจุดบกพร่องของระบบพร้อมทั้งกับการแก้ไขจุดบกพร่องที่เกิดขึ้น

1.4 ผลที่คาดว่าจะได้รับ

1. มีความรู้และความเข้าใจหลักการทำงานและการใช้งานของระบบ GPS
2. ได้เรียนรู้การใช้งานและการประยุกต์ใช้งาน GPS
3. มีความรู้และความเข้าใจในการเขียน Application Android และมีความเข้าใจวิธีการสื่อสารข้อมูลและการประมวลผลข้อมูล
4. สามารถควบคุมการใช้งานอุปกรณ์ eToken ตามพื้นที่ ที่กำหนด
5. สามารถค้นหาอุปกรณ์ eToken จากตำแหน่งที่ Smartphone อยู่
6. อุปกรณ์ eToken มีความปลอดภัยในการใช้งานเพิ่มขึ้น

บทที่ 2
ทฤษฎีและเทคโนโลยีที่เกี่ยวข้อง

ในการพัฒนาระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS ผู้พัฒนาได้ศึกษาค้นคว้าหลักการ ทฤษฎีและเทคโนโลยีต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาระบบ เพื่อให้สามารถนำมาประยุกต์ใช้งานและเป็นแนวทางในการพัฒนาระบบ โดยแบ่งหัวข้อต่าง ๆ ดังต่อไปนี้

2.1 ทฤษฎีที่เกี่ยวข้องในการพัฒนาระบบ

2.2 เทคโนโลยีที่เกี่ยวข้องในการพัฒนาระบบ

2.1 ทฤษฎีที่เกี่ยวข้องในการพัฒนาระบบ

ผู้พัฒนาได้ศึกษาทฤษฎีต่าง ๆ ที่เกี่ยวข้องเพื่อนำมาใช้ในการพัฒนาระบบร่วมกับฐานข้อมูล รวมถึงพิจารณาความต้องการของผู้ดูแลระบบ ซึ่งจากการศึกษาได้พบว่าสามารถนำภาษาพีเอชพี (PHP) มาใช้ในการพัฒนาระบบร่วมกับระบบจัดการฐานข้อมูลมายเอสคิวแอล (MySQL) ซึ่งเป็นดาต้าเบสเซิร์ฟเวอร์ โดยมีคุณสมบัติที่ดีเพียงพอในการตอบสนองความต้องการของผู้ใช้งาน

2.1.1 ภาษาพีเอชพี (PHP)

ภาษาพีเอชพี (PHP) เป็นภาษาประเภท Scripting Language คำสั่งต่าง ๆ จะเก็บอยู่ในไฟว์ที่เรียกว่า สคริปต์ (Scirp) โดยจะทำหน้าที่เป็นคำสั่งในการดึงข้อมูลจากฐานข้อมูลบน Server เพื่อให้แสดงผลผ่าน Web Brower และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปต์ เช่น JavaScript, Perl เป็นต้น ลักษณะของภาษาพีเอชพีที่แตกต่างจากภาษาสคริปต์แบบอื่น ๆ คือ ภาษาพีเอชพีได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ จึงกล่าวได้ว่าภาษาพีเอชพี เป็นภาษาที่เรียกว่า server-side หรือ HTML-embedded scripting language เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้น

เนื่องจากว่าภาษาพีเอชพีไม่ได้เป็นส่วนหนึ่งของตัว Web Server ดังนั้นถ้าจะใช้ ภาษาพีเอชพีก็จะต้องศึกษาก่อนว่า Web server นั้นสามารถใช้สคริปต์ของภาษาพีเอชพีได้หรือไม่ ยกตัวอย่าง เช่น ภาษาพีเอชพีสามารถใช้ได้กับ Apache Web Server และPersonal Web Server (PWP) สำหรับระบบปฏิบัติการ Windows 95/98/NT ในกรณีของ Apache สามารถใช้ภาษาพีเอชพีได้สองรูปแบบ คือ ในลักษณะของ CGI และ Apache Module ความแตกต่างอยู่ตรงที่ว่า ถ้าใช้ภาษาพีเอชพีเป็นแบบโมดูล ซึ่งภาษาพีเอชพีจะเป็นส่วนหนึ่งของ Apache หรือเป็นส่วนขยายในการทำงานนั่นเอง ซึ่งจะทำงานได้เร็วกว่าแบบที่เป็น CGI เพราะว่า ถ้าเป็น CGI แล้ว ตัวแปลชุดคำสั่งของภาษาพีเอชพี ถือว่า

เป็นแค่โปรแกรมภายนอก ซึ่ง Apache จะต้องเรียกขึ้นมาทำงานทุกครั้งเมื่อต้องการใช้คำสั่งของภาษาพีเอชพี ดังนั้นถ้ามองในเรื่องของประสิทธิภาพในการทำงาน การใช้ภาษาพีเอชพี แบบที่เป็นโมดูลหนึ่งของ Apache จะทำงานได้มีประสิทธิภาพมากกว่า

2.1.1.1 ลักษณะเด่นของภาษาพีเอชพี

- พีเอชพีเป็นภาษาที่มีขีดความสามารถไม่จำกัด
- พีเอชพีสามารถทำงานบนระบบปฏิบัติการต่าง ๆ ได้ เช่น ระบบปฏิบัติการ Unix ระบบปฏิบัติการ Linux และระบบปฏิบัติการ Windows เป็นต้น
- ภาษาพีเอชพีสามารถใช้งานร่วมกับภาษา XML ได้ เนื่องจากภาษาพีเอชพีสามารถฝังเข้าไปใน HTML ใช้โครงสร้างและไวยากรณ์ภาษาง่าย ๆ
- มีการประมวลผลที่เร็วและมีประสิทธิภาพ
- สามารถใช้กับระบบแฟ้มข้อมูลได้
- สามารถใช้งานกับโครงสร้างข้อมูลได้หลายแบบ
- สามารถใช้กับการประมวลผลภาพได้

2.1.1.2 ความเป็นมาของภาษาพีเอชพี (PHP Hypretext Preprocess)

ภาษาพีเอชพีเกิดในปี 1994 โดย Rasmus Lerdorf โปรแกรมเมอร์ชาวสหรัฐอเมริกาได้คิดค้นสร้างเครื่องมือที่ใช้ในการพัฒนาเว็บส่วนตัวของเขา โดยใช้ข้อดีของภาษา C และ Perl เรียกว่า Personal Home Page และได้สร้างส่วนติดต่อกับฐานข้อมูลชื่อว่า Form Interpreter (FI) รวมทั้งสองส่วน เรียกว่า PHP/FI ซึ่งก็เป็นจุดเริ่มต้นของภาษาพีเอชพีมีคนที่เข้ามาเยี่ยมชมเว็บไซต์ของเขาแล้วเกิดความสนใจจึงติดต่อขอเอาโค้ดไปใช้บ้าง และนำไปพัฒนาต่อ ในลักษณะของ Open Source ภายหลังมีความนิยมขึ้นเป็นอย่างมากภายใน 3 ปี มีเว็บไซต์ที่ใช้ ภาษา PHP/FI ในการติดต่อฐานข้อมูลและแสดงผลแบบ ไดนามิคและอื่นๆ มากกว่า 50,000 เว็บไซต์ ทำให้ช่วงเวลาดังกล่าวมีผู้สนใจภาษา PHP/FI เป็นจำนวนมาก

พีเอชพีเป็นภาษาสคริปต์ที่ประมวลผลที่ฝั่งเซิร์ฟเวอร์ แล้วส่งผลลัพธ์ไปแสดงผลที่ฝั่งไคลเอ็นต์ผ่านเว็บบราวเซอร์ เช่นเดียวกับ CGI และ ASP ต่อมาเมื่อมีผู้ใช้มากขึ้นจึงมีการร้องขอให้มีการพัฒนาประสิทธิภาพของ PHP/FI ให้สูงขึ้น Rasmus Lerdorf ได้นำผู้ช่วยพัฒนาเพิ่มอีก 2 ท่าน คือ Zeev Suraski และ Andi Gutmans ชาวอิสราเอล ซึ่งปรับปรุงโค้ดของ Lerdorf ใหม่โดยใช้ C++ ต่อมาก็มีเพิ่มเข้ามาอีก 3 ท่าน คือ Stig Bakken รับผิดชอบความสามารถในการติดต่อ Oracle ท่านที่ 2 คือ Shane Caraveo รับผิดชอบดูแล PHP บน Window 9x/NT, และ ท่านที่ 3 คือ Jim Winstead รับผิดชอบการตรวจหาขอบกพร่องต่างๆ และได้เปลี่ยนชื่อเป็น PHP (Professional Home Page)

พีเอชพี 3 ได้ออกสู่สายตาของนักพัฒนา เมื่อเดือนมิถุนายน 1998 ที่ผ่านมาในเวอร์ชั่นนี้มีคุณสมบัติเด่นคือสนับสนุนระบบปฏิบัติการทั้ง Window 95/98/ME/NT, Linux และเว็บเซร์ฟเวอร์อย่าง IIS, PWS, Apache, OmniHTTPd สนับสนุน ระบบฐานข้อมูลได้หลายรูปแบบเช่น SQL Server, MySQL, mSQL, Oracle, Informix, ODBC

ซึ่งเวอร์ชั่นล่าสุดในปัจจุบันคือ PHP5 (เวอร์ชั่น 6 อยู่ในช่วงของการพัฒนา) ซึ่งได้เพิ่ม Functions การทำงานในด้านต่างๆให้ใช้งานได้มากและง่ายขึ้นโดย Zend ซึ่งมี Zeev และ Andi Gutmans ได้ร่วมกันก่อตั้งขึ้น ในเวอร์ชั่นนี้จะเป็น compile script ซึ่งในเวอร์ชั่นหน้านี้จะเป็น embed script interpreter ในปัจจุบันมีคนใช้ PHP สูงกว่า 5,100,000 sites แล้วทั่วโลก ผู้พัฒนาได้ตั้งชื่อของง PHP ใหม่ว่า PHP: Hypertext Preprocessor ซึ่งหมายถึงมีประสิทธิภาพระดับโปรเฟสเซอร์สำหรับไฮเปอร์เท็กซ์ ความสามารถของ PHP นั้นในความสามารถพื้นฐานที่ภาษาสคริปต์ทั่ว ๆ ไปมีนั้น PHP ก็มีความสามารถทำได้ทัดเทียมเช่นเดียวกัน ตัวอย่าง เช่น การรับข้อมูลจากฟอร์ม การสร้าง Content ในลักษณะ Dynamic รับส่ง Cookies สร้าง เปิด อ่าน และปิดไฟล์ในระบบ การรองรับระบบจัดการฐานข้อมูลได้แสดงในตารางที่ 2.1ดังนี้

ตารางที่ 2.1 ประเภทระบบจัดการฐานข้อมูล

ประเภทระบบจัดการฐานข้อมูล			
Adabas D	Dbase	Direct MS-SQL	Empress
FilePro (Read-Only)	FrontBase	Hyperware	IBM DB2
Informix	Ingres	mSQL	MySQL
ODBC	Oracle	Ovrimos	PostgreSQL
Solid	Sybase	Unix dbm	Velocis

แต่ตัวจัดการฐานข้อมูลที่ทาง NINETO E-MAGAZINE ONLINE เลือกมาใช้ในบทความนี้คือ MySQL เหตุที่เลือกตัวนี้คือ เป็นที่นิยมกว้างขว้างและประเด็นหนึ่งที่จะต้องพิจารณา คือ ไม่เสียค่าใช้จ่ายแต่อย่างใด เพราะ MySQL จัดเป็น Software ประเภท Freeware รองรับ OS ได้หลายระบบด้วยกัน ท่านสามารถดาวน์โหลดได้ที่หน้า Download ซึ่งผู้พัฒนาได้จัดเตรียมไว้ให้แล้ว Protocol Support ความสามารถในการรองรับโปรโตคอลหลายแบบทั้ง IMAP, SNMP, NNTP, POP3, HTTP และยังมีไลบารีสำหรับติดต่อ กับแอพพลิเคชั่นได้มากมาย มีความยืดหยุ่นสูงสามารถนำไปสร้างแอพพลิเคชั่นได้หลากหลาย และข้อดีอีกข้อหนึ่งที่โดดเด่นของ PHP ก็คือสามารถแทรกลงในแท็ก HTML ในตำแหน่งใดก็ได้

2.1.1.3 ความต้องการของภาษาพีเอชพีต้องมีอะไรบ้าง

เนื่องจากว่า PHP ไม่ได้เป็นส่วนหนึ่งของ Web Server ดังนั้นถ้าจะใช้ พีเอชพี ก็จะต้องศึกษาก่อนว่า Web server นั้น สามารถใช้สคริปต์ PHP ได้หรือไม่ ยกตัวอย่าง เช่น PHP สามารถใช้ได้กับ Apache WebServer และ Personal Web Server (PWP) สำหรับระบบปฏิบัติการ Windows 95/98/NT ในกรณีของ Apache เราสามารถใช้ PHP ได้สองรูปแบบ คือ ในลักษณะของ CGI และ Apache Module ความแตกต่างอยู่ตรงที่ว่า ถ้าใช้ PHP เป็นแบบโมดูล PHP จะเป็นส่วนหนึ่งของ Apache หรือเป็นส่วนขยายในการทำงานนั่นเอง ซึ่งจะทำงานได้เร็วกว่าแบบที่เป็น CGI เพราะว่า ถ้าเป็น CGI แล้ว ตัวแปลชุดคำสั่งของ PHP ถือว่าเป็นแค่โปรแกรมภายนอก ซึ่ง Apache จะต้องเรียกขึ้นมาทำงานทุกครั้ง ที่ต้องการใช้ PHP ดังนั้น ถ้ามองในเรื่องของประสิทธิภาพในการทำงาน การใช้ PHP แบบที่เป็นโมดูลหนึ่งของ Apache จะทำงานได้มีประสิทธิภาพมากกว่า

2.1.1.4 รูปแบบการเขียนโค้ดภาษาพีเอชพี

การเขียนโค้ด เราสามารถเขียนได้จากโปรแกรม Editor ทั่วไป เช่น Notepad หรือ Editplus แน่นอนที่สะดวกที่สุดคงจะไม่พ้น Notepad เพราะแถมมากับ window อยู่แล้ว แต่ถ้าต้องการความสามารถและทางเลือกที่เพิ่มขึ้นก็แนะนำว่าโปรแกรม Editplus ใช้ได้ดีทีเดียว รูปแบบการเขียน PHP เขียนได้ 4 แบบดังตัวอย่าง ที่นิยมคือแบบที่ 1 และ 2 แบบที่ 3 ใช้งานคล้ายกับ Java script ส่วนแบบที่ 4 ตัว tag <% จะเหมือนกับ ASP โดยเมื่อรันจะได้ผลลัพธ์เหมือนกัน และสามารถแทรกลงในส่วนของภาษา HTML ส่วนใดก็ได้

2.1.2 ความรู้ทั่วไปเกี่ยวกับฐานข้อมูล

ข้อมูลเป็นการจัดเก็บข้อมูลอย่างเป็นระบบ ทำให้ผู้ใช้สามารถใช้ข้อมูลที่เกี่ยวข้องในระบบงานต่าง ๆ ร่วมกันได้ โดยที่จะไม่เกิดความซ้ำซ้อนของข้อมูล และยังสามารถหลีกเลี่ยงความขัดแย้งของข้อมูลด้วย อีกทั้งข้อมูลในระบบก็จะถูกต้องเชื่อถือได้ และเป็นมาตรฐานเดียวกัน โดยจะมีการกำหนดระบบความปลอดภัยของข้อมูลขึ้นนับได้ว่าปัจจุบันเป็นยุคของสารสนเทศ เป็นที่ยอมรับกันว่า สารสนเทศเป็นข้อมูลที่ผ่านการกลั่นกรองอย่างเหมาะสม สามารถนำมาใช้ประโยชน์อย่างมากมาย ไม่ว่าจะเป็นการนำมาใช้งานด้านธุรกิจ การบริหาร และกิจการอื่น ๆ องค์กรที่มีข้อมูลปริมาณมาก ๆ จะพบความยุ่งยากลำบากในการจัดเก็บข้อมูล ตลอดจนการนำข้อมูลที่ต้องการออกมาใช้ให้ทันต่อเหตุการณ์ ดังนั้นคอมพิวเตอร์จึงถูกนำมาใช้เป็นเครื่องมือช่วยในการจัดเก็บข้อมูล การประมวลผลข้อมูล ซึ่งทำให้ระบบการจัดเก็บข้อมูลเป็นไปได้สะดวก ทั้งนี้โปรแกรมแต่ละโปรแกรมจะต้องสร้างวิธีควบคุมและจัดการกับข้อมูลขึ้นเอง ฐานข้อมูลจึงเข้ามามีบทบาทสำคัญอย่างมาก โดยเฉพาะระบบงานต่าง ๆ ที่ใช้คอมพิวเตอร์ การออกแบบและพัฒนาระบบฐานข้อมูล

จึงต้องคำนึงถึงการควบคุมและการจัดการความถูกต้องตลอดจนประสิทธิภาพในการเรียกใช้ข้อมูลอีกด้วย

2.1.2.1 ความหมายของระบบฐานข้อมูล

ฐานข้อมูล (Database) หมายถึง กลุ่มของข้อมูลที่ถูกเก็บรวบรวมไว้ โดยมีความสัมพันธ์ซึ่งกันและกัน โดยไม่ได้บังคับว่าข้อมูลทั้งหมดนี้จะต้องเก็บไว้ในแฟ้มข้อมูลเดียวกันหรือแยกเก็บหลาย ๆ แฟ้มข้อมูล นั่นก็คือการเก็บข้อมูลในฐานข้อมูลนั้นเราอาจจะเก็บทั้งฐานข้อมูล โดยใช้แฟ้มข้อมูลเพียงแฟ้มข้อมูลเดียวกันได้ หรือจะเก็บไว้ในหลาย ๆ แฟ้มข้อมูล ที่สำคัญคือจะต้องสร้างความสัมพันธ์ระหว่างระเบียนและเรียกใช้ความสัมพันธ์นั้นได้ มีการกำจัดความซ้ำซ้อนของข้อมูลออกและเก็บแฟ้มข้อมูลเหล่านี้ไว้ที่ศูนย์กลาง เพื่อที่จะนำข้อมูลเหล่านี้มาใช้ร่วมกัน ควบคุมดูแลรักษาเมื่อผู้ต้องการใช้งานและผู้มีสิทธิ์จะใช้ข้อมูลนั้นสามารถดึงข้อมูลที่ต้องการออกไปใช้ได้ ข้อมูลบางส่วนอาจใช้ร่วมกับผู้อื่นได้ แต่บางส่วนผู้มีสิทธิ์เท่านั้นจึงจะสามารถใช้ได้ โดยทั่วไปองค์กรต่าง ๆ จะสร้างฐานข้อมูลไว้ เพื่อเก็บข้อมูลต่าง ๆ ของตัวองค์กร โดยเฉพาะอย่างยิ่งข้อมูลในเชิงธุรกิจ เช่น ข้อมูลของลูกค้า ข้อมูลของสินค้า ข้อมูลของลูกจ้าง และการจ้างงาน เป็นต้น การควบคุมดูแลการใช้ฐานข้อมูลนั้น เป็นเรื่องที่ยุ่งยากกว่าการใช้แฟ้มข้อมูลมาก เพราะเราจะต้องตัดสินใจว่าโครงสร้างในการจัดเก็บข้อมูลควรจะเป็นเช่นไร การเขียนโปรแกรมเพื่อสร้างและเรียกใช้ข้อมูลจากโครงสร้างเหล่านี้ ถ้าโปรแกรมเหล่านี้เกิดทำงานผิดพลาดขึ้นมา ก็จะเกิดความเสียหายต่อโครงสร้างของข้อมูลทั้งหมดได้ เพื่อเป็นการลดสภาวะการทำงานของผู้ใช้ จึงได้มีส่วนของฮาร์ดแวร์และโปรแกรมต่าง ๆ ที่สามารถเข้าถึงและจัดการข้อมูลในฐานข้อมูลนั้น เรียกว่าระบบจัดการฐานข้อมูล หรือ DBMS (Data base management system) ระบบจัดการฐานข้อมูล คือซอฟต์แวร์ที่เปรียบเสมือนสื่อกลางระหว่างผู้ใช้และโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับการใช้ฐานข้อมูล ซึ่งมีหน้าที่ช่วยให้ผู้ใช้เข้าถึงข้อมูลได้ง่ายสะดวกและมีประสิทธิภาพ การเข้าถึงข้อมูลของผู้ใช้อาจเป็นการสร้างฐานข้อมูล การแก้ไขฐานข้อมูล หรือการตั้งคำถามเพื่อให้ข้อมูลมา โดยผู้ใช้ไม่จำเป็นต้องรับรู้เกี่ยวกับรายละเอียดภายในโครงสร้างของฐานข้อมูล เปรียบเสมือนเป็นสื่อกลางระหว่างผู้ใช้และโปรแกรมต่าง ๆ ที่เกี่ยวข้องกับการใช้ฐานข้อมูล

2.1.2.2 ความสำคัญของระบบฐานข้อมูล

การจัดข้อมูลให้เป็นระบบฐานข้อมูลทำให้ข้อมูลมีส่วนดีกว่าการเก็บข้อมูลในรูปของแฟ้มข้อมูล เพราะการจัดเก็บข้อมูลในระบบฐานข้อมูล จะมีส่วนที่สำคัญกว่าการจัดเก็บข้อมูลในรูปของแฟ้มข้อมูลดังนี้

1. รักษาความถูกต้องของข้อมูล เนื่องจากฐานข้อมูลมีเพียงฐานข้อมูลเดียว ในกรณีที่มีข้อมูลชุดเดียวกันปรากฏอยู่หลายแห่งในฐานข้อมูล ข้อมูลเหล่านี้จะต้องตรงกัน ถ้ามีการแก้ไขข้อมูลนี้ทุก ๆ แห่งที่ข้อมูลปรากฏอยู่จะแก้ไขให้ถูกต้องตามกันหมดโดยอัตโนมัติด้วยระบบจัดการฐานข้อมูล

2. การป้องกันและรักษาความปลอดภัยให้กับข้อมูลทำได้อย่างสะดวก การป้องกันและรักษาความปลอดภัยกับข้อมูลระบบฐานข้อมูลจะให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้นจึงจะมีสิทธิ์เข้าไปใช้ฐานข้อมูลได้เรียกว่ามีสิทธิส่วนบุคคล (privacy) ซึ่งก่อให้เกิดความปลอดภัย (security) ของข้อมูลด้วย ฉะนั้นผู้ใดจะมีสิทธิ์ที่จะเข้าถึงข้อมูลได้จะต้องมีการกำหนดสิทธิ์กันไว้ก่อนและเมื่อเข้าไปใช้ข้อมูลนั้น ๆ ผู้ใช้จะเห็นข้อมูลที่ถูกเก็บไว้ในฐานข้อมูลในรูปแบบที่ผู้ใช้ออกแบบไว้ตัวอย่างเช่น ผู้ใช้สร้างตารางข้อมูลขึ้นมาและเก็บลงในระบบฐานข้อมูล ระบบจัดการฐานข้อมูลจะเก็บข้อมูลเหล่านี้ลงในอุปกรณ์เก็บข้อมูลในรูปแบบของระบบจัดการฐานข้อมูลซึ่งอาจเก็บข้อมูลเหล่านี้ลงในแผ่นจานบันทึกแม่เหล็กเป็นระเบียน บล็อกหรืออื่น ๆ ผู้ใช้ไม่จำเป็นต้องรับรู้ว่าโครงสร้างของแฟ้มข้อมูลนั้นเป็นอย่างไร ปล่อยให้เป็นหน้าที่ของระบบจัดการฐานข้อมูลดังนั้นถ้าผู้ใช้เปลี่ยนแปลงลักษณะการเก็บข้อมูล เช่น เปลี่ยนแปลงรูปแบบของตารางเสียใหม่ ผู้ใช้ก็ไม่ต้องกังวลว่าข้อมูลของเขาจะถูกเก็บลงในแผ่นจานบันทึกแม่เหล็กในลักษณะใด ระบบการจัดการฐานข้อมูลจะจัดการให้ทั้งหมด ในทำนองเดียวกันถ้าผู้ออกแบบระบบฐานข้อมูลเปลี่ยนวิธีการเก็บข้อมูลลงบนอุปกรณ์จัดเก็บข้อมูล ผู้ใช้ก็ไม่ต้องแก้ไขฐานข้อมูลที่เขาออกแบบไว้แล้ว ระบบการจัดการฐานข้อมูลจะจัดการให้ ลักษณะเช่นนี้เรียกว่า ความไม่เกี่ยวข้องกันของข้อมูล (data independent)

3. สามารถใช้ข้อมูลร่วมกันได้ เนื่องจากในระบบฐานข้อมูลจะเป็นที่เก็บรวบรวมข้อมูลทุกอย่างไว้ ผู้ใช้แต่ละคนจึงสามารถที่จะใช้ข้อมูลในระบบได้ทุกข้อมูล ซึ่งถ้าข้อมูลไม่ได้ถูกจัดให้เป็นระบบฐานข้อมูลแล้ว ผู้ใช้ก็จะใช้ได้เพียงข้อมูลของตนเองเท่านั้น

4. มีความเป็นอิสระของข้อมูล เมื่อผู้ใช้ต้องการเปลี่ยนแปลงข้อมูลหรือนำข้อมูลมาประยุกต์ใช้ให้เหมาะสมกับโปรแกรมที่เขียนขึ้นมา จะสามารถสร้างข้อมูลนั้นขึ้นมาใช้ใหม่ได้ โดยไม่มีผลกระทบต่อระบบฐานข้อมูล เพราะข้อมูลที่ผู้ใช้นำมาประยุกต์ใช้ใหม่นั้นจะไม่กระทบต่อโครงสร้างที่แท้จริงของการจัดเก็บข้อมูล นั่นคือ การใช้ระบบฐานข้อมูลจะทำให้เกิดความเป็นอิสระระหว่างการจัดเก็บข้อมูลและการประยุกต์ใช้

2.1.2.3 ฐานข้อมูล MySQL

MySQL เป็นโปรแกรมฐานข้อมูลที่ใช้จัดเก็บข้อมูลโปรแกรมหนึ่ง ทำงานในลักษณะ Client Server ทำงานบนระบบ Telnet บน Linux Redhad หรือ Unix System (ฟรี) และบน Win32 ทั่วไปบนระบบเครือข่าย Inter & Intranet นั้นหมายความว่าเราสามารถเรียกใช้ MySQL ได้ทั่วโลกกรณีเป็น Internet และ ทั่วบริเวณที่เป็น Intranet และยังสามารถเรียกใช้บน Web Browser ได้กรณีใช้ language เป็น Interface ในการเชื่อม language ที่ใช้เป็น Interface เช่น PHP, Perl, C, C++

MySQL เป็นฐานข้อมูลแบบ open source ที่ได้รับความนิยมในการใช้งานสูงสุดโปรแกรมหนึ่งบนเครื่องให้บริการ มีความสามารถในการจัดการกับฐานข้อมูลด้วยภาษา SQL อย่างมีประสิทธิภาพ มีความรวดเร็วในการทำงาน รองรับการทำงานจากผู้ใช้หลาย ๆ คน MySQL ถูก

พัฒนาขึ้นโดย MySQ LAB โดยมีลิขสิทธิ์การใช้งาน 2 แบบ นั่นคือ ผู้ดูแลระบบสามารถใช้งานซอฟต์แวร์ MySQL ได้โดยไม่มีค่าใช้จ่ายใด ๆ ภายใต้ลิขสิทธิ์ของ GNU (General Public License) หรืออาจเลือกใช้แบบที่มีลิขสิทธิ์ทางการค้าของ MySQLAB ซึ่งเป็นผู้ผลิตและพัฒนาซอฟต์แวร์

2.1.2.4 ความสามารถและการทำงานของโปรแกรม MySQL มีดังนี้

1. MySQL ถือเป็นระบบจัดการฐานข้อมูล DataBase Management System (DBMS) ฐานข้อมูลมีลักษณะเป็นโครงสร้างของการเก็บรวบรวมข้อมูล การที่จะเพิ่มเติม เข้าถึงหรือประมวลผลข้อมูลที่เก็บในฐานข้อมูลจำเป็นจะต้องอาศัยระบบจัดการฐานข้อมูล ซึ่งจะทำหน้าที่เป็นตัวกลางในการจัดการกับข้อมูลในฐานข้อมูลทั้งสำหรับการใช้งานเฉพาะ และรองรับการทำงานของแอพพลิเคชันอื่นๆ ที่ต้องการใช้งานข้อมูลในฐานข้อมูล เพื่อให้ได้รับความสะดวกในการจัดการกับข้อมูลจำนวนมาก MySQL ทำหน้าที่เป็นทั้งตัวฐานข้อมูลและระบบจัดการฐานข้อมูล

2. MySQL เป็นระบบจัดการฐานข้อมูลแบบ relational ฐานข้อมูลแบบ Relational จะทำการเก็บข้อมูลทั้งหมดในรูปแบบของตารางแทนการเก็บข้อมูลทั้งหมดลงในไฟล์เพียงไฟล์เดียว ทำให้ทำงานได้รวดเร็วและมีความยืดหยุ่น นอกจากนั้น แต่ละตารางที่เก็บข้อมูลสามารถเชื่อมโยงเข้าหากันทำให้สามารถรวมหรือจัดกลุ่มข้อมูลได้ตามต้องการ โดยอาศัยภาษา SQL ที่เป็นส่วนหนึ่งของโปรแกรม MySQL ซึ่งเป็นภาษามาตรฐานในการเข้าถึงฐานข้อมูล

3. MySQL แจกจ่ายให้ใช้งานแบบ open source นั่นคือ ผู้ใช้งาน MySQL ทุกคนสามารถใช้งานและปรับแต่งการทำงานได้ตามต้องการ สามารถดาวน์โหลดโปรแกรม MySQL ได้จากอินเทอร์เน็ตและนำมาใช้งานโดยไม่มีค่าใช้จ่ายใดๆในระบบปฏิบัติการ Red Hat Linux นั้น มีโปรแกรมที่สามารถใช้งานเป็นฐานข้อมูลให้ผู้ดูแลระบบสามารถเลือกใช้งานได้หลายโปรแกรม เช่น MySQL และ PostgreSQL ผู้ดูแลระบบสามารถเลือกติดตั้งได้ทั้งในขณะที่ติดตั้งระบบปฏิบัติการ Red Hat Linux หรือจะติดตั้งภายหลังจากที่ติดตั้งระบบปฏิบัติการก็ได้ อย่างไรก็ตาม สาเหตุที่ผู้ใช้งานจำนวนมากนิยมใช้งานโปรแกรม MySQL คือ MySQL สามารถทำงานได้อย่างรวดเร็ว น่าเชื่อถือและใช้งานได้ง่าย เมื่อเปรียบเทียบประสิทธิภาพในการทำงานระหว่างโปรแกรม MySQL และ PostgreSQL โดยพิจารณาจากการประมวลผลแต่ละคำสั่ง นอกจากนั้น MySQLถูกออกแบบและพัฒนาขึ้นมาเพื่อทำหน้าเป็นเครื่องให้บริการรองรับการจัดการกับฐานข้อมูลขนาดใหญ่ ซึ่งการพัฒนายังคงดำเนินอยู่อย่างต่อเนื่อง ส่งผลให้มีฟังก์ชันการทำงานใหม่ ๆ ที่อำนวยความสะดวกให้กับผู้ใช้งานเพิ่มขึ้นอยู่ตลอดเวลา รวมไปถึงการปรับปรุงด้านความต่อเนื่อง ความเร็วในการทำงาน และความปลอดภัย ทำให้ MySQL เหมาะสมต่อการนำไปใช้งานเพื่อเข้าถึงฐานข้อมูลบนเครือข่ายอินเทอร์เน็ต

4. phpMyAdmin คือ ตัวควบคุม MySQL Database ผ่านเว็บไซต์ ซอร์สโค้ดของ phpMyAdmin ได้ถูกเผยแพร่ให้กับนักพัฒนาภาษาพีเอชพีทั่วไป ตลอดจนผู้ที่เพิ่งเริ่มต้นเรียนรู้โดย

เปรียบเสมือนตัวกลางที่คั่นระหว่างผู้ใช้งานกับฐานข้อมูล MySql ที่พัฒนามาจากภาษาพีเอชพี อะไรที่เกี่ยวข้องกับการจัดการฐานข้อมูล MySql สามารถทำได้โดยผ่านหน้าเว็บบราวเซอร์ทำให้ไม่จำเป็นต้องจดจำและใช้งานคำสั่งต่างๆให้ยุ่งยากทำให้การสร้างแอพพลิเคชันฐานข้อมูลบนอินเตอร์เน็ตกลายเป็นเรื่องที่ไม่ยุ่งยากอีกต่อไป ทั้งนี้นอกจาก phpMyAdmin จะเป็นซอร์สโค้ดที่มีประสิทธิภาพระดับหนึ่งแล้วสามารถนำไปพัฒนาเพื่อเพิ่มความสามารถให้มากยิ่งขึ้นอีกด้วย

2.1.2.5 ความสามารถของ PHP My Admin

PHP My Admin ทำหน้าที่เป็นเครื่องมือช่วยเหลือการจัดการฐานข้อมูลสามารถทำงานได้ดังนี้

1. สร้างและลบฐานข้อมูล
2. สร้าง คัดลอกและลบตารางออกจากฐานข้อมูล
3. ลบ แก้ ไข เพิ่มเติมฟิลด์ต่าง ๆ ในตาราง
4. ประมวลผลคำสั่ง SQL หรือ Batch Queries จัดการคีย์ต่าง ๆ หรือคุณสมบัติของฟิลด์ อ่านค่าจาก Text File เข้าไปยังตารางของคุณได้
5. สามารถอ่านและสร้าง Dump Table ได้
6. Export และ Import ข้อมูลชนิด .CSV
7. สนับสนุนการแสดงภาษามากกว่า 10 ภาษา เช่น จีน ญี่ปุ่นและอื่น ๆ

2.1.3 การรักษาความปลอดภัยข้อมูล

ระบบคอมพิวเตอร์ปัจจุบันถูกคุกคามมากขึ้นจากผู้ไม่ประสงค์ดี ที่ต้องการคัดลอกข้อมูลเพื่อนำข้อมูลที่ได้มานั้นไปใช้ในทางที่ผิด ทำให้เกิดความเสียหายต่อผู้ใช้งาน เพราะฉะนั้นความปลอดภัยคอมพิวเตอร์ (Computer Security) จึงเป็นสิ่งที่ต้องคำนึงถึงมากที่สุด ซึ่งจุดประสงค์หลักของด้านความปลอดภัยทางข้อมูลถูกแบ่งออกเป็น 4 ลักษณะ ดังนี้

1. **การรักษาความปลอดภัย (Confidentiality)** คือ การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ โดยอนุญาตให้ผู้มีสิทธิ์เท่านั้น จึงจะสามารถเข้าถึงข้อมูลได้ ขณะที่ผู้ไม่มีสิทธิ์หรือไม่ได้รับอนญาตจะไม่สามารถเข้าถึงข้อมูลได้ไม่ว่ากรณีใด ๆ

2. **การรักษาความสมบูรณ์ (Integrity)** คือ การรับรองว่าข้อมูลนั้นจะไม่ถูกเปลี่ยนแปลงหรือทำลายจากสภาพเดิมไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา โดยข้อมูลนั้นจะต้องคงสภาพเดิมอยู่และมีความน่าเชื่อถือ

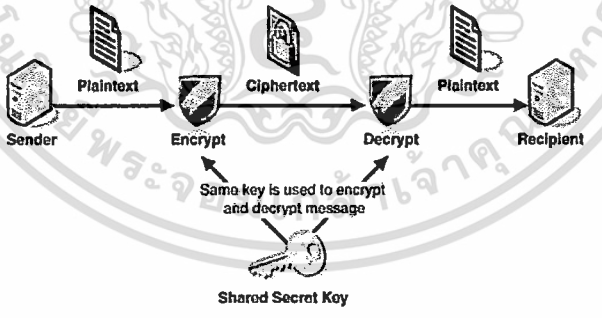
3. **การพิสูจน์ตัวตน (Authentication)** คือ การรับรองว่าผู้ที่อ้างอิงนั้นมีตัวตนจริงและเป็นผู้ที่มีสิทธิ์หรือได้รับอนุญาตใด ๆ โดยมีความถูกต้อง ตลอดจนสามารถเข้าสู่ระบบหรือเข้าถึงข้อมูลที่เป็นความรลับซึ่งจะทำให้เกิดความมั่นใจในอีกฝ่ายหนึ่งเกิดขึ้นระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล

4. **ไม่สามารถปฏิเสธความรับผิดชอบได้** (Non-Repudiation) คือ วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันหรือพิสูจน์ทราบตัวตนว่าผู้ส่งเป็นใคร ดังนั้นหากมีกรณีใด ๆ ก็ตามที่เกิดขึ้น ทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

2.1.3.1 การเข้ารหัสลับ (Encryption)

การเข้ารหัสลับ คือ กระบวนการเปลี่ยนรูปข้อมูลต้นฉบับให้อยู่ในรูปข้อมูลที่ไม่สามารถเข้าใจได้เพื่อเป็นการป้องกันสิทธิ์การเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ซึ่งกลไกการเข้ารหัสจะต้องประกอบด้วย 5 ส่วน คือ ข้อความต้นฉบับ (Plaintext) อัลกอริทึมเข้ารหัส (Encryption Algorithm) ข้อความรหัส (Cipher text) กุญแจรหัสลับ (Key) และอัลกอริทึมถอดรหัส (Decryption Algorithm) โดยวิธีการเข้ารหัสแบ่งออกเป็น 2 ประเภท คือ

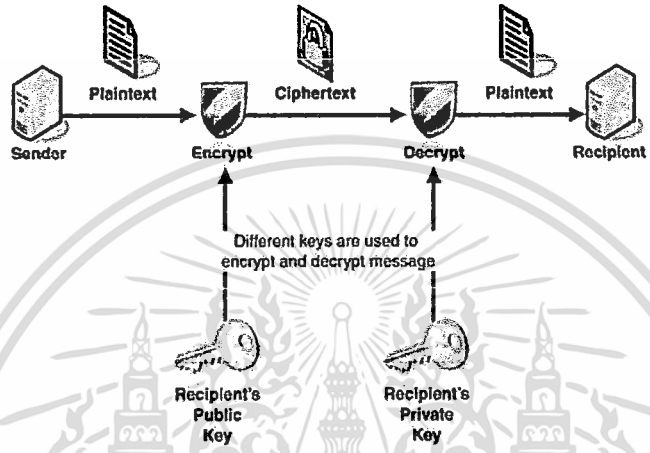
1. **การเข้ารหัสลับแบบสมมาตร (Symmetric Key Encrytion)** เป็นการเข้ารหัสลับโดยใช้การเข้าและถอดรหัสเดียวกัน เรียกว่ากุญแจลับ
(Secret Key) ซึ่งต้องมีการส่งผ่านถึงกันระหว่างผู้รับและผู้ส่งผ่านช่องสัญญาณปลอดภัย (Secure Channel) หลังจากนั้นผู้ส่งจะทำการเข้ารหัสข้อมูลด้วยกุญแจลับที่ได้ตกลงกับทางฝั่งผู้รับกลายเป็นข้อความรหัสลับส่งผ่านช่องทางการสื่อสารซึ่งอาจเป็นช่องสัญญาณสาธารณะ (Public Channel) ไปยังผู้รับ ซึ่งข้อความรหัสลับหากถูกดักจับไปได้ก็ไม่สามารถถอดรหัสลับได้ มีเพียงผู้รับที่สามารถถอดรหัสลับโดยใช้กุญแจเดียวกันกลับมาเป็นข้อความต้นฉบับดังรูปที่ 2.1



รูปที่ 2.1 แสดงกระบวนการเข้ารหัสลับแบบสมมาตร

หลักของการเข้ารหัสแบบสมมาตรนั้นจะใช้การแทนที่ (Substitution) และการสลับค่า (Permutation) เพื่อให้เกิดความยากและซับซ้อนการทอดรหัส อัลกอริทึมที่นิยมใช้งานอยู่ในปัจจุบัน คือ DES และ AES ข้อดีของการเข้ารหัสแบบสมมาตร คือ มีความสะดวกรวดเร็ว แต่ก็มีข้อด้อยตรงที่จำเป็นต้องเก็บรักษากุญแจรหัสลับให้รู้เฉพาะผู้ส่งและผู้รับผ่านทางช่อง สัญญาณปลอดภัยเท่านั้น ในโลกของความเป็นจริงแล้วช่องสัญญาณนี้มีโอกาสเกิดขึ้นได้น้อยมาก ซึ่งหากมีผู้อื่นทราบกุญแจรหัสลับก็สามารถถอดรหัสลับได้เช่นกัน

2. **การเข้ารหัสลับแบบอสมมาตร (Asymmatric Key Encryption)** ถูกพัฒนาขึ้นมาเพื่อแก้ไขปัญหาการส่งผ่านกุญแจรหัสรับ ผ่านช่องสัญญาณปลอดภัย และจำนวนกุญแจที่ต้องเก็บรักษาเมื่อมีการสื่อสารมากขึ้นของการเข้ารหัสแบบสมมาตร โดยใช้บนพื้นฐานทฤษฎีที่เรียกว่า "One way function" ในการสร้างกุญแจสำหรับเข้ารหัสและถอดรหัสต่างกันซึ่งเป็นคู่กุญแจกัน (Key Pair) ประกอบด้วยกุญแจส่วนตัว (Private Key) เก็บไว้เป็นความลับ และกุญแจสาธารณะ (Public Key) สำหรับแจกจ่ายให้ผู้อื่น ซึ่งมีลักษณะการทำงานดังรูปที่ 2.2



รูปที่ 2.2 แสดงกระบวนการเข้ารหัสลับแบบอสมมาตร

ขั้นตอนการสร้างคู่กุญแจในที่นี้จะยกตัวอย่างอัลกอริทึมที่มีชื่อว่า RSA ซึ่งนิยมใช้งานกันในปัจจุบันและอัลกอริทึม Diffie Hellman สำหรับการแลกเปลี่ยนกุญแจ (Key Agreement) ระหว่างผู้รับและผู้ส่ง โดยไม่ต้องส่งกุญแจลับผ่านช่องสัญญาณปลอดภัย

- **อัลกอริทึม RSA**

1. ผู้รับเลือกจำนวนเฉพาะ p และ q

2. คำนวณ N=pq

3. คำนวณ Ø (N)=(p-1)(n-1)

4. เลือกค่ากุญแจสาธารณะ e โดย gcd (e,Ø(N))=1

5. คำนวณกุญแจส่วนตัว d โดย $d=e^{-1} \bmod Ø(N)$ เก็บค่า d, Ø (N) และ p,q ไว้เป็นความลับ ส่วนที่ค่ากุญแจสาธาณะคือ (e,N) ส่งให้แก่ผู้ส่งข้อมูล

การเข้ารหัสลับ

ผู้ส่งข้อมูลใช้กุญแจสาธารณะของผู้รับเข้ารหัสข้อมูล M ตามสมการ $C=M^e \bmod N$ แล้วส่งข้อความรหัส C ไปยังผู้รับ

การถอดรหัสลับ

ผู้รับทำการถอดรหัสลับโดยใช้กุญแจส่วนตัวได้ข้อมูล M ตามสมการ $M=C^d \bmod N$

ข้อจำกัดการเข้ารหัสลับแบบ RSA อยู่ที่จำนวนความยาวของกุญแจซึ่งปัจจุบันมีขนาด 512 บิต ซึ่ง

ในการป้องกันการโจมตีแบบไม่มีกุญแจส่วนตัวสามารถทำได้โดยเพิ่มความยาวบิตของกุญแจ N แต่ก็ทำให้ใช้เวลาในการคำนวณมากขึ้นตามไปด้วย จึงไม่เหมาะสมกับการรับส่งข้อมูลที่มีขนาดใหญ่

- **อัลกอริทึม Diffle-Hellman**

1. ผู้ส่งและผู้รับตกลงค่าตัวแปลสาธารณะ g และ p โดยที่ g เป็นค่าราก primitive ของ p

2. ผู้ส่งและผู้รับเลือกตัวแปลลับ x และ y ตามลำดับ จากนั้นทำการคำนวณ X และ Y ผู้ส่งคำนวณ $X = g^x \bmod p$ ผู้รับคำนวณ $Y=g^y \bmod p$

3. ผู้ส่งและผู้รับแลกค่า X และ Y ซึ่งกันและกัน และนำค่าที่ได้รับมาคำนวณกุญแจรหัสลับ ซึ่งผลจากการคำนวณของทั้งสองฝ่ายจะได้ค่ากุญแจรหัสลับเดียวกัน โดย

กุญแจของผู้ส่ง $Y^x=g^{yx} \text{mon} N=K_{AB}$

กุญแจของผู้รับ $Xy=g^{xy} \text{mod} N=K_{AB}$

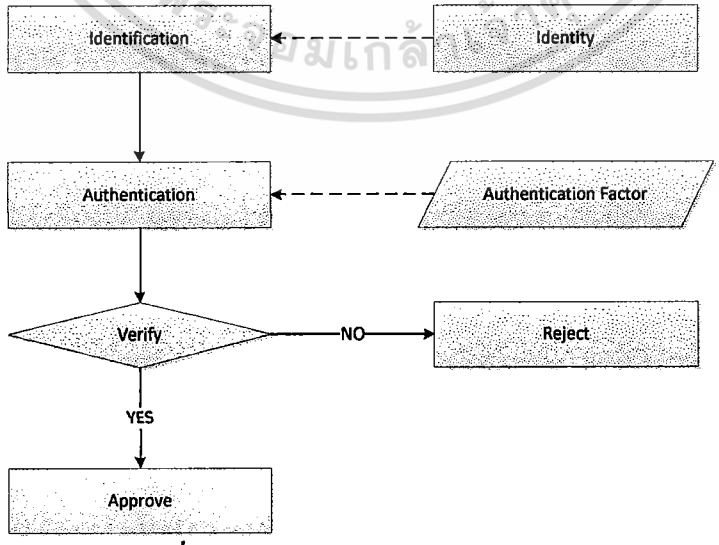
ซึ่งเมื่อทั้งสองฝ่ายคำนวณ K_{AB} ได้แล้วก็จะทำการส่งข้อมูลโดยเข้าและถอดรหัสลับด้วย K_{AB} ได้อย่างมีความปลอดภัย

2.1.4. การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อของผู้ใช้ (Username)

การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวจริง



รูปที่ 2.3 แสดงกระบวนการพิสูจน์ตัวตน

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวสสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากนั้นระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้ว ถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะปฏิเสธจากระบบ

หลักฐานที่ผู้ใช้นำมากล่าวอ้าง ที่เกี่ยวกับเรื่องของความปลอดภัยนั้น สามารถแบ่งออกได้ 2 ประเภทดังนี้

1. Actual identity คือหลักฐานที่สามารถบอกได้ว่า ในความจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

2. Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะ คือ

- สิ่งที่คุณมี (Passession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น
- สิ่งที่คุณรู้ (Knowlrdge factor) เช่น รหัสผ่าน (Password) หรือการใช้พิน (PINs)
- สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns)

2.1.4.1 ประเภทของการพิสูจน์ตัวตนลักษณะต่างๆ

- **ไม่มีการพิสูจน์ตัวตน (No Authentication)** ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น เมื่อข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือ ข้อมูลข่าวสาร หรือแหล่งของข้อมูลนั้น ๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น
- **การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)** รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ แต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

- **การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN)** PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่น บัตร ATM และเครดิตการ์ดต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น
- **การพิสูจน์ตัวตนโดยใช้ Password Authenticators** หรือ Tokens เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password) ในขณะที่กำลังเข้าสู่ระบบเครือข่ายมี 2 วิธีคือ

  1. **การพิสูจน์ตัวตนแบบขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication)** เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกดโทเคน เพื่อให้โทเคนสร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกดโทเคน ใส่ลงในฟอร์มสำหรับรับข้อมูล เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อนว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบ
  2. **การพิสูจน์ตัวตนโดยขึ้นอยู่กับเวลา (Time-synchronous authentication)** เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุก ๆ หนึ่งนาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (โดยรหัสผ่านจะถูกสร้างขึ้นมาจากโทเคน) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ

ตารางที่ 2.2 เปรียบเทียบข้อดีและข้อเสียของการพิสูจน์ตัวตน

รูปแบบการพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
ไม่มีการพิสูจน์ตัวตน	ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ	ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่

ตารางที่ 2.2 (ต่อ)

รูปแบบการพิสูจน์ตัวตน	ข้อดี	ข้อเสีย
การพิสูจน์ตัวตนโดยใช้ PIN	- ง่ายต่อการจำและความปลอดภัยค่อนข้างดี (ATM CARD) - สามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่างปลอดภัย	- ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN - ไม่สามารถใช้กับต่างระบบกันได้ - ราคาแพง
การพิสูจน์ตัวตนโดยใช้ Password authenticator หรือ tokens	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - ผู้ที่ละเมิดเข้ามาไม่สามารถจะเข้าจู่โจมได้	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - Authenticator เป็นวัตถุจึงง่ายต่อการสูญหายและการถูกขโมยได้

2.1.4.2 PKI-Public Key Infrastructure

ส่วนประกอบโดยหลักของ PKI คือ หน่วยผู้ประกอบการรับรอง (Certificate Authority) ระบบไดเรกทอรี (Directory Services) เพื่อจัดเก็บใบรับรองอิเล็กทรอนิกส์และระบบจัดการบริหารกุญแจ (Certificate Management System) โดยแนวคิดหลักที่มีบทบาทสำคัญ คือ ใช้เทคโนโลยีระบบรหัสกุญแจคู่ (Cryptographic Keys) ผู้ใช้มีกุญแจ 2 ดอก คือกุญแจสาธารณะที่เปิดเผยให้ผู้อื่นนำไปใช้งานได้ โดยจัดเก็บไว้บนใบรับรองอิเล็กทรอนิกส์ และกุญแจส่วนตัวที่เจ้าของต้องเก็บเป็นความลับ สามารถนำไปใช้เข้าและถอดรหัสด้วยระบบรหัสแบบอสมมาตรหรือสร้างลายมือชื่อดิจิตอล (Digital Signature) นอกจากนั้น หน่วยผู้ประกอบการรับรองจะดูแลการเผยแพร่ใบรับรองอิเล็กทรอนิกส์ ตรวจสอบและประกาศสถานะของใบรับรองอิเล็กทรอนิกส์ที่หมดอายุด้วย

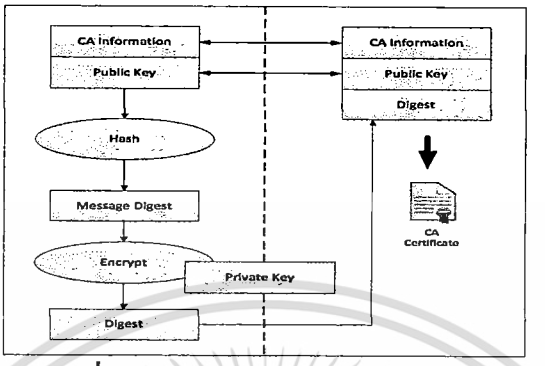
2.1.4.3 ส่วนประกอบของ PKI

PKI มีส่วนประกอบหลายส่วนที่ทำงานร่วมกันเพื่อสร้าง (Issue) แจกจ่าย (Distribute) และจัดการเกี่ยวกับการใช้งาน (Manage) ใบรับรองอิเล็กทรอนิกส์ ได้แก่

- Certification Authority (CA)
- Registration Authority (RA)
- Certificate Revocation
- Certificate Repository

1. **Certification Authority (CA)** คือหน่วยผู้ประกอบการรับรอง ที่เป็นหน่วยงานภายนอก (Trusted Third Party) ซึ่งมีหน้าที่หลักคือ เป็นผู้ออกใบรับรองอิเล็กทรอนิกส์ให้กับบุคคลหรือสิ่ง

อื่น ๆ (ในที่นี่จะเรียกรวมว่าเป็น Subject) ทั้งนี้ Self-signed Certificate จะเป็นสิ่งที่ระบุตัวตนของหน่วยผู้ประกอบการรับรองเอง ทั้งนี้ ขั้นตอนการสร้าง Self-signed Certificate ของ CA เป็นดังในรูปที่ 2.3



รูปที่ 2.4 แสดง Self-signed Certificate

ดังนั้นหน่วยผู้ประกอบการับรองจึงเป็นจุดเริ่มต้นของการสร้างความไว้วางใจ (Trust) แต่ละเอ็นทิตีจะต้องมอบความไว้วางใจต่อหน่วยผู้ประกอบการรับรองและสิ่งใดก็ตามที่หน่วยผู้ประกอบการรับรองได้ออกใบรับรองให้การสร้าง Self-signed Certificate ในการเริ่มต้นเป็นหน่วยผู้ประกอบการรับรอง จะต้องสร้างใบรับรองอิเล็กทรอนิกส์ของ CA เองก่อน

หน่วยผู้ประกอบการรับรองเป็นหัวใจสำคัญของ PKI และรับผิดชอบหน้าที่สำคัญหลายประการ ได้แก่ Certificate Management กล่าวคือ Issuance, Revocation, Update และ Renewal การเผยแพร่ใบรับรองอิเล็กทรอนิกส์และ CRL (Certificate Revocation List) และทำการบันทึกล็อกจากเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบขั้นตอนโดยทั่วไปในการออกใบรับรองให้กับ Subject ใด ๆ นั้นจะประกอบไปด้วย

- Subject ส่งคำร้องขอ (Certificate Request)
- Subject เป็นผู้สร้างกุญแจคู่โดยหน่วยผู้ประกอบการรับรองเป็นผู้จัดเตรียมฟังก์ชันนี้ให้
- หน่วยผู้ประกอบการรับรองจะจัดการออกใบรับรองให้ ทั้งนี้คำร้องดังกล่าวอาจเป็นไปได้ตั้งแต่ขอใหม่ การปรับเปลี่ยนหรือขอให้ออกให้ใหม่
- รอการอนุมัติจากหน่วยผู้ประกอบการรับรอง
- หน่วยผู้ประกอบการรับรองตรวจสอบ Identity ของผู้ร้องขอ เมื่อผ่านแล้วหน่วยผู้ประกอบการรับรองจะทำการ Sign Request นั้น โดยการสร้างใบรับรองอิเล็กทรอนิกส์
- เผยแพร่ใบรับรองอิเล็กทรอนิกส์ดังกล่าว เพื่อให้ผู้ร้องขอมารับไป

2. Registration Authority (RA) คือหน่วยรับจดทะเบียน ในการดำเนินงานจริงหน่วยผู้ประกอบการรับรองบางแห่งอาจจะแบ่งหน้าที่บางอย่างให้กับ RA ใน RFC 2510 Internet Public

Key Infrastructure Certificate Management Protocols ซึ่งอ้างถึงหน้าที่ของ RA ไว้ว่าเป็นการตรวจสอบความถูกต้องของบุคคล (Personal Authentication) การแจกจ่าย Token (Token distribution) รายงานการเพิกถอนใบรับรอง (Revocation reporting) การกำหนดชื่อ (Name assignment) การสร้างกุญแจคู่ (Key generation) การจัดเก็บกุญแจคู่ (Archival of Key pairs) เป็นต้น แต่ในทางปฏิบัติแล้วส่วนใหญ่ RA จะทำหน้าที่ตรวจสอบความถูกต้องของบุคคล หรือ Subject ใดๆ ระหว่างกระบวนการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Enrollment Process)

3. **Certificate Management Protocol (CMP)** คือขั้นตอนหรือโพรโตคอลในการจัดการใบรับรองอิเล็กทรอนิกส์ โดยที่ Certificate Management Protocol หลายแบบได้ระบุถึงขั้นตอน Certificate Enrollment ในบางกรณีก็ระบุถึงขั้นตอน Certificate Revocation Process เวนเดอร์บางแห่งก็เพิ่มเติมฟังก์ชันการทำงานของโพรโตคอลนอกเหนือจากนี้เช่น Key recovery และ Automated certificate renewal

4. **Public Key Cryp0tographic Standard (PKCS)** เป็นชุดโพรโตคอลมาตรฐานของ RSA Security ที่ระบุวิธีการรักษาความปลอดภัยของการแลกเปลี่ยนข้อมูลระหว่างกัน PKCS #1, #3, #5, #6, #7, #8, #9, #10, #11, #12 และ #15 เป็นมาตรฐานที่มีการใช้งานในปัจจุบัน ส่วน PKCS #13 และ #14 ยังคงอยู่ในระหว่างการอนุมัติ ส่วน PKCS #2 และ #4 ได้ถูกรวมเข้ากับ PKCS #1 แล้ว

- PKCS #1 : RSA Cryptography Standard
- PKCS #2 : ถูกรวมเข้ากับ PKCS #1 แล้ว
- PKCS #3 : Diffie-Hellman Key Agreement Standard
- PKCS #4 : ถูกรวมเข้ากับ PKCS #1 แล้ว
- PKCS #5 : Password-Based Cryptography Standard
- PKCS #6 : Extended-Certificate Syntax Standard
- PKCS #7 : Cryptographic Message Syntax Standard
- PKCS #8 : Private-Key Information Syntax Standard
- PKCS #9 : Selected Attribute Types
- PKCS #10 : Certification Request Syntax Standard
- PKCS #11 : Cryptographic Token Interface Standard
- PKCS #12 : Personal Information Exchange Syntax Standard
- PKCS #13 : Elliptic Curve Cryptography Standard
- PKCS #15 : Cryptographic Token Information Format Standard

5. **Certificate Revocation** คือกระบวนการเพิกถอนใบรับรองอิเล็กทรอนิกส์ (Certificate Revocation) เนื่องจากหมดอายุหรือใบรับรองอิเล็กทรอนิกส์ถูกผู้อื่นนำไปใช้ วิธีที่นิยมใช้ ซึ่งก็

ได้แก่ CRL (Certificate Revocation List) เป็นรายชื่อของใบรับรองที่ถูกเพิกถอน ใน RFC 2459Internet X.509 Public Key Infrastructure Certificate and CRL Profile ได้ระบุรูปแบบของ X.509 CRL Version 2 ไว้ OCSP (Online Certificate Status Protocol) ในการใช้งาน PKI กับงานบางประเภท ช่วงเวลาระหว่างการอัพเดท CRL แต่ละครั้งไม่เป็นที่ยอมรับ ดังนั้นจึงเกิด OCSP ขึ้น ซึ่งเป็นกลไกในการตรวจสอบการเพิกถอนของใบรับรองอิเล็กทรอนิกส์แบบเรียลไทม์ เอ็นทิตีจะส่ง Certificate Status Check ไปยัง OCSP Responder ที่อาจเป็นหน่วยผู้ประกอบการรับรองหรือแบ่งหน้าที่ให้กับหน่วยอื่นก็ได้ โดยทั้งนี้ใบรับรองอิเล็กทรอนิกส์จะไม่ได้รับการยอมรับจนกว่า OCSP Responder จะตอบ Message มายืนยันหรือปฏิเสธสถานะของใบรับรองอิเล็กทรอนิกส์นั้น

6. **Certificate Repository** ใช้สำหรับจัดเก็บและประกาศใบรับรองอิเล็กทรอนิกส์ให้สาธารณะรับทราบในการพัฒนาระบบเล็ก ๆ ส่วนนี้อาจจะไม่จำเป็น เพราะอาจทำการแลกเปลี่ยนใบรับรองหรือ CRL ผ่านทางจดหมายอิเล็กทรอนิกส์ได้ แต่เมื่อต้องเกี่ยวพันกับใบรับรองจำนวนมากก็จำเป็นต้องมีการจัดเก็บให้เป็นไปในทิศทางเดียวกัน ซึ่งอาจจะเลือกใช้ Directory Services หรือ FTP และ HTTP ก็ได้

2.1.4.4 ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

เทคโนโลยีใบรับรองอิเล็กทรอนิกส์นั้นมีความมุ่งเน้นที่จะแก้ไขปัญหาที่สำคัญอีกประการหนึ่งซึ่งไม่อาจมองข้ามได้และส่งผลกระทบต่อความเชื่อมั่นอย่างมากในการทำธุรกรรมพาณิชย์อิเล็กทรอนิกส์ต่าง ๆ ไม่แพ้กับการรักษาความลับ การรักษาความสมบูรณ์หรือการพิสูจน์ตัวตน นั่นคือเรื่องของการห้ามปฏิเสธความรับผิดชอบระหว่างผู้ให้บริการกับผู้กระทำธุรกรรม

แนวทางการแก้ไขปัญหาคือ การจัดตั้งองค์กรกลางเพื่อทำหน้าที่ในการรับรองความมีตัวตนของบุคคลที่กล่าวอ้าง รวมถึงรับรองกุญแจรหัสลับ กุญแจสาธารณะของเขาว่าเป็นของจริง สามารถเชื่อถือได้ โดยมีหลักฐานที่ใช้ในการตรวจสอบบุคคลอย่างถูกต้องแม่นยำ ไม่ผิดพลาด จึงสามารถแก้ปัญหาการปฏิเสธความรับผิดชอบต่อปัญหาต่าง ๆ ที่อาจเกิดขึ้นภายหลัง เราเรียกองค์กรกลางดังกล่าวว่า “ผู้ออกใบรับรอง” (Certification Authority-CA) ซึ่งทำหน้าที่ในการตรวจสอบข้อมูลรับรองความถูกต้อง และออกใบรับรองอิเล็กทรอนิส์ให้เพื่อเป็นหลักฐานที่ยืนยันความมีตัวตนอยู่จริงของเจ้าของใบรับรองอิเล็กทรอนิกส์เสมือนเป็นบัตรประจำตัวประชาชนในโลกดิจิตอล

ขั้นตอนของการขอใบรับรองอิเล็กทรอนิกส์ในปัจจุบันแบ่งออกได้เป็น 2 วิธี

1. การขอใบรับรองอิเล็กทรอนิกส์ผ่านทางเครือข่าย โดยการใช้เว็บบราวเซอร์ โดยผู้ใช้เข้าไปยังโฮส (CA) ที่ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ซึ่งทาง CA จะทำการสร้างคู่รหัสกุญแจรหัสลับแล้ว ส่งผ่านกุญแจส่วนตัวมาเก็บไว้ที่เครื่องโดยโปรโตคอลที่มีความปลอดภัย และทำการ

จัดเก็บและบันทึกค่ากุญแจสาธารณะของเราลงยังไดเรกทอรีของ CA จากนั้นจะทำการรับรองข้อมูลและส่งใบรับรองอิเล็กทรอนิกส์กลับมาที่เครื่องเราผ่านเว็บบราวเซอร์

2. การขอใบรับรองอิเล็กทรอนิกส์โดยไม่ผ่านเครือข่าย ซึ่งผู้ที่ขอใบรับรองจะต้องไปขอที่สำนักงานของ CA โดยตรง ทำเรื่องขอใบรับรองอิเล็กทรอนิกส์และกรอกข้อมูลส่วนตัว ซึ่ง CA จะรับรองข้อมูลของผู้ขอใบรับรองพร้อมส่งใบรับรองอิเล็กทรอนิกส์และกุญแจส่วนตัวให้กับผู้ขอในรูปแผ่นดิสก์ให้ผู้ขอนำไปบันทึกในเครื่องตนเองต่อไป

สำหรับรูปแบบของใบรับรองอิเล็กทรอนิกส์ในปัจจุบันส่วนใหญ่นั้นจะอ้างอิงมาตรฐาน X.509 ซึ่งเป็นอนุกรมย่อยของ X.500 ซึ่งเป็นมาตรฐานที่กำหนดโดย ITU-T โดยในขณะที่ X.500 เป็นตัวกำหนดโครงสร้างในลักษณะที่เป็นไดเรกทอรีนั้น X.509 จะทำหน้าที่พิสูจน์สิทธิ์ให้กับส่วนต่างๆ ของไดเรกทอรี ซึ่งรูปแบบการใช้งานจะเน้นไปที่การพิสูจน์ตัวตนเพื่อยืนยันการติดต่อเป็นสำคัญ

การทำงานของ X.509 จะมีโครงสร้างการทำงานเป็นไดเรกทอรี ซึ่งบรรจุข้อมูลที่สำคัญสำหรับการพิสูจน์ตัวตน โดยทั่วไปจะอยู่ในรูปของใบรับรองอิเล็กทรอนิกส์ซึ่งภายในมีการบรรจุกุญแจสาธารณะของผู้ใช้แล้วเข้ารหัสลับด้วยกุญแจส่วนตัวของ CA สำหรับการทำงานของ X.509 นั้น มีขอบเขตการใช้งานที่กว้างขวางมาก เช่นการทำ Web Security, Mail Security หรือ IPSec ซึ่งอาจกล่าวได้ว่าเมื่อใดต้องการการพิสูจน์ตัวตน (Authentication) แล้วนั้นก็จะอยู่ในขอบเขตการทำงานของ X.509 เสมอ

ใบรับรองอิเล็กทรอนิกส์นั้นจะมีการกำหนดช่วงเวลาใช้งานที่จำกัดแน่นอน หากต้องการใช้งานต่อเมื่อใกล้หมดอายุก็ต้องทำการร้องขอการต่ออายุใบรับรอง หากมีการหมดอายุโดยที่ไม่ขอต่ออายุหรือการลาออกของพนักงานในองค์กรก็จำเป็นที่จะต้องทำการเพิกถอนสิทธิ์ (Revoke) ซึ่ง CA ต้องมีการจัดทำรายการใบรับรองที่ถูกเรียกคืน (Certificate Revocation List-CRL) ซึ่งจะมีการเก็บไว้ในไดเรกทอรีที่รับรองโดย CA ผู้ใดต้องการตรวจสอบว่าใบรับรองอิเล็กทรอนิกส์ของตนได้ถูกเพิกถอนก็ทำการขอรายชื่อไปตรวจสอบได้

ส่วนประกอบของใบรับรองอิเล็กทรอนิกส์ จะแบ่งออกเป็น 2 ส่วนหลัก ๆ คือข้อมูลพื้นฐานและข้อมูลเพิ่มเติม

ข้อมูลพื้นฐานของใบรับรองอิเล็กทรอนิกส์

1. Version เวอร์ชันของใบรับรองอิเล็กทรอนิกส์ที่ใช้ตามมาตรฐาน X.509 Certificate จะมีด้วยกันทั้งหมด 3 เวอร์ชัน โดยในเวอร์ชัน 3 จะรองรับการใช้งานใบรับรองอิเล็กทรอนิกส์ที่มีข้อมูลเพิ่มเติม

2. Serial Number หมายถึง หมายเลขที่กำหนดในใบรับรองอิเล็กทรอนิกส์ในแต่ละใบเพื่อป้องกันความซ้ำซ้อนกัน และจะใช้ในการบันทึกเมื่อใบรับรองอิเล็กทรอนิกส์ถูกเพิกถอน

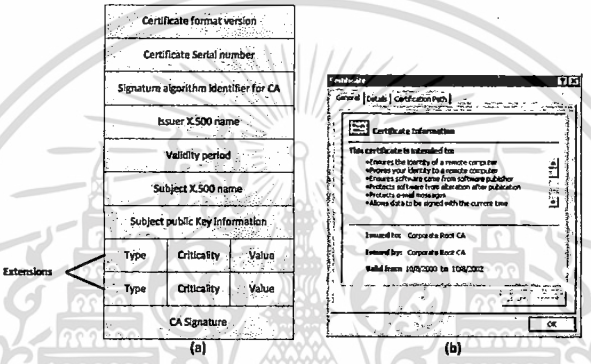
3. Signature แสดงอัลกอริทึมที่ใช้ในการลงลายมือชื่อดิจิตอลควบคู่กับการย่อยข้อมูล เช่น SHA1withRSAEncryption เป็นต้น

4. Issuer หมายถึง ชื่อของผู้ออกใบรับรองที่ทำการสร้างอละออกใบรับรองอิเล็กทรอนิกส์

5. Validity หมายถึง ช่วงระยะเวลาที่สามารถใช้งานใบรับรองอิเล็กทรอนิกส์ โดยมีการระบุถึงวัน-เวลาเริ่มต้น และสิ้นสุดของการใช้งาน

6. Subject หมายถึง ชื่อของผู้เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์

7. Subject Public Key Information หมายถึง กุญแจรหัสลับสาธารณะของผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์ และอัลกอริทึมที่ใช้ในการสร้างกุญแจรหัสลับสาธารณะ เช่น RSA Encryption เป็นต้น



รูปที่ 2.5 (a) แสดงข้อมูลส่วนต่าง ๆ ภายในใบรับรองอิเล็กทรอนิกส์
(b) แสดงตัวอย่างใบรับรองอิเล็กทรอนิกส์ที่มีการใช้งานจริง

ข้อมูลเพิ่มเติมของใบรับรองอิเล็กทรอนิกส์

โครงสร้างของข้อมูลเพิ่มเติมจะประกอบด้วย 3 ส่วน คือชนิดของข้อมูล (Extension Type) ความจำเป็นของข้อมูล (Extension Criticality) และค่าของข้อมูล (Extension Value)

ในฟิลด์ชนิดของข้อมูล จะบอกถึงชนิดของข้อมูลที่อยู่ในฟิลด์ค่าของข้อมูล เช่น ข้อความ ตัวเลข วันที่ เป็นต้น โดยที่ฟิลด์ความจำเป็นของข้อมูล จะใช้ในการบ่งบอกถึงความจำเป็นของข้อมูลเพิ่มเติมในใบรับรองอิเล็กทรอนิกส์ที่ใช้งานร่วมกับแอพพลิเคชัน ถ้าฟิลด์นี้กำหนดว่ามีความจำเป็น แสดงข้อมูลเพิ่มเติมนี้มีความสำคัญ ดังนั้นแอพพลิเคชันที่มีการใช้งานใบรับรองอิเล็กทรอนิกส์ที่มีการระบุความจำเป็น จะต้องทำการอ่านค่าและประมวลผลค่าของข้อมูลดังกล่าว เนื่องจากบางแอพพลิเคชันมีความจำเป็นต้องใช้ข้อมูลเพิ่มเติมพิเศษ ดังนั้น การกำหนดความจำเป็นสำหรับข้อมูลเพิ่มเติมที่อยู่ในใบรับรองอิเล็กทรอนิกส์ก็เพื่อป้องกันการใช้งานในทางที่ไม่ถูกต้องและความไม่ปลอดภัยของใบรับรองอิเล็กทรอนิกส์ข้อมูลเพิ่มเติมนั้นประกอบด้วย 2 ส่วนกล่าวคือ

1. ข้อมูลเพิ่มเติมที่เป็นมาตรฐาน (Standard Extensions) ซึ่งประกอบด้วยข้อมูลต่าง ๆ ดังนี้

- Authority Key Identifier
- Subject Key Identifier
- Key Usage
- Private Key

- Certificate Policy	- Policy Mapping
- Subjrct Alternative Name	- Issuer Alternative Name
- Subject Directory Attribute	- Basic Constraints
- Name Constraints	- Policy Constraints
- Extended Key	- CRL Distribution Points
- Inhibit Any-Policy	- Freshest CRL

2. ข้อมูลเพิ่มเติมที่ใช้ในอินเตอร์เน็ต (Internet Certificate Extensions) ประกอบด้วย

-Authority Information Access ระบุถึงวิธีการในการเข้าถึงข้อมูลและบริการของผู้ออกใบรับรอง สำหรับใบรับรองอิเล็กทรอนิกส์ของผู้ออกใบรับรองที่มีการใช้ฟิลด์นี้

- Subject Information Access ระบุถึงวิธีการในการเข้าถึงข้อมูลและบริการสำหรับใบรับรองอิเล็กทรอนิกส์ที่มีการใช้ฟิลด์นี้ ซึ่งจะรวมถึงนโยบายของผู้ออกใบรับรอง ในกรณีที่เป็นใบรับรองอิเล็กทรอนิกส์ของผู้ออกใบรับรองด้วย

2.1.4.5 การประยุกต์ใช้งาน Certificate

1. **ระบบจดหมายอิเล็กทรอนิกส์แบบปลอดภัย (Secure Electronic Mail System)** คือ ระบบจดหมายอิเล็กทรอนิกส์สามารถนำใบรับรองอิเล็กทรอนิกส์มาใช้ในการเข้ารหัสลับและลงลายมือชื่อดิจิตอล เพื่อเป็นการยืนยันตัวผู้ส่ง ยืนยันความถูกต้องครบถ้วนของข้อมูล รวมทั้งยังสามารถรักษาความลับของข้อมูลในจดหมายให้อ่านได้เฉพาะผู้รับที่ถูกระบุไว้ได้อีกด้วย

2. **การยืนยันตัวตนของผู้ใช้บริการ (Client Authentication)** คือผู้ใช้บริการสามารถใช้บริการเว็บไซต์ได้ (ในกรณีที่เว็บไซต์นั้นต้องการยืนยันตัวบุคคล) เพื่อเป็นการยืนยัน ระบุตัวตนของผู้ใช้บริการ อีกทั้งยังเป็นการสร้างช่องทางการสื่อสารแบบปลอดภัยระหว่างเครื่องให้บริการ (Server) และเครื่องใช้บริการ (Client) ด้วย

3. **การประยุกต์ใช้งานกับแอพลเคชันอื่น ๆ** คือใบรับรองอิเล็กทรอนิกส์สามารถนำไปประยุกต์ใช้งานกับแอพพลิเคชันต่าง ๆ นอกเหนือจากที่ได้กล่าวข้างต้น โดยพิจารณาว่าส่วนใดของแอพพลิเคชันที่ต้องการความปลอดภัยของข้อมูล ก็สามารถนำเทคโนโลยีฌครงสร้างพื้นฐานของระบบกุญแจสาธารณะไปผนวกกับส่วนนั้น ๆ ซึ่งการประยุกต์ในลักษณะดังกล่าว จะต้องมีการพัฒนาแอพพลิเคชันเฉพาะ เพื่อให้สามารถทำงานร่วมกับใบรับรองอิเล็กทรอนิกส์ได้

2.2 เทคโนโลยีที่เกี่ยวข้องในการพัฒนาระบบ

2.2.1 ความหมายของ GPS

GPS คือ ระบบระบุตำแหน่งบนพื้นโลก ย่อมาจากคำว่า Global Positioning System ซึ่งระบบ GPS ประกอบไปด้วย 3 ส่วนหลัก คือ

1. ส่วนอวกาศ ประกอบด้วยเครือข่ายดาวเทียมหลัก 3 ค่าย คือ อเมริกา รัสเซีย ยุโรป

- ของอเมริกา ชื่อ NAVSTAR (Navigation Satellite Timing and Ranging GPS) มีดาวเทียม 28 ดวง ใช้งานจริง 24 ดวง อีก 4 ดวงเป็นตัวสำรอง บริหารงานโดย Department of Defenses มีรัศมีวงโคจรจากพื้นโลก 20,162.81 กม.หรือ 12,600 ไมล์ ดาวเทียมแต่ละดวงใช้ เวลาในการโคจรรอบโลก 12 ชั่วโมง
- ยุโรป ชื่อ Galileo มี 27 ดวง บริหารงานโดย ESA หรือ European Satellite Agency จะพร้อมใช้งานในปี 2008
- รัสเซีย ชื่อ GLONASS หรือ Global Navigation Satellite บริหารโดย Russia VKS (Russia Military Space Force) ในขณะนี้ภาคประชาชนทั่วโลกสามารถใช้ข้อมูลจากดาวเทียมของทางอเมริกา (NAVSTAR) ได้ฟรี เนื่องจาก นโยบายสิทธิการเข้าถึงข้อมูลและข่าวสารสำหรับประชาชนของรัฐบาลสหรัฐ จึงเปิดให้ประชาชนทั่วไปสามารถใช้ข้อมูลดังกล่าวในระดับความแม่นยำที่ไม่เป็นภัยต่อความมันคงของรัฐ กล่าวคือมีความแม่นยำในระดับบวก / ลบ 10 เมตร

2. ส่วนควบคุม ประกอบด้วยสถานีภาคพื้นดิน สถานีใหญ่อยู่ที่ Falcon Air Force Base ประเทศ อเมริกา และศูนย์ควบคุมย่อยอีก 5 จุด กระจายไปยังภูมิภาคต่าง ๆ ทั่วโลก

3. ส่วนผู้ใช้งาน ผู้ใช้งานต้องมีเครื่องรับสัญญาณที่สามารถรับคลื่นและแปรรหัสจากดาวเทียมเพื่อนำมาประมวลผลให้เหมาะสมกับการใช้งานในรูปแบบต่าง ๆ

2.2.1.1 หลักการพื้นฐานของ GPS เป็นเรื่องง่ายๆ แต่อุปกรณ์ของเครื่องมือจะต้องถูกสร้างขึ้นด้วยวิทยาการขั้นสูง GPS ทำงานโดยการรับสัญญานจากดาวเทียมแต่ละดวง สัญญาณดาวเทียมนี้ประกอบไปด้วยข้อมูลที่ระบุตำแหน่งของดาวเทียมดวงนั้นๆ และเวลาขณะส่งสัญญาณ เครื่องรับสัญญาณ GPS จะต้องประมวลผลความแตกต่างของข้อมูลเวลา (ขณะส่งสัญญาณ) ที่ได้รับเทียบกับเวลาจริง ณ ปัจจุบัน เพื่อแปรเป็นระยะทางระหว่างเครื่องรับสัญญานกับดาวเทียมแต่ละดวง

การทำงานของเครื่องรับสัญญาณ GPS มีหลักการและข้อควรคำนึงถึงดังต่อไปนี้ คือ

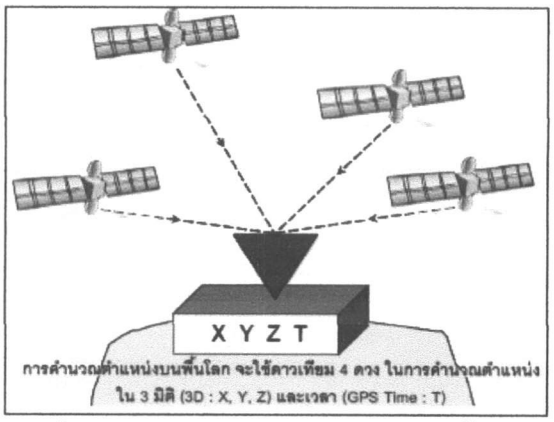
1. การรับสัญญาณจากดาวเทียมโดยหลักการรูปสามเหลี่ยม ระหว่างดาวเทียมกับเครื่องรับ

2. การหาระยะทาง ระหว่างเครื่องรับและดาวเทียมใช้การคำนวนจากเวลาเดินทางของคลื่นวิทยุ

3. ในดาวเทียมและเครื่องรับสัญญาณ GPS จาเป็นจะต้องมีนาฬิกาที่มีความละเอียดสูงมา

4. นอกจากระยะทางแล้วจะต้องทราบตำแหน่งของดาวเทียมที่อยู่ในอวกาศด้วย

5. ความเร็วของคลื่นวิทยุจะเดินทางได้ช้าลงในชั้นบรรยากาศไอโอโนสเฟียร์ (Ionosphere) และชั้นบรรยากาศโลก (Atmosphere) จึงต้องทำการปรับแก้ สำหรับจุดนี้ด้วย



รูปที่ 2.6 แสดงการคำนวณตำแหน่งบนพื้นโลก

2.2.1.2 การรับสัญญาณจากดาวเทียม

ดาวเทียมจะเป็นเหมือนหมุดหลักฐานสำหรับการคำนวณหาตำแหน่งโดยใช้หลักการรูปสามเหลี่ยม เครื่องรับสัญญาณ GPS จะต้องคำนวณหาระยะระหว่างดาวเทียมกับตัวของมันเอง สิ่งที่เราต้องรู้เพื่อใช้ในการคำนวณคือ ตำแหน่งของดาวเทียมดวงนั้นเพื่อให้ได้ระยะทางที่ถูกต้อง สมมุติว่าเราคำนวณได้ว่าเราอยู่ห่างจากดาวเทียม A 11,000 ไมล์ ขณะเดียวกันเราก็อยู่ห่างจากดาวเทียม B 12,000 ไมล์ ดังนั้นตำแหน่งของเราจึงอยู่บนโลกทรงกลม (จุดสีแดง) ณ ตำแหน่งที่ดาวเทียม A (รัศมี 11,000 ไมล์) และดาวเทียม B (12,000 ไมล์) ตัดกัน ดังนั้นถ้าเราได้ระยะจากดาวเทียมมากดวงขึ้น ก็จะสามารถบอกตำแหน่งได้แน่นอนยิ่งขึ้น เช่น ถ้าเรารู้ว่าอยู่ห่างจากดาวเทียม C เป็นระยะ 13,000 ไมล์ ก็จะบอกตำแหน่งที่ทรงกลมตัดกันได้ 2 จุด ถ้าเราวัดหาระยะดาวเทียมดวงที่ 4 ได้ จะยิ่งคำนวณตำแหน่งได้แม่นยำยิ่งขึ้น อย่างไรก็ดี จากการวัดระยะดาวเทียม 3 ดวงก็สามารถบอกตำแหน่งได้แล้ว ระยะห่างจากดาวเทียมทั้ง 3 ดวงกับเครื่องรับสัญญาณ GPS จะสามารถระบุตำแหน่งบนผิวโลกได้หากพื้นผิวโลกแบนเป็นแนวราบ เช่น ในทะเล จะเลือกใช้วัดแบบ 2D (2 มิติ) คือ พิกัดราบอย่างเดียวได้ แต่ในความเป็นจริงพื้นผิวโลกมีความโค้งเว้าเนื่องจากสัณฐานของโลกมีลักษณะกลมแป้นและประกอบไปด้วยพื้นที่ราบและเทือกเขาสูงต่างๆ ดังนั้นหากต้องการได้ตำแหน่ง 3D (3 มิติ) จะต้องวัดจากดาวเทียม 4 ดวง จึงจะทำให้สามารถคำนวณหาความสูงได้เพื่อทำให้ได้ค่าพิกัดตำแหน่งที่ถูกต้องมากขึ้น

2.2.1.3 การวัดระยะจากดาวเทียม

การวัดระยะห่างระหว่างดาวเทียมกับเครื่องรับทำได้โดยการใช้สมการง่ายๆ คือ ระยะทาง = ความเร็ว * ระยะเวลา ตัวอย่างวิธีการคำนวณ เช่น ถ้ารถยนต์คันหนึ่งเคลื่อนที่ด้วยความเร็ว 60 กม./ชม. เป็นเวลา 2 ชม. รถยนต์คันนี้จะเคลื่อนที่ได้เป็นระยะทางเท่าใด? วิธีการคิดจะใช้ความเร็ว (60 กม./ชม.) คูณกับเวลาที่รถวิ่ง (2 ชม.) ได้ระยะทาง (120 กม.) ระบบ GPS ก็เช่นเดียวกัน ทำงานโดยการหาว่าสัญญาณวิทยุที่ส่งออกมาจากดาวเทียมจนถึงเครื่องรับใช้เวลาเดินทางนานเท่าไร แล้วจึงนำ

เวลาที่หาได้มาคำนวณหาระยะทางโดยที่เราทราบว่าคลื่นวิทยุเดินทางด้วยความเร็วแสง คือ 186,000 ไมล์/วินาที ดังนั้นถ้าเรารู้เวลาที่แน่นอนในขณะที่ดาวเทียมเริ่มปล่อยสัญญาณวิทยุ และเวลาที่เราเริ่มรับสัญญาณนั้นได้ ก็จะได้เวลาที่คลื่นวิทยุเดินทาง นำมาคูณกับความเร็วในการของคลื่น (186,000 ไมล์) ก็จะได้ระยะทางระหว่างเครื่องรับสัญญาณกับดาวเทียม เราต้องได้ระยะเช่นนี้เป็นจานวน 3 ค่า จากดาวเทียม 3 ดวง จึงจะสามารถคำนวณหาตำแหน่งได้

เมื่อหลักการคำนวณเป็นเช่นนี้ แน่นอนว่านาฬิกาที่ใช้ในเครื่องรับสัญญาณ GPS และที่ติดตั้งบนดาวเทียมจะต้องเป็นนาฬิกาที่ดีมากๆ เพราะเวลาที่วัดได้จะต้องน้อยมาก เนื่องจากแสงเดินทางเร็วมาก โดยปกติถ้าดาวเทียมดวงที่ส่งสัญญาณอยู่เหนือศีรษะเราพอดีคลื่นวิทยุจะใช้เวลาเพื่อเดินทางมาถึงเราเพียง 0.06 วินาทีเท่านั้น ด้วยเหตุนี้ GPS จึงได้นำเอาวิวัฒนาการทางอิเลคทรอนิคส์มาใช้ การที่จะได้ความถูกต้องของเวลาในระดับที่ GPS ต้องการ จะต้องใช้นาฬิกาอิเลคทรอนิคส์ที่มีราคาแพงมาก ซึ่งให้เวลาที่ละเอียดถูกต้องสูง นาฬิกาดาวเทียมจะอ่านเวลาได้เป็นนาโนเซคกัน (Nano second) หรือ 0.000000001 วินาที เรารู้เวลาที่สัญญาณเริ่มส่งจากดาวเทียมได้อย่างไร? เคล็ดลับที่สำคัญในการหาเวลาการเดินทางของคลื่นวิทยุก็คือ ต้องรู้ว่าเวลาที่แน่นอนที่สัญญาณเริ่มถูกปล่อยออกจากดาวเทียม ผู้ออกแบบเครื่อง รับสัญญาณ GPS ใช้หลักการจาลองแบบสัญญาณที่อยู่ในเครื่องรับให้เหมือนกันกับที่ส่งจากดาวเทียม และเครื่องทั้งสองจะต้องสร้างรหัสในเวลาที่ตรงกัน (Pseudo Random Code) ดังนั้นสิ่งที่เราต้องกระทำก็คือ การรอรับรหัสที่ดาวเทียมปล่อยออกมา และมองย้อนกลับไปว่าเครื่องของเราได้เริ่มสร้างรหัสที่มีรูปร่างเหมือนกันแล้วเป็นเวลานานเท่าใด เวลาที่แตกต่างก็คือ เวลาที่คลื่นวิทยุใช้ในการเดินทางมาถึงเครื่องรับ การที่ต้องสร้างรหัสให้เป็นชุดรหัสเชิงตัวเลขที่ซับซ้อนก็เพื่อสามารถนำรหัส ทั้งสองมาเปรียบเทียบกันได้ง่ายและไม่วุ่นวาย นอกจากนี้ ด้วยเหตุผลทางวิชาการแล้ว รหัสซ้ำซ้อนนี้จะทำให้มองเห็นเหมือนคลื่นวิทยุที่ต่อเนื่องกันยาวๆ

2.2.1.4 การคำนวณหาเวลาที่ถูกต้อง

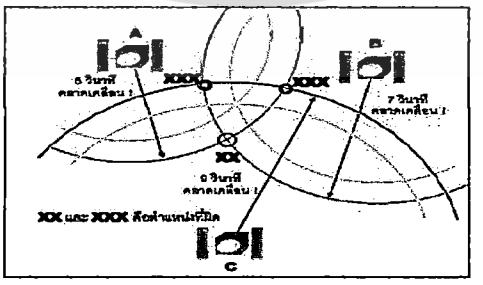
เมื่อแสงเดินทางด้วยความเร็ว 186,000 ไมล์/วินาที จะเกิดอะไรขึ้นหากเครื่องรับสัญญาณบันทึกเวลาคลาดไป 1/100 วินาที ผลก็คือ เราจะคำนวณระยะทางผิดไปถึง 1,860 ไมล์ และเราจะมั่นใจได้อย่างไรว่านาฬิกาที่ใช้มีความถูกต้องแม่นยำ ปัญหานี้สามารถอธิบายให้เกิดความมั่นใจได้ว่านาฬิกาที่ติดตั้งอยู่ในดาวเทียมใช้ นาฬิกาอะตอม ซึ่งจะให้เวลาที่ถูกต้อง ดาวเทียมแต่ละดวงจะมีนาฬิกาอะตอมนี้ติดตั้งอยู่ถึง 4 เครื่อง นาฬิกาอะตอมไม่ได้เดินด้วยพลังงานอะตอม ที่ให้ชื่อว่าอะตอมเป็นเพราะใช้การวัดจังหวะจากอนุภาคของสารเฉพาะ เหมือนเครื่องเคาะจังหวะ อะตอมนี้จะให้เวลาที่แน่นอนและถูกต้องที่สุดที่มนุษย์เราประดิษฐ์ขึ้นมาได้ ดังนั้นถ้านาฬิกาบอกเวลาเที่ยง 12:00 น. ก็หมายถึงเวลาเที่ยง 12:00 จริงๆ ในกรณีนี้แม้ว่านาฬิกาที่ติดตั้งอยู่ในเครื่องรับสัญญาณ GPS จะเป็นนาฬิกาที่มีความถูกต้องธรรมดาเท่านั้น ก็ยังสามารถอาศัยการวัดระยะจากดาวเทียมเข้า

มาช่วยได้ โดยทำการวัดระยะจากดาวเทียมเพิ่มอีกหนึ่งดวงเพื่อใช้ในการปรับแก้เวลาของเครื่องรับที่ไม่สมบูรณ์ ในขั้นต่อไปจะได้อธิบายให้เห็นว่าการวัดระยะจากดาวเทียมเพิ่มอีกหนึ่งดวงสามารถช่วยได้อย่างไร

หากว่านาฬิกาในเครื่องรับสัญญาณ GPS ส่วนใหญ่เป็นควอทซ์ ซึ่งไม่เที่ยงตรงเท่ากับนาฬิกาอะตอม สมมุตินาฬิกาภายในเครื่องรับสัญญาณเดินช้าไป 1 วินาที ถ้าตัวเครื่องบอกเวลาเที่ยงตรง เวลาจริงก็จะเป็น 12:00:01 น. ปกติเราใช้หน่วยวัดระยะไมล์หรือกิโลเมตร แต่เนื่องจากระยะทางในการคำนวณภายในเครื่องรับสัญญาณ GPS คำนวณจากเวลา ดังนั้นจะกล่าวถึงเวลาแทนระยะทาง สมมุติว่าความจริงเราอยู่ห่างจากดาวเทียม A เป็นเวลา 4 วินาที และห่างจากดาวเทียม B เป็นเวลา 6 วินาที คิดในแนวระนาบสองมิติ จะหาจุดที่เส้นตัดกันได้ สมมุติตัดกันได้ที่ตำแหน่ง X

ดังนั้นที่ X คือ ตำแหน่งที่เราอยู่จริง และเราควรจะคำนวณได้ค่า X ถ้านาฬิกาทำงานถูกต้อง แต่หาก นาฬิกาเครื่องรับสัญญาณเดินช้าไป 1 วินาที เครื่องรับสัญญาณก็จะระบุระยะจาก A 5 วินาที และ ระยะจากดาวเทียม B 7 วินาที ทำให้เส้นตัดกันที่จุด XX ดังนั้นเครื่องรับสัญญาณก็จะบอกเวลาที่ XX และถ้าเราไม่มีวิธีที่จะรู้ว่าเครื่องรับเดินช้า เราก็จะคิดว่าตำแหน่งที่ได้ถูกต้องแล้ว แต่ในความเป็นจริงระยะที่ได้อาจคลาดเคลื่อนเป็นกิโลเมตรก็ได้ และเราจะรู้ว่าไม่ถูกต้องก็เมื่อเราเดินตามที่เครื่องบอกแล้วจุดนั้นไม่ตรงกับความเป็นจริง เช่น เข้าไปในกำแพงหรือภูเขา แต่ในการคำนวณจะไม่ แสดงให้เรารู้ได้เลย

ตามหลักวิชาตรีโกณเพื่อหาตำแหน่ง เราต้องมีจุดอ้างอิงเพิ่มขึ้นอีกหนึ่งจุด เพื่อวัดระยะทางเพิ่มขึ้นอีกหนึ่งเส้นตามรูปที่แสดง ซึ่งในที่นี้ ก็จะเป็นระยะจากดาวเทียมดวงที่สาม สมมติว่าถ้าระยะจริงจากดาวเทียม C มีค่า 8 วินาที จะเห็นวงกลมทั้งสามวงตัดกันตามรูป แต่หากว่าเราเพิ่มระยะทางของรัศมี แต่ละวงอีกหนึ่งวินาทีตามค่าช้าของนาฬิกา แสดงในรูปด้วยเส้นประซึ่งจะเป็นระยะเทียม (Pseudo Range) ที่เกิดจากการที่นาฬิกาเดินช้า คาว่า Pseudo Range ใช้ในวงการ GPS เพื่อบอกว่าระยะที่ คำนวณได้นั้นยังมีค่าผิดพลาดอยู่(ซึ่งโดยปกติแล้วจะเกิดจากเวลา)



รูปที่ 2.7 แสดงการทำของวงกลมจากดาวเทียม A ดาวเทียม B ตัดกันที่จุด XX

จากภาพจะเห็นได้ว่า วงกลมจากดาวเทียม A ดาวเทียม B ตัดกันที่จุด XX แต่วงกลมจากดาวเทียม C จะไม่ตัดตรงจุดเดียวกัน (ทั้งที่ความจริงเราทราบว่าหากเครื่องมือและการคำนวณทุก

อย่างถูกต้องวงกลมทั้งสามของดาวเทียม A 4 วินาที B 6 วินาที และ C 8 วินาที จะต้องตัดที่จุดเดียวกัน) ดังนั้นจึงทราบได้ว่า การวัดมีความบกพร่องเกิดขึ้นเนื่องจากไม่มีจุดที่จะเกิดขึ้นได้จริงจากการที่ระยะห่างจากดาวเทียม A 5 วินาที B 7 วินาที และC 9 วินาที ภายในเครื่องรับ GPS จะมีโปรแกรมที่จะนาชุดของการวัดที่ไม่สมบูรณ์มาคำนวณ และหาค่าที่นาพิกาเดินคลาดเคลื่อนมาปรับแก้ให้ถูกต้อง

ขั้นตอนการปรับแก้ความคลาดเคลื่อนทำโดยการลบ (หรือบวก) เวลาให้กับทุกๆ ค่าโดยเท่าๆ กัน จนกว่าจะได้ค่าคำตอบที่ทุกๆ ระยะมาตัดกันที่ตำแหน่งเดียวกัน สำหรับกรณีตัวอย่างนี้สุดท้ายโปรแกรมก็จะพบว่าการลบเวลาออกจากระยะที่วัดได้หนึ่งวินาทีจะทำให้วงกลมทั้งสามตัดกันที่จุดเดียวกัน จึงแสดงได้ว่านาพิกาเดินช้าไป 1 วินาที ที่จริงแล้ว วิธีการที่โปรแกรมภายในเครื่องรับสัญญาณ GPS ใช้ในการคำนวณหาคำตอบนั้นใช้หลักการง่ายๆ ของการแก้สมการพิชคณิต 4 สมการนั่นเอง ดังนั้นแนวคิดก็คือ การรับสัญญาณจากดาวเทียมเพิ่มขึ้นอีกหนึ่งดวงจะทำให้สามารถขจัดความคลาดเคลื่อนของเวลาที่เกิดจากนาพิกาเดินไม่ถูกต้องได้ดียิ่งขึ้น (เนื่องจากมีตัวแปรให้แก้สมการเพิ่ม) การวัดหาค่าแบบ 3 มิติ ต้องการใช้ดาวเทียม 4 ดวง ได้ค่าการวัดถึง 4 ค่าเพื่อจะได้กำจัดข้อผิดพลาดที่อาจเกิดขึ้น

การออกแบบระบบ GPS นั้น จะมีดาวเทียมอย่างน้อย 4 ดวง บนท้องฟ้าเสมอ ทุกตำแหน่ง การออกแบบเครื่องรับสัญญาณ GPS จะต้องทำให้สามารถรับสัญญาณดาวเทียมได้ 4 ดวงด้วย โดยมีหลักอยู่ว่า ถ้าต้องการให้เครื่องแสดงผลการวัดต่อเนื่องและเป็นแบบทันทีทันใด (Real Time) เครื่องรับต้องมีช่องรับสัญญาณ 4 ช่อง โดยช่องรับสัญญาณแต่ละช่องจะรับสัญญาณจากดาวเทียมแยกแต่ละดวง เพื่อจะสามารถรับสัญญาณ 4 ดวงในเวลาพร้อมกันได้ และประมวลผลค่าตำแหน่งพิกัดแบบทันทีทันใดได้อย่างต่อเนื่อง แต่สำหรับการใช้งานบางครั้งก็ไม่ต้องการความถูกต้องและแสดงผลรวดเร็วทันที ในกรณีนี้เครื่องรับสัญญาณเพียงช่องเดียวอาจเพียงพอสำหรับการใช้งาน เครื่องรับสัญญาณที่มีช่องรับสัญญาณช่องเดียวจะทำการรับดาวเทียม 4 ดวงได้โดยการจัดลำดับเรียงการรับสัญญาณจากดาวเทียมจนครบทั้ง 4 ดวง จึงนาค่าเวลาที่ได้มาประมวลผลเวลา การคำนวณนี้อาจใช้เวลาระหว่าง 2 - 30 วินาที ซึ่งในการใช้งานบางอย่างก็เร็วพอเพียงแล้ว ข้อเสียที่ชัดเจนของเครื่องรับประเภทนี้คือ จะทำงานในการหาความเร็วได้ไม่ดี การใช้หาความเร็วเป็นการใช้ประโยชน์อย่างหนึ่งของเครื่องรับสัญญาณ GPS เครื่องสามารถแสดงความเร็วในการเดินทางได้ถูกต้องมาก สำหรับเครื่องรับประเภทหนึ่งช่องสัญญาณ หากเครื่องรับมีการเคลื่อนไหวในขณะที่ทำการรับสัญญาณจากดาวเทียมอยู่นั้น จะมีผลทำให้การคำนวณค่าตำแหน่งมีความผิดพลาดได้มาก

ข้อเสียอีกประการหนึ่งของเครื่องรับสัญญาณช่องเดียวจะเกิดขึ้นเมื่อดาวเทียมส่งรายงานสภาพระบบ(System Condition Message) สำหรับการเปลี่ยนรับดาวเทียมดวงใหม่ ซึ่งต้องใช้เวลาติดต่อถึง 30 วินาที ในเวลานั้นเครื่องรับสัญญาณจะไม่สามารถคำนวณทิศทางได้ ดังนั้นเครื่องรับสัญญาณ GPS ที่ได้รับความนิยมใช้ก็คือ เครื่องรับสัญญาณที่มี 2 ช่องรับสัญญาณ โดยในการทำงาน

ช่องหนึ่งจะทำการคำนวณหาเวลาในขณะที่อีกช่องหนึ่งพยายามจับคลื่นวิทยุจากดาวเทียมดวงต่อไป เมื่อช่องแรกวัดเสร็จก็สามารถเปลี่ยนไปรับสัญญาณดาวเทียมดวงใหม่ได้ทันที โดยไม่ต้องเสียเวลาในการค้นหาและรับสัญญาณดาวเทียมอย่างเครื่องรับสัญญาณประเภทช่องเดียว

2.2.1.5 ต้องรู้ตำแหน่งของดาวเทียมก่อน

การคำนวณที่กล่าวมาทั้งหมดจะทำได้ต่อเมื่อเรารู้ตำแหน่งของดาวเทียมแล้วเท่านั้น จึงจะสามารถสร้างรูปสามเหลี่ยมขึ้นมาคำนวณตามหลักตรีโกณได้ ทีนี้ปัญหาก็คือ เราจะรู้ตำแหน่งของดาวเทียมที่อยู่สูงถึง 11,000 ไมล์ ได้อย่างไร? จริงๆ แล้วเป็นเรื่องที่ง่ายมาก เนื่องจากวัตถุที่อยู่ที่ระดับความสูงผ่านพ้นจากชั้นบรรยากาศของโลกระดับนี้จะไม่มีคลื่นจากโลกไปรบกวนได้ ซึ่งหมายความว่า วงโคจรดาวเทียมรอบโลกสามารถแสดงได้ด้วยสมการคณิตศาสตร์ธรรมดาเหมือนกับดวงจันทร์ที่หมุนรอบโลกเป็นเวลาล้านๆ ปี โดยไม่มีการเปลี่ยนแปลง

ดาวเทียม GPS ที่ถูกปล่อยขึ้น โดยกองทัพอากาศสหรัฐจะเดินตามแนววงโคจรที่กำหนดไว้แน่นอน และเนื่องจากในอวกาศว่างเปล่าไม่มีแรงเสียดทาน ดาวเทียมก็จะโคจรอยู่ในแนวที่แน่นอนตามกำหนด เมื่อวงโคจรของดาวเทียมแต่ละดวงถูกกำหนดไว้ล่วงหน้าแล้ว เครื่องรับ GPS ก็สามารถบันทึกตารางดาวเทียม (Almanac) ไว้ในหน่วยความจำได้ ตารางดาวเทียมนี้จะบอกได้ว่าบนท้องฟ้าจะมีดาวเทียมดวงไหนขึ้นลงเวลาใดบ้าง

แม้ว่าดาวเทียมจะเคลื่อนที่ตามตัวเลขสมการวงโคจรที่ถูกต้องของมันเองอยู่แล้ว แต่เพื่อให้ทุกอย่างถูกต้องสมบูรณ์ กระทรวงกลาโหมสหรัฐฯ จึงต้องทำการติดตามการโคจรของดาวเทียมทุกดวงอย่างสม่ำเสมอ การที่ต้องติดตามการโคจรของดาวเทียมนี้เป็นเหตุผลหนึ่งที่ทำให้ต้องสร้างดาวเทียม GPS ให้เดินทางเร็วกว่าการหมุนของโลก ดาวเทียมหมุนรอบโลกครบหนึ่งรอบทุกๆ 12 ชั่วโมง และจะโคจรผ่านสถานีติดตามดาวเทียมของ DoD (Department of Defense) วันละ 2 ครั้ง ทำให้สถานีติดตามนี้สามารถวัดความสูง ตำแหน่ง และความเร็วของดาวเทียมได้อย่างถูกต้อง โดยสถานีจะติดตามค้นหาความแปรเปลี่ยนของวงโคจร เรียกว่า ค่าความคลาดเคลื่อนของอีฟีเมอริส (Ephemeris Error) ซึ่งปกติจะมีขนาดน้อยมาก เป็นความคลาดเคลื่อนที่เกิดจากแรงดึงดูดของดวงจันทร์และดวงอาทิตย์ และการแผ่รังสีดวงอาทิตย์ที่มีต่อดาวเทียม

เมื่อ DoD วัดค่าตำแหน่งของดาวเทียมได้ ค่าตำแหน่งใหม่นี้ก็จะถูกส่งกลับเข้าไปบันทึกไว้ในดาวเทียมดวงนั้น ดาวเทียมก็จะส่งค่าแก้นี้พร้อมกับข้อมูลอื่นๆ ให้เครื่องรับ ดาวเทียม GPS ไม่เพียงแต่ส่งรหัส Pseudo Random เพื่อใช้ในการหาเวลาเท่านั้น แต่ยังส่งข้อมูลเกี่ยวกับตำแหน่งของวงโคจรและค่าความสมบูรณ์ของระบบด้วย เครื่องรับสัญญาณ GPS ใช้ข้อมูลนี้ควบคู่กับตารางดาวเทียมที่ติดตั้งไว้ในตัวเครื่องในการคำนวณตำแหน่งที่ถูกต้องของดาวเทียม

ความคลาดเคลื่อนของการคำนวณพิกัดตำแหน่งที่อาจเกิดขึ้นจากการรับสัญญาณ

เราทราบแล้วว่าทุกส่วนในระบบ GPS ถูกสร้างและจัดทำขึ้นเพื่อให้ได้ความถูกต้องและแม่นยำสูงสุด เช่น ใช้นาฬิกาอะตอมในดาวเทียม การวัดระยะห่างจากดาวเทียมเพิ่มขึ้นอีกหนึ่งดวงเพื่อใช้ขจัดความคลาดเคลื่อนของนาฬิกาในเครื่องรับ และการส่งข้อมูลรายงานค่าปรับแก้วงโคจรทุกนาทีจากดาวเทียม แต่ความแม่นยำของการคำนวณพิกัดตำแหน่งในเครื่องรับสัญญาณ GPS นั้นขึ้นอยู่กับปัจจัยต่างๆ หลายปัจจัย ทั้งที่ผู้ใช้สามารถควบคุมได้และที่ไม่สามารถควบคุมได้ ในที่นี้จะขอนำเสนอปัจจัยหลักๆ ที่มีผลให้เกิดความคลาดเคลื่อนของการคำนวณพิกัดตำแหน่ง ดังนี้

1. ตำแหน่งของดาวเทียมที่รับสัญญาณ กล่าวคือ ถ้ากลุ่มดาวเทียมอยู่ห่างกันย่อมให้ค่าที่แม่นยำมากกว่ากลุ่มที่อยู่ใกล้กัน และยิ่งมีจำนวนดาวเทียมที่รับสัญญาณได้มากก็ยิ่งมีความแม่นยำมากยิ่งขึ้น

2. นอกจากตำแหน่งและการวางตัวของดาวเทียมนอกชั้นบรรยากาศโลกแล้ว ความแปรปรวนของชั้นบรรยากาศ ยังเป็นอีกปัจจัยหนึ่งที่มีผลกระทบต่อความถูกต้องแม่นยำของเครื่องรับสัญญาณ GPS เนื่องจากชั้นบรรยากาศประกอบด้วยประจุไฟฟ้า ความชื้น อุณหภูมิ และความหนาแน่น ที่เปลี่ยนแปลงตลอดเวลา เมื่อคลื่นตกกระทบอนุภาคเหล่านี้ จะเกิดการหักเหและทำให้สัญญาณที่ได้อ่อนลง

3. สัญญาณส่วนที่สามารถเดินทางผ่านชั้นบรรยากาศลงมายังผิวโลกได้ยังอาจถูกหักเหโดยปัจจัยสภาพแวดล้อมในบริเวณรับสัญญาณ ความคลาดเคลื่อนชนิดนี้เรียกว่า ความคลาดเคลื่อนจากการรับสัญญาณสะท้อนจากหลายทิศทาง (Multipath Error) อันเนื่องจากสภาพแวดล้อมรอบๆ บริเวณ ค่าความผิดพลาดแบบนี้เกิดขึ้นเนื่องจากเครื่องรับได้รับสัญญาณทั้งจากดาวเทียมโดยตรงและสัญญาณที่สะท้อนจากสัญญาณดังกล่าว ซึ่งสะท้อนจากสิ่งที่อยู่รอบบริเวณรับสัญญาณ ไม่ว่าจะเป็น ตึก ภูเขา หรือต้นไม้ สัญญาณส่วนนี้ไม่ได้เป็นสัญญาณจากดาวเทียม และมีผลต่อการรับเหมือนกับที่เกิดกับการรับสัญญาณทีวีเช่นเดียวกัน คือ ทำให้เกิดภาพพร่าซ้อนให้เห็นบนจอ สิ่งเหล่านี้มีผลต่อความถูกต้องแม่นยำในการคำนวณพิกัดตำแหน่งทั้งสิ้น เนื่องจากถ้าสัญญาณจากดาวเทียมมีการหักเหก็จะทำให้ค่าที่คำนวณได้จากเครื่องรับสัญญาณเพี้ยนไป ค่าความผิดพลาดแบบนี้สามารถลดได้โดยการทำ Position Fix Averaging เครื่องรับสัญญาณ GPS รุ่นใหม่ ใช้วิธีการประมวลผล ที่ดีขึ้นและมีการใช้เสาอากาศที่ป้องกันสัญญาณซ้อนได้ แต่ในบางครั้งถ้าสัญญาณสะท้อนมีความรุนแรงมาก ก็ยังอาจมีผลต่อการวัดพิกัดตำแหน่งได้เหมือนกัน นอกจากนี้ ในบางครั้งเมื่อถูกรบกวนด้วยคลื่นวิทยุ อาจทำให้รหัส Pseudo Random มีลักษณะผิดเพี้ยนทำให้โปรแกรมการคำนวณทำงานไม่ถูกต้อง ความคลาดเคลื่อนอาจมีขนาดเล็กมากหรือขนาดใหญ่มากก็ได้ ค่าที่ใหญ่จะสามารถรู้ได้ง่ายกว่าเนื่องจากเห็นได้ชัดเจน แต่ถ้าค่าความคลาดเคลื่อนมีขนาดเล็กจะเป็นการยากที่จะหาได้พบ ความคลาดเคลื่อนแบบนี้มีผลทำให้การบอกตำแหน่งผิดไปประมาณ 0.5 - 1 เมตร

4. อีกสาเหตุของความคลาดเคลื่อนที่กาจัดได้ยาก ได้แก่ ความคลาดเคลื่อนที่เกิดจากบรรยากาศชั้นไอโอโนสเฟียร์ ซึ่งเป็นชั้นของอนุภาคประจุไฟฟ้า อยู่สูงจากโลกระหว่าง 80 - 120 ไมล์ อนุภาคเหล่านี้มีผลต่อความเร็วของแสงและความเร็วของสัญญาณวิทยุจากดาวเทียม GPS เช่นกัน บางคนอาจคิดว่าความเร็วของแสงเป็นค่าคงที่อยู่ตลอดเวลา แต่ความเป็นจริงคลื่นแสงเดินทางด้วยความเร็วคงที่เมื่ออยู่ในสุญญากาศเท่านั้น ซึ่งเป็นสภาพที่อยู่ในอวกาศที่สูงจากผิวโลกมากๆ แต่เมื่อคลื่นแสงหรือคลื่นวิทยุเดินทางผ่านตัวกลางที่มีความหนาแน่น เช่น ชั้นบรรยากาศที่มีอนุภาคประจุไฟฟ้าซึ่งมีความหนาหลายไมล์ย่อมทำให้ความเร็วลดลงบ้าง และการที่คลื่นวิทยุเดินทางช้าลงนี้จะมีผลทำให้คำนวณระยะทางได้ไม่ถูกต้อง

วิธีการที่ใช้ลดความคลาดเคลื่อนจากการที่สัญญาณเดินทางช้ามีอยู่ด้วยกันสองวิธี วิธีที่หนึ่ง เราต้องรู้ค่าความแปรเปลี่ยนเฉลี่ยรายวันตามสภาพบรรยากาศชั้นไอโอโนสเฟียร์ จึงสามารถนำมาปรับแก้กับทุกค่าที่วัดได้ช่วยให้ได้ความถูกต้องสูงขึ้น แต่ความจริงแล้วสภาพอากาศจะไม่คงที่ตลอดเวลา ดังนั้นการนำค่าเฉลี่ยมาใช้จึงไม่ถูกต้องทั้งหมด อีกวิธีหนึ่งที่ใช้ในการลดความคลาดเคลื่อนทำโดยการวัดหาค่าความแปรความเร็วของคลื่นวิทยุ โดยการวัดความเร็วสัมพัทธ์ของสัญญาณสองแบบ ที่ส่งมาจากดาวเทียมพร้อมๆ กัน แนวคิดพื้นฐานของวิธีนี้คือ เมื่อแสงเดินทางผ่านชั้นบรรยากาศ ไอโอโนสเฟียร์จะเดินทางช้าลงเป็นอัตราส่วนกลับกับความถี่ของสัญญาณยกกาลังสอง ถ้าความถี่ยิ่งต่ำการเดินทางจะยิ่งช้าลง เมื่อทำการเปรียบเทียบเวลาที่สัญญาณความถี่ต่างกันเดินทางถึงเครื่องรับก็จะได้ค่าของเวลาที่คลื่นเดินทางช้าลงไป วิธีการนี้มักใช้กับเครื่องรับสัญญาณ GPS ที่มีความละเอียดถูกต้องสูง หรือที่เรียกว่า เครื่องรับสัญญาณความถี่คู่ (Dual Frequency) เครื่องแบบนี้จะขจัดค่าความคลาดเคลื่อนจากไอโอโนสเฟียร์ได้มาก

5. ค่าความผิดพลาดที่แก้ไขได้อีกแบบหนึ่งคือ ผลของ Selective Availability (SA) ซึ่ง SA เป็นมาตรการที่กระทรวงกลาโหมสหรัฐฯ ใช้ในการทำให้ค่าความแม่นยำของเครื่องรับสัญญาณ GPS ลดต่ำลง หรือเกิดความผิดพลาดสูงขึ้น โดยการใส่ค่าความผิดพลาดเข้าไปในสัญญาณ GPS ที่ส่งออกจากดาวเทียม ซึ่งเป็นมาตรการที่ทำเพื่อผลประโยชน์ทางทหารสำหรับสหรัฐอเมริกา และกองกาลังพันธมิตร ค่าความผิดพลาดทั้งหมดที่กล่าวนี้มีความเหมือนกันอยู่อย่างหนึ่งคือ ปริมาณและทิศทางของค่าความผิดพลาด ในเวลาใดเวลาหนึ่งจะไม่มีการเปลี่ยนแปลงอย่างกะทันหัน ดังนั้นเครื่องรับ GPS 2 เครื่องที่อยู่ในระยะห่างกันไม่มากนัก จะได้รับผลกระทบจากค่าความผิดพลาดในปริมาณและทิศทางที่เท่ากันหรือใกล้เคียงกัน ดังนั้นเราจึงสามารถทำการหาค่าความผิดพลาดดังกล่าวได้

6. อีกปัจจัยที่มีผลต่อความแม่นยำของการคำนวณค่าพิกัดตำแหน่งก็คือ ประสิทธิภาพของตัวเครื่อง รับสัญญาณเองว่ามีความไวในการรับสัญญาณและความเร็วในการประมวญผลมากน้อยเพียงใด ปัญหาในส่วนนี้ได้รับการแก้ไขจากบริษัทผู้ผลิตอย่างต่อเนื่อง สาเหตุของการเกิดการคลาดเคลื่อนทั้งหมดที่กล่าวมาเป็นผลทำให้การระบุพิกัดตำแหน่ง หรือการวัดระยะทางของ

เครื่องรับสัญญาณ GPS มีความไม่แน่นอน ซึ่งหมายความว่า แทนที่จะกล่าวได้ว่าของชิ้นหนึ่งอยู่ห่างไป 10 เมตร พอดี กลับต้องกล่าวว่าของอยู่ห่างไป 10 เมตร บวกหรือลบเศษหนึ่งส่วนสิบเซนติเมตร เป็นต้น อย่างไรก็ตาม ค่าความคลาดเคลื่อนทั้งหมดเมื่อรวมกันแล้วก็ยังไม่มากนัก ความถูกต้องจะสูงยิ่งขึ้นถ้าเครื่องรับสัญญาณมีคุณภาพดี เพื่อให้ได้ค่าความถูกต้องที่ดีที่สุดเครื่องรับสัญญาณที่ดีจะใช้หลักการของวิชาเรขาคณิต ซึ่งเรียกว่า Geometric Dilution of Precision (GdoP) GdoP เป็นค่าที่ชี้ให้เห็นความถูกต้องของพิกัดตำแหน่งที่เครื่องรับสัญญาณ GPS คำนวณได้ โดยค่าพิกัดตำแหน่งที่คำนวณ ได้มาจากการหาระยะจากดาวเทียมหลายดวง ประกอบกับลักษณะการเรียงตัวของดาวเทียมรูปเรขาคณิตหรือขนาดของมุมระหว่างดาวเทียมแต่ละดวงภายในกลุ่ม ปัจจัยเหล่านี้มีส่วนทำให้ความคลาดเคลื่อนของค่าพิกัดตำแหน่งเพิ่มขึ้นหรือลดลงได้ เปรียบเทียบเหมือนกับ การเล่นสนุกเกอร์ที่ต้องเลือกลูกที่มีมุมแทงลูกให้ลงหลุมได้ง่าย บางลูกอยู่ในมุมที่ดีแทงได้เต็มลูก ในขณะที่บางลูกต้องแทงบางมากจึงอาจเกิดการผิดพลาดได้ ดังนั้นในเครื่องรับสัญญาณ GPS จึงมีโปรแกรมวิเคราะห์ตำแหน่งของดาวเทียมที่อยู่บนท้องฟ้า เครื่องรับประเภทละเอียดจะเลือกคำนวณค่าพิกัดตำแหน่งโดยการรับสัญญาณจากชุดดาวเทียม 4 ดวง ที่มีค่า GdoP ดีที่สุด วิธีนี้จะทำให้ค่าความคลาดเคลื่อนจาก GdoP เหลือน้อยที่สุด

2.2.2 ระบบแผนที่

แผนที่ที่ใช้อยู่ในปัจจุบันแบ่งได้เป็น 2 ชนิดใหญ่ ๆ คือ แผนที่เฉพาะเรื่อง (Thematic Map) และแผนที่ภูมิประเทศ (Topographic Map) โดยที่แผนที่เฉพาะเรื่องนี้เป็นแผนที่ที่มีองค์ประกอบอื่น ๆ เข้ามามาก ส่วนแผนที่ภูมิประเทศจะเป็นแผนที่ที่เน้นแสดงสภาพทางภูมิศาสตร์โดยเฉพาะ

แผนที่เฉพาะเรื่อง คือแผนที่ที่แสดงรายละเอียดของข้อมูลเชิงพื้นที่ที่ต้องการนำเสนอโดยการแปลงข้อมูลเหล่านั้นให้เป็นเครื่องหมายแผนที่เสียก่อน แล้วนำไปพิมพ์ซ้อนทับลงบนแผนที่ฐานตามตำแหน่งที่ตั้งของข้อมูลนั้น ๆ ซึ่งประกอบไปด้วย ข้อมูลเชิงพื้นที่ (Spatial Data) และแผนที่ฐาน (Base Map) ในการทำแผนที่นี้เตรียมการเสร็จแล้วจะทำการพิมพ์ลงบนกระดาษ (Paper Map) สำหรับปัญหาแผนที่บนกระดาษ คือ ถ้ามีการเพิ่มเติมหรือแก้ไขจะไม่สามารถแก้ไขในเวลาสั้น ๆ ได้ จะต้องทำการพิมพ์แผนที่ออกมาใหม่ทั้งหมด ทำให้เสียเวลาและค่าใช้จ่ายมาก ปัจจุบันได้ทำการดัดแปลงแผนที่เฉพาะเรื่อง มาจัดเก็บไว้ในคอมพิวเตอร์โดยนำข้อมูลไปเก็บไว้ในฐานข้อมูลคอมพิวเตอร์ มีการแสดงผลโดยวางซ้อนทับฐานข้อมูล การนำคอมพิวเตอร์เข้ามาใช้ในการเก็บข้อมูลนี้จะทำได้ดีกว่าแผนที่กระดาษ เพราะว่าสามารถเลือกดูชั้นข้อมูลที่จำเป็นเท่านั้น ทำให้เข้าใจง่ายกว่าแผนที่กระดาษ

2.2.2.1 แผนที่ดิจิตอล

แผนที่ดิจิตอล (Digital Map) หรือแผนที่เชิงตัวเลขที่แผนที่ที่ใช้คอมพิวเตอร์ในการประมวลผลและมีการจัดเก็บข้อมูลของแผนที่ให้อยู่ในรูปของข้อมูลคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์จะทำการจัดเก็บในรูปแบบของฐานข้อมูลคอมพิวเตอร์ แผนที่ดิจิตอลแบ่งตามการจัดเก็บออกเป็น 2 แบบ คือแบบราสเตอร์และแบบเวกเตอร์

แผนที่แบบราสเตอร์ หมายถึงแผนที่ที่มีการจัดเก็บและแสดงผลในรูปของจุดภาพ การสร้างแผนที่แบบนี้จะทำได้โดยรับภาพแผนที่จากแผนที่กระดาษผ่านทางเครื่องสแกนภาพซึ่งวิธีการสแกนภาพเป็นการนำรูปภาพทั้งรูปเข้าไปไว้ในลักษณะของรูปภาพ ซึ่งการแก้ไขจะทำได้ยาก รวมทั้งใช้เนื้อที่ในการจัดเก็บมาก

แผนที่แบบเวกเตอร์ หมายถึงแผนที่ที่มีการจัดเก็บและแสดงผลในรูปของลายเส้น และมีทิศทางการสร้างแผนที่แบบนี้ทำได้โดยใช้วิธีการลอกแบบจากเครื่องดิจิตอลไตเซอร์ ซึ่งจะเก็บเฉพาะข้อมูลในส่วนที่ต้องการลอกแบบ ดังนั้นข้อมูลแบบนี้จึงใช้เนื้อที่ในการจัดเก็บน้อยกว่าสามารถแก้ไขได้ในภายหลังโดยที่มาตราส่วนไม่ผิดไปจากเดิม

2.2.2.2 ระบบพิกัดบนแผนที่

ระบบพิกัดบนแผนที่จะมีการอ้างอิงพิกัดที่เหมือนกับระบบพิกัดฉากในทางเลขาคณิตที่ประกอบไปด้วยแกน X และแกน Y โดยจุดกำเนิดหมายถึงจุดตัดระหว่างแกน X และแกน Y เมื่อแทนด้วยระบบพิกัดบนที่แผนที่แล้ว แกน X จะหมายถึงเส้น Latitude และแกน Y จะหมายถึงเส้น Longitude เมื่อพิจารณาระบบพิกัดบนโลกแล้วเราจะพิจารณาเป็นลักษณะของ 3 มิติ คือ X, Y, Z โดย Z จะหมายถึงค่าความสูง ระบบนี้จะใช้ในการอ้างอิงในระบบระบุตำแหน่ง GPS

Latitude เป็นเส้นที่ลากวนรอบโลกในแนวนอน โดยพิกัด Latitude ก็คือระยะทางเชิงมุมที่วัดไปทางเหนือและใต้ของเส้นศูนย์สูตร นับจาก 0 องศาไปทางเหนือและทางใต้ 90 องศา โดยเส้นศูนย์สูตรก็คือเส้น Latitude ที่วนรอบจุดศูนย์กลางของโลก

Longitude เป็นเส้นแนวตั้งที่ลากระหว่างขั้วโลกเหนือกับขั้วโลกใต้ ทุกเส้นของ Longitude จะต้องตัดกับเส้นศูนย์สูตร โดยเส้น Longitude ที่ศูนย์อยู่ที่กรีนิช (Greenwich) ประเทศอังกฤษ โดยพิกัด Longitude คือ ระยะทางเชิงมุมที่วัดจากเส้น Longitude ที่ศูนย์ ไปทางตะวันออก 180 องศาตะวันออก และทางตะวันตก 180 องศาตะวันตก

2.2.2.3 ระบบกูเกิลแผนที่ (Google Map)

กูเกิลแผนที่ คือบริการแผนที่โดยสามารถดูในเว็บเบราว์เซอร์ซึ่งขึ้นอยู่กับตำแหน่งที่ต้องการ สามารถดูแผนที่พื้นฐานหรือแผนที่ที่กำหนดเองและข้อมูลธุรกิจท้องถิ่น รวมถึงตำแหน่งของธุรกิจข้อมูลที่อยู่ติดต่อ และเส้นทางการขับขี่ด้วย คลิกและลากแผนที่เพื่อดูส่วนที่ติดกันได้ทันที ดูภาพจากดาวเทียมของตำแหน่งที่ต้องการ สามารถขยายและกวาดดูได้

ผู้ใช้ทุกคนที่มีการเชื่อมต่ออินเตอร์เน็ต และเว็บเบราว์เซอร์ที่สนับสนุน จะสามารถใช้บริการฟรีนี้ในคอมพิวเตอร์และจะสามารถเพิ่มความสามารถของการใช้งานหากสมัครเป็นสมาชิกของเว็บไซต์ ซึ่งสามารถดูกูเกิลแผนที่ได้หลายวิธีดังนี้

- ไปที่ maps.google.co.th
- ดูหน้าเว็บที่มีกูเกิลแผนที่ฝังอยู่
- ดูกูเกิลแผนที่บนโทรศัพท์มือถือ
- ดูแผนที่ส่วนบุคคลที่สร้างโดย ผลิตภัณฑ์ Google Earth Enterprise

2.2.3 เทคโนโลยีสมาร์ทการ์ดโทเคน (Smartcard USB Token)

eToken เป็นเทคโนโลยีสมาร์ทการ์ดที่สนับสนุนการยืนยันตัวตนแบบ 2 ระดับ โดยได้รับการรับรองมาตรฐานความปลอดภัยระดับสากล ทั้งในแบบการรักษาความปลอดภัย และการรักษาความเป็นส่วนบุคคล ซึ่ง สามารถจัดเก็บใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) เพื่อนำไปใช้ในการตรวจสอบหรือพิสูจน์ตัวตนของผู้ใช้งาน เช่น การยืนยันเข้าสู่คอมพิวเตอร์ผ่านระบบเครือข่าย (Network Logon) การลงลายมือชื่ออิเล็กทรอนิกส์ (Digital Signing) การเข้ารหัสถอดรหัสอีเมล์ (E-Mail Encryption) การยืนยันตัวตนเข้าสู่เว็บไซต์ (Secure web logon) และการยืนยันตัวตนเข้าสู่ระบบเครือข่ายเสมือน (Virtual Private Network) เป็นต้น

รูปที่ 2.8 แสดงภาพอุปกรณ์ eToken Pro 72K

อุปกรณ์ eToken ไม่สามารถทำซ้ำหรือเรียนแบบได้ มีลักษณะภายนอกคล้ายกับอุปกรณ์จัดเก็บข้อมูล (Flash Drive) ซึ่งต่างจากอุปกรณ์ eToken ที่ไม่สามารถจัดเก็บข้อมูล แต่สามารถเก็บใบรับรองอิเล็กทรอนิกส์ได้ โดยใช้หลักการพิสูจน์ตัวตนคล้ายกับระบบธนาคารในการตรวจสอบผู้ใช้งานบัตร ATM ซึ่งปัจจุบันองค์กรทั้งภาครัฐและภาคเอกชนมีการนำอุปกรณ์ eToken เข้ามาใช้ในการพิสูจน์ตัวตน เพื่อเข้าใช้งานระบบต่าง ๆ

2.2.4 แอนดรอยด์ (ระบบปฏิบัติการ)

แอนดรอยด์ (อังกฤษ: Android) เป็นระบบปฏิบัติการที่มีพื้นฐานอยู่บนลินุกซ์ ถูกออกแบบมาสำหรับอุปกรณ์ที่ใช้จอสัมผัส เช่นสมาร์ตโฟน และแท็บเล็ตคอมพิวเตอร์ ถูกคิดค้นและพัฒนาโดยบริษัท แอนดรอยด์ (Android, Inc.) ซึ่งต่อมา กูเกิล ได้ทำการซื้อต่อบริษัทในปี พ.ศ. 2548 แอนดรอยด์ถูกเปิดตัวเมื่อ ปี พ.ศ. 2550 พร้อมกับการก่อตั้งโอเพนแฮนด์เซตอัลไลแอนซ์ ซึ่งเป็นกลุ่มของบริษัทผลิตฮาร์ดแวร์, ซอฟต์แวร์ และการสื่อสารคมนาคม ที่ร่วมมือกันสร้างมาตรฐานเปิดสำหรับอุปกรณ์พกพา โดยสมาร์ตโฟนที่ใช้ระบบปฏิบัติการแอนดรอยด์เครื่องแรกของโลกคือ เอชทีซี ดรีม วางจำหน่ายเมื่อปี พ.ศ. 2551

แอนดรอยด์เป็นระบบปฏิบัติการโอเพนซอร์ซ และกูเกิลได้เผยแพร่ภายใต้ลิขสิทธิ์อาปาเช ซึ่งโอเพนซอร์ซจะอนุญาตให้ผู้ผลิตปรับแต่งและวางจำหน่ายได้ รวมไปถึงนักพัฒนาและผู้ให้บริการเครือข่ายด้วย อีกทั้งแอนดรอยด์ยังเป็นระบบปฏิบัติการที่รวมนักพัฒนาที่เขียนโปรแกรมประยุกต์ มากมาย ภายใต้ภาษาจาวา ในเดือนตุลาคม พ.ศ. 2555 มีโปรแกรมมากกว่า 700,000 โปรแกรมสำหรับแอนดรอยด์ และยอดดาวน์โหลดจากกูเกิล เพลย์ มากถึง 2.5 หมื่นล้านครั้ง จากการสำรวจในช่วงเดือน เมษายน ถึง พฤษภาคม ในปี พ.ศ. 2556 พบว่าแอนดรอยด์เป็นระบบปฏิบัติการที่นักพัฒนาเลือกที่จะพัฒนาโปรแกรมมากที่สุด ถึง 71%

รูปที่ 2.9 แสดงภาพสัญลักษณ์ของ Android

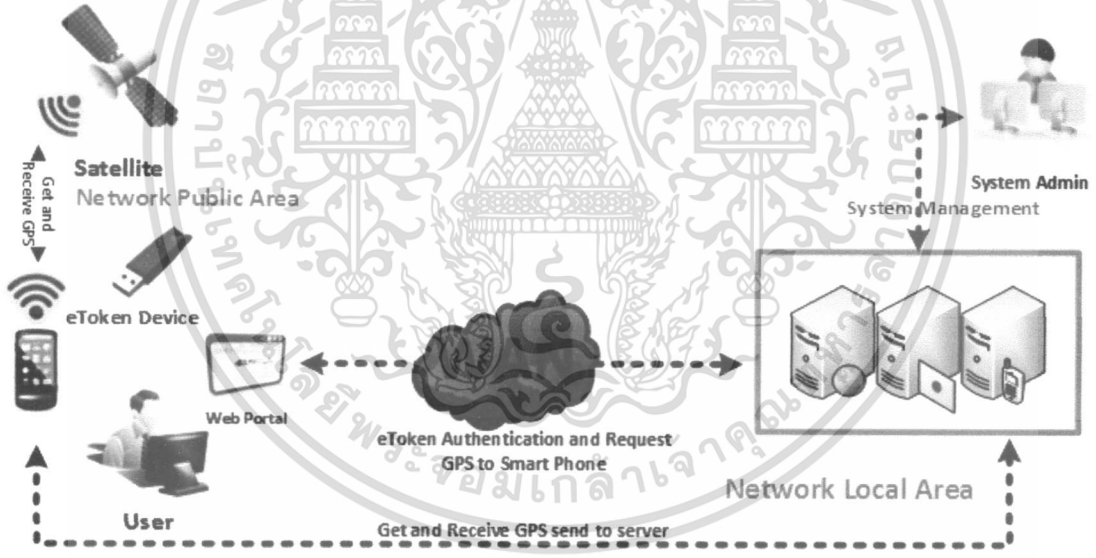
ปัจจัยเหล่านี้ทำให้แอนดรอยด์เป็นระบบปฏิบัติการที่ใช้กันอย่างแพร่หลายในปัจจุบัน นำหน้าซิมเบียน ในไตรมาสที่ 4 ของปี พ.ศ. 2553 และยังเป็นทางเลือกของผู้ผลิตที่จะใช้ซอฟต์แวร์ที่มีราคาต่ำ, ตอบสนองความต้องการของผู้ใช้ได้ดี สำหรับอุปกรณ์ในสมัยใหม่[13] แม้ว่าแอนดรอยด์จะดูเหมือนได้รับการพัฒนาเพื่อใช้กับสมาร์ตโฟนและแท็บเล็ต แต่มันยังสามารถใช้ได้กับโทรทัศน์, เครื่องเล่นวิดีโอเกม, กล้องดิจิทัล และอุปกรณ์อิเล็กทรอนิกส์อื่นๆ แอนดรอยด์เป็นระบบเปิด ทำให้นักพัฒนาสามารถพัฒนาคุณสมบัติใหม่ๆ ได้ตลอดเวลา

บทที่ 3
การวิเคราะห์และออกแบบระบบ

การวิเคราะห์ระบบปัจจุบันจะเป็นการศึกษาการทำงานและขั้นตอนการทำงานของระบบที่มีอยู่เดิมและวิเคราะห์ปัญหา ข้อจำกัดของระบบงานเดิมที่มีอยู่ในแต่ละแบบ เพื่อประเมินกับความต้องการของผู้ใช้ระบบ ซึ่งนำมาประกอบการวิเคราะห์และออกแบบระบบงานใหม่ให้บรรลุวัตถุประสงค์ตรงตามความต้องการของผู้ใช้งานมากที่สุด

3.1 องค์ประกอบหลักของระบบ

ระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS เป็นการทำงานร่วมกัน 2 ส่วน คือ ส่วนเซิฟเวอร์ (Server) และไคลเอนต์ (Client) ดังรูปที่ 3.1



รูปที่ 3.1 แสดงการทำงานของระบบโดยรวม

3.1.1 ส่วนรับข้อมูล

เป็นส่วนที่ใช้ติดต่อระหว่าง Server และ Client โดยจะทำหน้าที่ในการรับส่งข้อมูลจาก Client และทำการจัดเก็บลงฐานข้อมูลรวมถึงการจัดการกับข้อมูลเพื่อที่จะนำไปใช้ประมวลผลและแสดงตำแหน่งปัจจุบันของอุปกรณ์ eToken โดยการตรวจสอบจากตำแหน่งสถานะของ Smartphone ที่อยู่ ณ ปัจจุบัน ซึ่งจะแบ่งออกเป็น 4 ส่วน คือ

3.1.1.1 ส่วนตรวจสอบข้อมูล

การทำงานในส่วนนี้จะเป็นการตรวจสอบข้อมูลที่ได้รับมาจาก Client (Smartphone) ว่ามีความถูกต้องครบถ้วนหรือไม่ เพื่อไม่ให้เกิดปัญหาข้อมูลตำแหน่งหรือพิกัดผิดพลาดอันเนื่องมาจากการรับส่งข้อมูลจาก Client

3.1.1.2 ส่วนจัดเก็บข้อมูล

หลังจากที่ได้มีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับจาก Client แล้ว ระบบจะทำการจัดเก็บข้อมูลลงฐานข้อมูลเพื่อนำไปใช้ในการวิเคราะห์หรือประมวลอีกครั้ง

3.1.2 ส่วนประมวลผล

การทำงานในส่วนนี้เป็นการนำค่าพิกัดที่ได้ มาคำนวณหาจุดที่ Smartphone อยู่ ณ ปัจจุบัน เพื่อนำไปเปรียบเทียบค่าพิกัดที่เก็บอยู่ในฐานข้อมูลหลังจากมีการเปรียบเทียบแล้ว ระบบจะทำการตรวจสอบตามเงื่อนไขที่ได้กำหนด ว่าสามารถใช้งานอุปกรณ์ eToken ในพิกัดนั้นได้หรือไม่

3.1.3 ส่วนแสดงผล

การทำงานในส่วนนี้เป็นการแสดงข้อมูลที่ถูกจัดเก็บไว้ในฐานข้อมูลออกมาในรูปแบบของกราฟหรือตาราง ซึ่งผู้ดูแลระบบสามารถปรับปรุงแก้ไขข้อมูลของระบบได้

3.1.4 ระบบจีพีเอส

ในส่วนนี้จะเป็นองค์ประกอบหลักสำคัญคือ Smartphone จะได้รับสัญญาณ GPS สามารถบอกพิกัดหรือตำแหน่งปัจจุบันได้ โดยผู้ใช้ต้องทำการส่งค่าพิกัดจาก Smartphone ไปยัง Server ในกรณีที่ผู้ใช้ต้องการยืนยันตัวตนในตำแหน่งปัจจุบัน ซึ่งการร้องขอพิกัดนั้น ขึ้นอยู่กับความต้องการของผู้ใช้ ที่ต้องการใช้งานจึงจะมีการร้องขอ ทำให้ Service บน Smartphone ไม่ต้องทำงานอยู่ตลอดเวลา ข้อดี คือ ประหยัดพลังงาน

3.2 การทำงานของระบบ

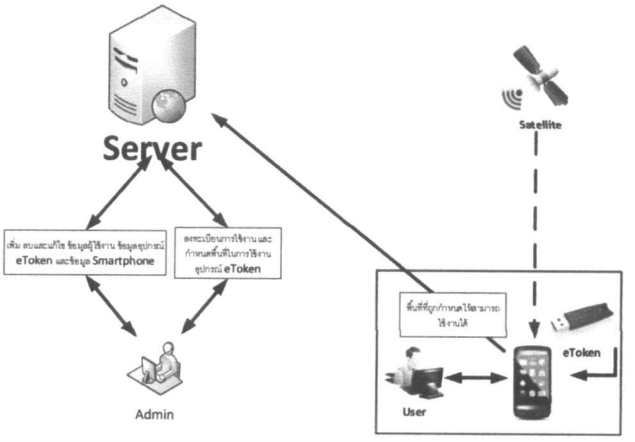
หลักการทำงานของระบบการตรวจสอบการใช้งานอุปกรณ์ eToken ได้มีการแบ่งระดับการใช้งานระบบออกเป็น 2 ส่วน คือ

1. ระดับผู้ใช้งานอุปกรณ์ eToken (User)

ผู้ใช้งานมีหน้าที่ใช้งานอุปกรณ์ eToken ผ่านระบบที่องค์กรได้พัฒนาขึ้นมาและสามารถใช้งานอุปกรณ์ eToken ได้ตามพื้นที่ที่ถูกกำหนดเท่านั้น

2. ระดับผู้ดูแลระบบ (Administrator)

ผู้ดูแลระบบมีสิทธิ์ลงทะเบียนการใช้งานอุปกรณ์ eToken การเพิ่ม ลบ แก้ไข ข้อมูลของผู้ใช้งาน และข้อมูล Device ID ของ Smartphone รวมถึงการตรวจสอบรายงาน พร้อมทั้งการกำหนดพื้นที่ในการใช้งานอุปกรณ์ eToken อีกด้วย



รูปที่ 3.2 แสดงภาพการทำงานของระบบ

3.3 โครงสร้างของระบบ

โครงสร้างด้านอุปกรณ์ (Hardware) ประกอบด้วยอุปกรณ์ต่าง ๆ ดังนี้

3.3.1 อุปกรณ์ eToken Pro (SafeNet Product)

USB Token คือ อุปกรณ์สำหรับใช้ในการแสดงตน (Authentication) เพื่อเข้าใช้งานระบบคอมพิวเตอร์ หรือใช้เก็บข้อมูลความลับเช่น รหัสผ่าน มีรูปร่างหน้าตาคล้าย กับ Flash Drive หรือ USB Drive แต่ภายในจะเป็นชิปแบบเดียวกับชิปที่ใช้กับบัตรสมาร์ทการ์ดซึ่งช่วยในการป้องกันข้อมูลความลับที่เก็บไว้ วัตถุประสงค์ของการพัฒนา USB Token ขึ้นมาก็เพื่อให้มี อุปกรณ์ที่เป็นเครื่องมือช่วยเก็บข้อมูลความลับ เช่น ใบรับรองอิเล็กทรอนิกส์ และข้อมูลของผู้ใช้ เป็นต้น

รูปที่ 3.3 แสดงภาพอุปกรณ์ eToken Pro (SafeNet Product)

3.3.2 Smartphone

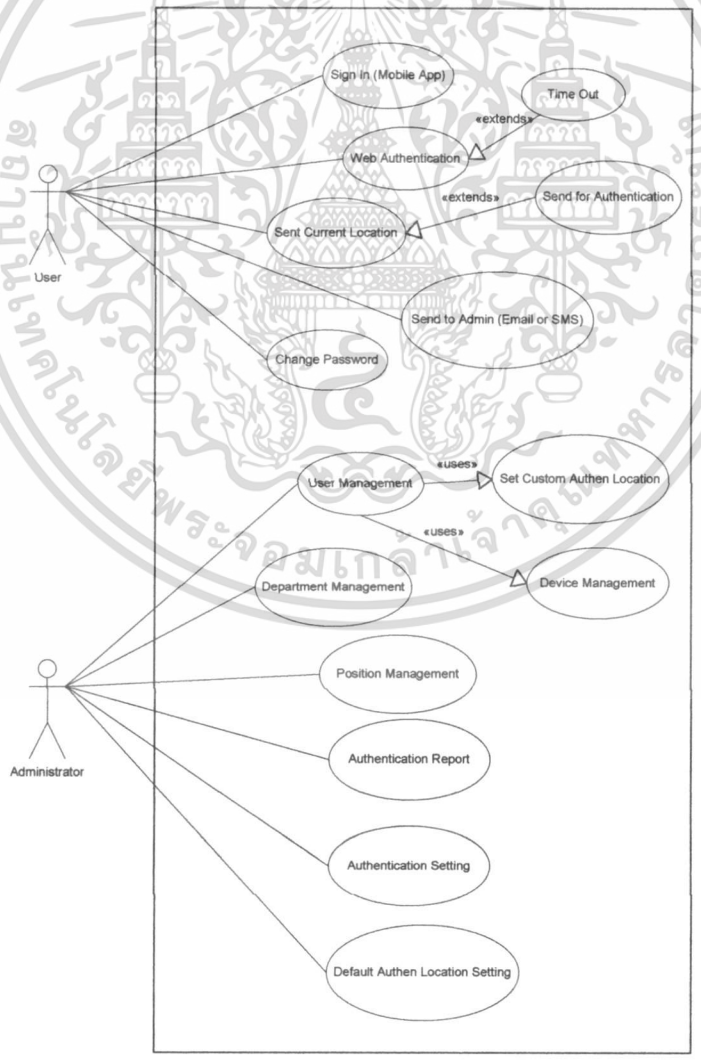
สมาร์ทโฟน (อังกฤษ: smartphone, smartphone) เป็นโทรศัพท์เคลื่อนที่ที่มีความสามารถที่เพิ่มเติมนอกเหนือจากโทรศัพท์มือถือทั่วไป สมาร์ตโฟนได้ถูกมองว่าเป็นคอมพิวเตอร์พกพาที่ทำงานในลักษณะของโทรศัพท์เคลื่อนที่ โดยที่สามารถเชื่อมต่อความสามารถหลักของโทรศัพท์มือถือ เข้าร่วมกับแอปพลิเคชันของโทรศัพท์เอง[5]สมาร์ตโฟนสามารถให้ผู้ใช้งานติดตั้งโปรแกรมเสริมสำหรับเพิ่มความสามารถของโทรศัพท์ตัวเอง โดยรูปแบบนั้นขึ้นอยู่กับแพลตฟอร์มของโทรศัพท์และระบบปฏิบัติการ

รูปที่ 3.4 แสดงภาพ Smartphone

3.4 การออกแบบ

3.4.1 ยูสเคสไดอะแกรม (Use case diagram)

ยูสเคสไดอะแกรมการทำงานของระบบทั้งหมด โดยจะมีผู้เกี่ยวข้องกับระบบได้แก่ ผู้ดูแลระบบ มีหน้าที่ในการเพิ่ม ลบ แก้ไขข้อมูลต่างๆ ซึ่งจะทำงานตามฟังก์ชันการงานหลัก ๆ ที่แสดงในยูสเคสไดอะแกรม และผู้ใช้ มีหน้าที่ส่งพิกัดหรือตำแหน่งมาเก็บในฐานข้อมูล เพื่อใช้ในการวิเคราะห์และประมวลผล โดยระบบจะทำงานได้นั้น จะต้องมีการเชื่อมต่อไปยังฐานข้อมูล เพื่อเก็บข้อมูลการทำรายการทั้งหมดไว้ในฐานข้อมูล ดังรูปภาพที่ 3.5



รูปที่ 3.5 แสดงภาพยูสเคสไดอะแกรมการทำงานของระบบ

คำอธิบายยูสเคสไดอะแกรม (Use Case Description)

จากยูสเคสไดอะแกรม มีคำอธิบายรายละเอียดของแต่ละยูสเคส ดังตารางที่ 3.1 ถึง 3.11

ตารางที่ 3.1 คำอธิบายยูสเคส Sign In (Mobile App)

Use Case Name :	Sign In (Mobile App)	
Triggering Event :	ต้องการยืนยันตัวตนเพื่อเข้าสู่ระบบบนสมาร์ทโฟน	
Brief Description :	ยูสเคสในการยืนยันตัวตันเข้าสู่ระบบบนสมาร์ทโฟน	
Actors :	User	
Pre-Conditions	มีชื่อผู้ใช้อยู่ในระบบ	
Post-Conditions	เข้าสู่ระบบเรียบร้อย	
Normal Flows :	**Actor Actions**	**System Response**
	1. ผู้ใช้งานเปิดแอพพลิเคชั่น 3. ใส่ชื่อและรหัสผ่านผู้ใช้	2. แสดงหน้าจอให้ใส่ชื่อและรหัสผ่านผู้ใช้ 4. เมื่อระบบตรวจสอบข้อมูลถูกต้องก็จะเข้าสู่หน้าแรกของแอพพลิเคชั่นบนสมาร์ทโฟน
Exception Conditions :	4a. หากชื่อผู้ใช้หรือรหัสผ่านไม่ถูกต้อง : กลับไปขั้นตอนที่ 2	

ตารางที่ 3.2 คำอธิบายยูสเคส Web Authentication

Use Case Name :	Web Authentication	
Triggering Event :	ต้องการยืนยันตัวตนเพื่อเข้าสู่ระบบผ่านเว็บ	
Brief Description :	ยูสเคสในการยืนยันตัวตันผู้ใช้งานเข้าสู่ระบบผ่านเว็บ	
Actors :	User	
Pre-Conditions	มีชื่อผู้ใช้อยู่ในระบบและมีอุปกรณ์ eToken	
Post-Conditions	เข้าสู่ระบบเรียบร้อย	
Normal Flows :	**Actor Actions**	**System Response**
	1. ผู้ใช้เสียบอุปกรณ์ eToken ที่เครื่องคอมพิวเตอร์ และเปิดหน้าเว็บเพื่อยืนยันตัวตน	2. ระบบจะตรวจสอบข้อมูลการยืนยันตัวตนกับฐานข้อมูลและรอการส่งพิกัดจากสมาร์ทโฟน
Exception Conditions :	2a. ถ้าผู้ใช้ไม่ส่งพิกัดในเวลาที่กำหนด ก็จะทำให้ไม่สามารถเข้าใช้งานเว็บได้เนื่องจากหมดเวลาเชื่อมต่อ : กลับไปที่ขั้นตอนที่ 1	

ตารางที่ 3.3 คำอธิบายยูสเคส Send Current Location

Use Case Name :	Send Current Location	
Triggering Event :	ต้องการส่งละติจูด ลองจิจูด เพื่อแจ้งพิกัดตำแหน่งของผู้ใช้งาน	
Brief Description :	ยูสเคสในการส่งละติจูด ลองจิจูด เพื่อแจ้งพิกัดตำแหน่งของผู้ใช้งาน	
Actors :	User	
Pre-Conditions	มีข้อมูลลงทะเบียนใช้งานอยู่แล้ว	
Post-Conditions	ส่งละติจูด ลองจิจูด เข้าระบบ	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Send Current Location	
		2. ระบบรอรับการยืนยันตัวตนผ่านเว็บ
	3. ผู้ใช้ยืนยันตัวตนผ่านเว็บ	
		4. ระบบตรวจสอบและอนุญาตให้เข้าใช้งานแอพพลิเคชั่น ถ้าเงื่อนเป็นไปตามที่กำหนด
Exception Conditions :	3a. หากผู้ใช้ไม่ทำการยืนยันตัวตนผ่านเว็บ : กลับไปขั้นตอนที่ 2	

ตารางที่ 3.4 คำอธิบายยูสเคส Send to Admin (Email or SMS)

Use Case Name :	Send to Admin (Email or SMS)	
Triggering Event :	ต้องการส่งอีเมลหรือข้อความให้ผู้ดูแลระบบ	
Brief Description :	ยูสเคสส่งอีเมลหรือข้อความให้ผู้ดูแลระบบ	
Actors :	User	
Pre-Conditions	เมื่อเข้าสู่ระบบแอพพลิเคชั่นบนสมาร์ทโฟน	
Post-Conditions	ส่งอีเมลหรือข้อความให้กับผู้ดูแลระบบได้	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Sent Email or SMS 3. กรอกข้อมูลรายละเอียดที่ต้องการส่งถึงผู้ดูแลระบบ	2. แสดงหน้าจอให้ใส่รายละเอียดของอีเมลหรือข้อความที่ต้องการส่งถึงผู้ดูแลระบบ 4. ระบบส่งอีเมลหรือข้อความถึงผู้ดูแลระบบ
Exception Conditions :		

ตารางที่ 3.5 คำอธิบายยูสเคส Change Password

Use Case Name :	Change Password	
Triggering Event :	ต้องการเปลี่ยนรหัสผ่านผู้ใช้	
Brief Description :	ยูสเคสในการเปลี่ยนรหัสผ่านผู้ใช้	
Actors :	User	
Pre-Conditions	มีข้อมูลลงทะเบียนใช้งานอยู่แล้ว	
Post-Conditions	เปลี่ยนรหัสผ่านเรียบร้อยแล้ว	
Normal Flows :	**Actor Actions**	**System Response**
	1. ผู้ใช้เปิดแอพพลิเคชันบนสมาร์ทโฟน	
		2. แสดงหน้าจอให้รหัสผ่านผู้ใช้
	3. ใส่รหัสผ่านผู้ใช้	
		4. ระบบตรวจสอบและอนุญาตให้เข้าใช้งานแอพพลิเคชั่น
	5. ผู้ใช้เลือกเมนู Change Password	
		6. ระบบแสดงหน้าจอให้ใส่รหัสผ่านเดิม รหัสผ่านใหม่และยืนยันรหัสผ่านใหม่
	7. ผู้ใช้ใส่รหัสผ่านเดิม รหัสผ่านใหม่และยืนยันรหัสผ่านใหม่ คลิกปุ่ม Submit	
		7. ระบบตรวจสอบข้อมูลรหัสผ่านเดิม เมื่อถูกต้องจะทำการเปลี่ยนรหัสผ่านใหม่และบันทึกลงฐานข้อมูล
Exception Conditions :		

ตารางที่ 3.6 คำอธิบายยูสเคส User Management

Use Case Name :	User Management	
Triggering Event :	ต้องการจัดการข้อมูลของผู้ใช้งาน	
Brief Description :	ยูสเคสในการสร้างข้อมูลผู้ใช้งาน	
Actors :	Administrator	
Pre-Conditions	-	
Post-Conditions	ข้อมูลผู้ใช้ถูกเพิ่ม ลบ แก้ไข และบันทึกลงในฐานข้อมูล	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู User Management	
		2. แสดงหน้าจอจัดการข้อมูลผู้ใช้
	3. เลือกเมนูที่ต้องการจัดการข้อมูลผู้ใช้	
		4. แสดงรายการที่เลือก
	5. คลิกเลือกรายการจัดการผู้ใช้ที่ต้องการ และทำการเพิ่ม ลบ หรือแก้ไข คลิกปุ่ม Submit	
		6. ระบบทำการเพิ่ม แก้ไขหรือลบข้อมูลผู้ใช้และบันทึกลงฐานข้อมูล
Exception Conditions :		

ตารางที่ 3.7 คำอธิบายยูสเคส Department Management

Use Case Name :	Department Management	
Triggering Event :	ต้องการจัดการข้อมูลแผนก	
Brief Description :	ยูสเคสในการจัดการข้อมูลแผนก	
Actors :	Administrator	
Pre-Conditions	-	
Post-Conditions	ข้อมูลแผนกถูกจัดการและบันทึกลงในฐานข้อมูล	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Department Management 3. เลือกเมนูที่ต้องการจัดการข้อมูลแผนก 5. คลิกเลือกรายการจัดการแผนกที่ต้องการ และทำการเพิ่ม ลบ หรือแก้ไข คลิกปุ่ม Submit	2. แสดงหน้าจอจัดการข้อมูลผู้ใช้ 4. แสดงรายการที่เลือก 6. ระบบทำการเพิ่ม แก้ไขหรือลบข้อมูลแผนกและบันทึกลงฐานข้อมูล
Exception Conditions :		

ตารางที่ 3.8 คำอธิบายยูสเคส Position Management

Use Case Name :	Position Management	
Triggering Event :	ต้องการจัดการข้อมูลตำแหน่ง	
Brief Description :	ยูสเคสในการจัดการข้อมูลตำแหน่ง	
Actors :	Administrator	
Pre-Conditions	-	
Post-Conditions	ข้อมูลตำแหน่งถูกจัดการและบันทึกลงในฐานข้อมูล	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Position Management	
		2. แสดงหน้าจอจัดการข้อมูลผู้ใช้
	3. เลือกเมนูที่ต้องการจัดการข้อมูลตำแหน่ง	
		4. แสดงรายการที่เลือก
	5. คลิกเลือกรายการจัดการตำแหน่งที่ต้องการ และทำการเพิ่ม ลบ หรือแก้ไข คลิกปุ่ม Submit	
		6. ระบบทำการเพิ่ม แก้ไขหรือลบข้อมูลตำแหน่งและบันทึกลงฐานข้อมูล
Exception Conditions :		

ตารางที่ 3.9 คำอธิบายยูสเคส Authentication Report

Use Case Name :	Authentication Report	
Triggering Event :	ต้องการดูรายงานการเข้าใช้งานของผู้ใช้	
Brief Description :	ยูสเคสในการดูรายงานการเข้าใช้งานของผู้ใช้	
Actors :	Administrator	
Pre-Conditions	มีประวัติการเข้าใช้งานของผู้ใช้แล้ว	
Post-Conditions	แสดงรายงานการเข้าใช้งานของผู้ใช้	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Report	2. แสดงหน้าจอรายงานการเข้าใช้งานของผู้ใช้
Exception Conditions :		

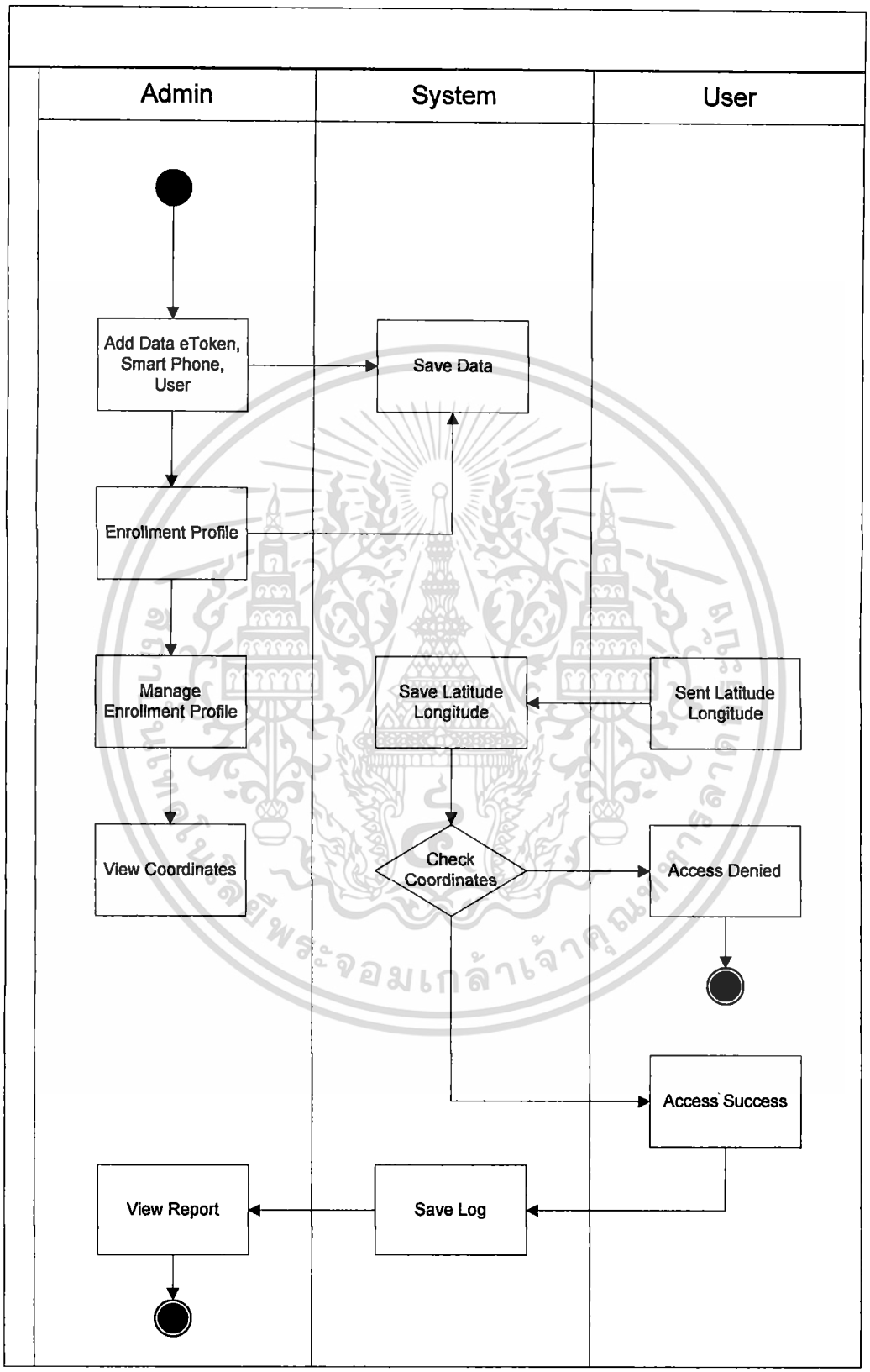
ตารางที่ 3.10 คำอธิบายยูสเคส Authentication Setting

Use Case Name :	Authentication Setting	
Triggering Event :	ต้องการตั้งค่าการใช้งานระบบ	
Brief Description :	ยูสเคสในการตั้งค่าการใช้งานระบบ	
Actors :	Administrator	
Pre-Conditions	-	
Post-Conditions	ตั้งค่าการใช้งานระบบเรียบร้อย	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Authentication Setting 3. ตั้งค่าต่าง ๆ ตามความต้องการ	2. แสดงหน้าจอการตั้งค่าต่าง ๆ ของระบบ 4. ระบบทำการบันทึกข้อมูลลงฐานข้อมูล
Exception Conditions :		

ตารางที่ 3.11 คำอธิบายยูสเคส Default Authen Location Setting

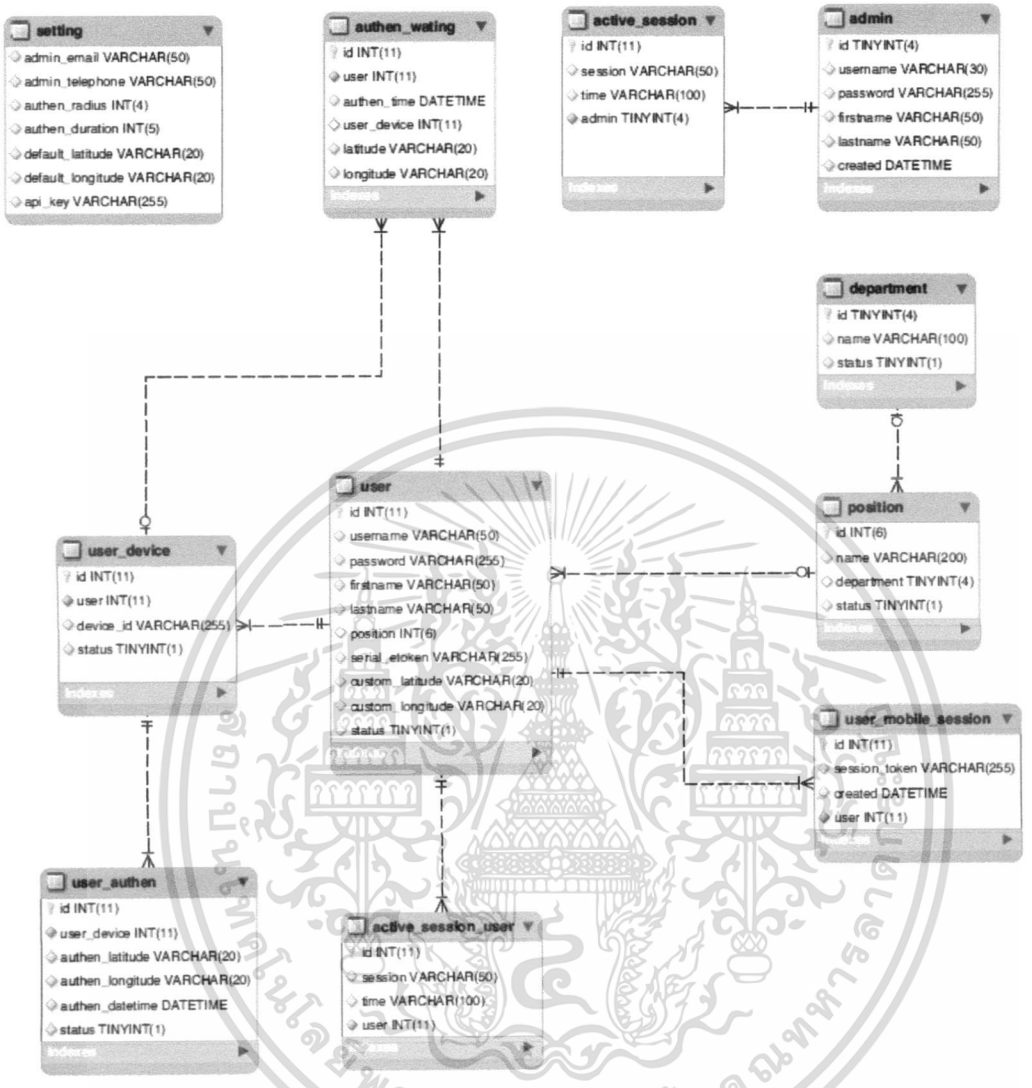
Use Case Name :	Default Authen Location Setting	
Triggering Event :	ต้องการตั้งค่าพิกัดมาตรฐาน	
Brief Description :	ยูสเคสในการตั้งค่าพิกัดมาตรฐาน	
Actors :	Administrator	
Pre-Conditions	-	
Post-Conditions	ตั้งค่าพิกัดมาตรฐานเรียบร้อยแล้ว	
Normal Flows :	**Actor Actions**	**System Response**
	1. เลือกเมนู Default Authen Location Setting	
		2. แสดงหน้าแผนที่และการตั้งค่าพิกัด
	3. กำหนดพิกัดในแผนที่หรือกำหนดโดยการใส่ละติจูด ลองจิจูด เข้าไปในระบบ	
		4. ระบบทำการบันทึกพิกัดลงฐานข้อมูล
Exception Conditions :		

3.5 ขั้นตอนการทำงานของระบบ (Activity Diagram)



รูปที่ 3.6 แสดงแผนภาพขั้นตอนการทำงานของระบบ

3.6 แผนภาพความสัมพันธ์ของข้อมูล (ER-Diagram)



รูปที่ 3.7 แสดงความสัมพันธ์ของข้อมูลในแต่ละตาราง ER-Diagram

จากภาพที่ 3.7 แสดงความสัมพันธ์ของข้อมูลแต่ละตาราง โดยมีแฟ้มข้อมูลทั้งหมด 6 แฟ้ม

- Setting เป็นตารางสำหรับการกำหนดค่าการใช้งานต่าง ๆ
- Authen_Waiting สำหรับเก็บข้อมูลการเข้าใช้ระบบผ่านหน้าเว็บ แล้วมีการร้องขอพิกัดจาก Mobile App เพื่อจะได้ทราบสถานะของการร้องขอพิกัดว่ามีการเข้าใช้งานระบบผ่านหน้าจริงหรือไม่
- Active_Session สำหรับเก็บ Session การเข้าระบบของผู้ดูแลระบบ
- Admin สำหรับเก็บข้อมูลผู้ดูแลระบบ เพื่อเข้าใช้งาน Web Management
- User_device สำหรับเก็บข้อมูล Device ID ของผู้ใช้งาน

- User สำหรับเก็บข้อมูลผู้ใช้ โดยจะมี Custom_Latitude, Custom_Longitude กรณีต้องการกำหนดพิกัดให้กับผู้ใช้โดยตรง
- Position สำหรับเก็บข้อมูลตำแหน่ง
- Department สำหรับเก็บข้อมูลแผนก
- Active_Session_User สำหรับเก็บ Session ของผู้ใช้ที่มีการยืนยันเข้าระบบผ่านหน้าเว็บสำเร็จ
- User_Authen สำหรับเก็บข้อมูลการยืนยันตัวตนของผู้ใช้งาน กรณียืนยันตัวตนสำเร็จ
- User_Mobile_Session สำหรับเก็บ Session ของผู้ใช้ในการเข้าระบบผ่าน Mobile App

3.7 พจนานุกรมข้อมูล (Data Dictionary)

พจนานุกรมข้อมูลของระบบควบคุมการใช้งานอุปกรณ์ ETOKEN ด้วยเทคโนโลยี GPS เพื่อแสดงความสัมพันธ์ของข้อมูลระหว่างตาราง มีองค์ประกอบที่สำคัญของตารางดังนี้

ตารางที่ 3.12 รายละเอียดตาราง Setting

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
Admin_email	E-Mail ผู้ดูแลระบบ	VARCHAR(50)		
Admin_telephone	เบอร์โทรศัพท์ผู้ดูแลระ	VARCHAR(50)		
Authen_radius	รัศมีการยืนยันพิกัด	INT(4)		
Authen_duration	ระยะเวลาในการรอพิกัด	INT(5)		
Default_latitude	พิกัด default ค่า latitude	VARCHAR(20)		
Default_lomgitude	พิกัด default ค่า longitude	VARCHAR(20)		
Api_key	Key สำหรับเรียกใช้ API	VARCHAR(255)		

ตารางที่ 3.13 รายละเอียดตาราง Authen_Wating

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
Id		INT(11)	PK	
User	รหัสผู้ใช้	INT(11)	FK	ตาราง User
Authen_time	ตรวจสอบเวลารอพิกัด	DATETIME		
User_device	รหัส Deivce	INT(11)		

ตารางที่ 3.13 (ต่อ)

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
Latitude	พิกัด Latitude ของผู้ใช้	VARCHAR(20)		
Longitude	พิกัด Longitude ของผู้ใช้	VARCHAR(20)		

ตารางที่ 3.14 รายละเอียดตาราง Active_Session

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(11)	PK	
Session	ข้อมูล Session String	VARCHAR(50)		
Time	ระยะเวลาของ Session	VARCHAR(100)		
Admin	รหัสผู้ดูแลระบบ	TINYINT(4)	FK	ตาราง **Admin**

ตารางที่ 3.15 รายละเอียดตาราง Admin

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		TINYINT(4)	PK	
Username	สำหรับเข้าใช้ระบบ	VARCHAR(30)		
Password	รหัสผ่าน	VARCHAR(255)		
Firstname	ชื่อ	VARCHAR(50)		
Lastname	นามสกุล	VARCHAR(50)		
Created	วันที่สร้างรายชื่อ	DATETIME		

ตารางที่ 3.16 รายละเอียดตาราง User_Device

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(11)	PK	
User	รหัสผู้ใช	INT(11)	FK	ตาราง User
Device_id	หมายเลข IMEI	VARCHAR(255)		
Status	สถานะของ Device	TINYINT(1)		

ตารางที่ 3.17 รายละเอียดตาราง User

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(11)	PK	

ตารางที่ 3.17 (ต่อ)

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
Username	สำหรับเข้าใช้ระบบ	VARCHAR(50)		
Password	รหัสผ่าน	VARCHAR(255)		
Firstname	ชื่อ	VARCHAR(50)		
Lastname	นามสกุล	VARCHAR(50)		
Position	ตำแหน่ง	INT(6)		
Seriel_eToken	Serial อุปกรณ์ eToken	VARCHAR(255)		ตาราง Position
Custom_latitude	พิกัด latitude เฉพาะ	VARCHAR(20)		
Custom_longitude	พิกัด longitude เฉพาะ	VARCHAR(20)		
Status	สถานะของผู้ใช้	TINYINT(1)		

ตารางที่ 3.18 รายละเอียดตาราง Position

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(6)	PK	
Name	ชื่อแผนก	VARCHAR(200)		
Department	รหัสแผนก	TINYINT(4)	FK	ตาราง Department
Status	สถานะของตำแหน่ง	TINYINT(1)		

ตารางที่ 3.19 รายละเอียดตาราง Department

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(4)	PK	
Name	ชื่อแผนก	VARCHAR(100)		
Status	สถานะของแผนก	TINYINT(1)		

ตารางที่ 3.20 รายละเอียดตาราง Active_Session_User

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(4)	PK	
Session	ข้อมูล Session	VARCHAR(50)		
Time	ระยะเวลาของ Session	VARCHAR(100)		
User	รหัสผู้ใช้	INT(11)	FK	ตาราง User

ตารางที่ 3.21 รายละเอียดตาราง User_Authen

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(11)	PK	
User_device	รหัส Device	INT(11)	FK	ตาราง User_Device
Authen_latitude	พิกัด latitude ที่ผู้ใช้เข้ามา	VARCHAR(20)		
Authen_langitude	พิกัด longitude ที่ผู้ใช้เข้ามา	VARCHAR(20)		
Authen_datetime	เวลาการยืนยัน	DATETIME		
Status	สถานะการ	TINYINT(1)		

ตารางที่ 3.22 รายละเอียดตาราง User_Mobile_Session

ชื่อแอตทริบิวต์	คำอธิบาย	ชนิดข้อมูล	คีย์	ตารางที่อ้างถึง
ID		INT(11)	PK	
Session_token	Session เข้าระบบ	VARCHAR(20)		
Created	เวลาในการสร้าง Session	DATETIME		
User	รหัสผู้ใช้	INT(11)	FK	ตาราง User

บทที่ 4

ผลการทดลอง

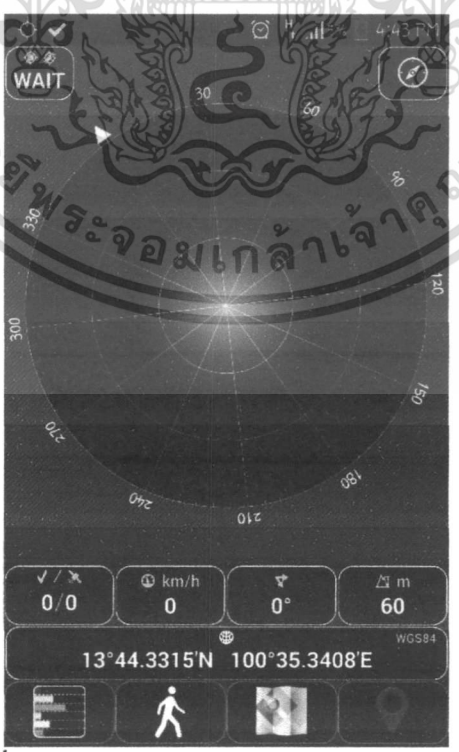
จากการดำเนินการที่ผ่านมาทางผู้พัฒนาระบบได้ทำการออกแบบโครงสร้างการทำงานของการพัฒนาโปรแกรมบน Smartphone โดยการพัฒนาโปรแกรมให้สามารถทำงานได้บนระบบปฏิบัติการ Android และทำการจำลองสร้างหน้าเว็บแอพพลิเคชั่น เพื่อให้เห็นการทำงานโดยรวมของระบบ ซึ่งผลการใช้งานระบบแบ่งออกเป็น 3 ส่วน คือ ส่วนแรกกเป็นการทดสอบการรับค่าพิกัดจาก Smartphone ส่วนที่สองเป็นการใช้งานของผู้ดูแลระบบ และส่วนที่สามเป็นการใช้งานของผู้ใช้ ตามที่ได้นำเสนอต่อไปนี้

4.1 ผลการทดลองรับค่าพิกัด

4.1.1 การทดลองรับค่าจาก Smartphone โดยใช้โปรแกรม Android TS GPS Test

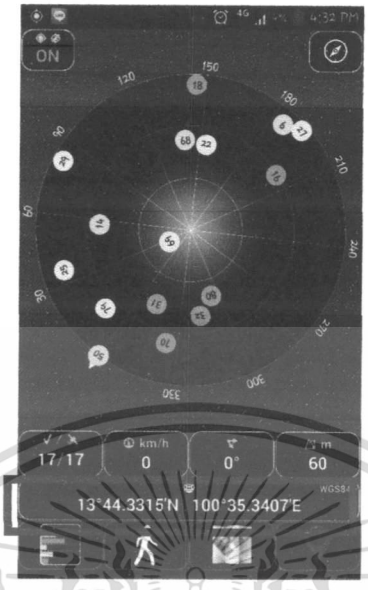
ขั้นตอนการใช้งาน

- เปิดฟังก์ชันการใช้งาน Mobile Data
- เปิดโปรแกรม Android TS GPS Test
- จากนั้น Smartphone จะทำการค้นหาสัญญาณ GPS



รูปที่ 4.1 หน้าจอโปรแกรม Android TS GPS Test

- รอสักครู่ Smartphone จะรับสัญญาณ GPS และแสดงค่าต่าง ๆ



รูปที่ 4.2 หน้าจอแสดงการรับค่า Latitude Longitude จาก Android TS GPS Test

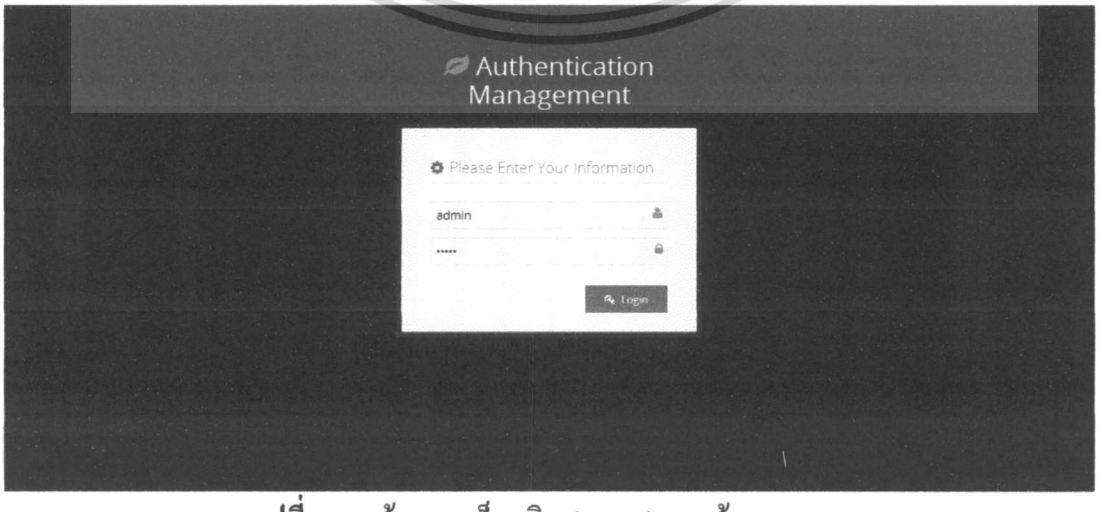
4.2 การใช้งานเว็บแอพพลิเคชั่นของผู้ดูแลระบบ

4.2.1 การใช้งานเว็บแอพพลิเคชั่น

ระบบควบคุมการใช้งานอุปกรณ์ eToken ด้วยเทคโนโลยี GPS ได้ถูกพัฒนาขึ้นมาเพื่อทำการตรวจสอบการใช้งานอุปกรณ์ eToken ให้อยู่ในพื้นที่ที่กำหนดให้ใช้งานเท่านั้น

4.2.2 หน้าจอล็อกอิน (Login)

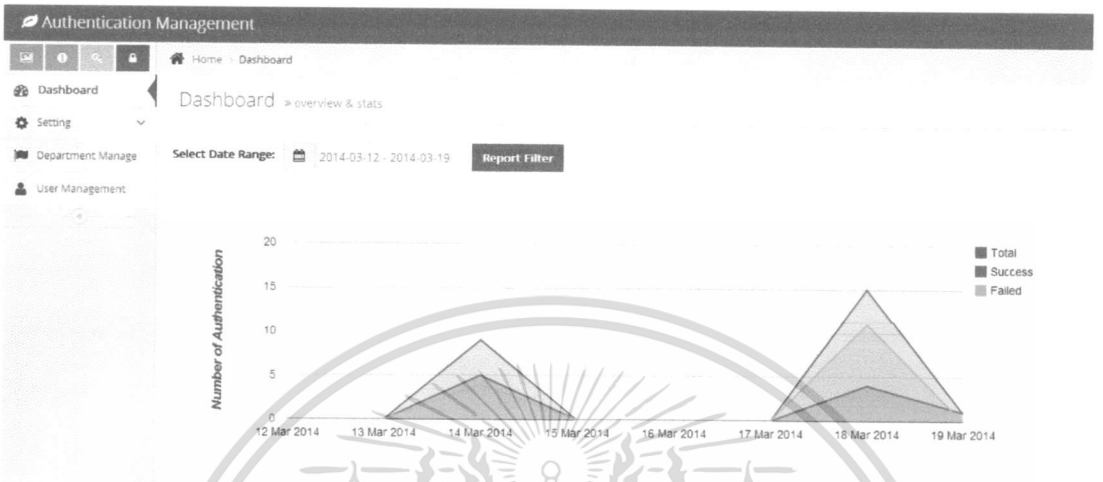
เจ้าหน้าที่ดูแลระบบต้องทำการล็อกอินเข้าสู่ระบบก่อนทุกครั้งเพื่อใช้งานในส่วนต่าง ๆ ของโปรแกรม หน้าจอล็อคอินดังรูปภาพที่ 4.3



รูปที่ 4.3 หน้าระบบล็อกอิน (Login) ของผู้ดูแลระบบ

4.2.3 หน้าจอของผู้ดูแลระบบ

หลังจากทำการล็อคอิน (Login) เข้าระบบโดยผู้ดูแลระบบจะพบกับเมนูการใช้งานต่าง ๆ ซึ่งจะแยกตามประเภทของการใช้งาน โดยจะมีรายละเอียด ดังรูปภาพที่ 4.4



รูปที่ 4.4 หน้าจอการทำงานโดยรวมของผู้ดูแลระบบ

การใช้งานของผู้ดูแลระบบจะถูกแบ่งการทำงานออกเป็นทั้งหมด 4 เมนู ซึ่งแต่ละเมนู มีรายละเอียดดังนี้

เมนู Dashboard

- ส่วนนี้เป็นการแสดงรายละเอียดการเข้าใช้ระบบของผู้ใช้ โดยจะแสดงส่วนประกอบของการเข้าใช้ที่อยู่ในรูปแบบของกราฟและตาราง ซึ่งสามารถแสดงรายงานการเข้าใช้ระบบโดยระบุเป็นช่วงเวลา เช่น รายวัน รายสัปดาห์ รายเดือน และรายปี เป็นต้น

เมนู Setting ประกอบด้วย 2 ส่วน ดังนี้

- ส่วนที่ 1 GEO Setting เป็นการตั้งค่าพิกัดมาตรฐาน สำหรับการกำหนดพื้นที่การใช้งานของอุปกรณ์ eToken เช่น ที่ตั้งของบริษัทหรือหน่วยงานที่ต้องใช้งานเป็นประจำ
- ส่วนที่ 2 Authentication Setting ประกอบด้วย 4 ส่วน ของการตั้งค่าการใช้งานดังนี้
    - Admin E-Mail ใช้สำหรับกำหนด E-Mail Account ของผู้ดูแลระบบ เมื่อผู้ใช้จำเป็นที่จะต้องส่งพิกัดกลับมายังผู้ดูแลระบบตาม E-Mail Account ที่ได้แจ้งเอาไว้ในระบบ
    - Telephone ใช้สำหรับกำหนดเบอร์โทรศัพท์ของผู้ดูแลระบบ เมื่อผู้ใช้จำเป็นที่จะต้องส่งพิกัดกลับมายังผู้ดูแลระบบตามเบอร์โทรศัพท์ที่ได้แจ้งเอาไว้ในระบบ

- ระยะทาง ใช้สำหรับการกำหนดระยะรัศมีการเข้าใช้งานของอุปกรณ์ eToken ว่าสามารถใช้งานได้กี่กิโลเมตรจากจุดที่ Smartphone อยู่ ณ ปัจจุบัน
- ระยะเวลา ใช้สำหรับการกำหนดเวลาในการยืนยันตัวตนเข้าระบบ ถ้าเกินจากเวลาที่ระบบได้กำหนดไหว้ ระบบจะให้ทำการยืนยันเข้าระบบใหม่อีกครั้ง หรือกว่าผู้ใช้งานจะทำการส่งพิกัดจาก Smartphone ไปยัง Server

เมนู Department และ Position

- ส่วนนี้เป็นการแสดงข้อมูล Department และ Position ซึ่งสามารถทำการค้นหา เพิ่ม ลบ และแก้ไขข้อมูลของ Department และ Position

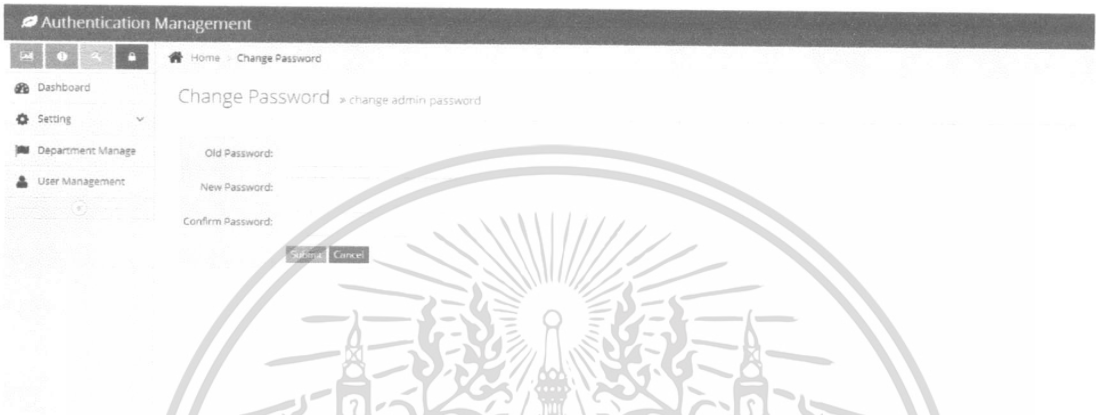
เมนู User Mangement

- ส่วนนี้เป็นการแสดงข้อมูลผู้ใช้และข้อมูล Smartphone ซึ่งจะประกอบไปด้วยรายละเอียดต่าง ๆ ดังนี้
  - ชื่อ นามสกุล (FirstName, Lastname)
  - ชื่อเข้าใช้ระบบ
  - แผนก (Department)
  - ตำแหน่ง (Position)
  - จำนวนของอุปกรณ์ที่ผู้ใช้มีการใช้งานร่วมอยู่ด้วย (Device)
  - วันและเวลาที่ผู้ใช้ทำการยืนยันตัวตนด้วยพิกัด (Last Login Time)
  - พิกัดที่ผู้ใช้ ใช้งานอยู่ ณ ปัจจุบัน (Authen Location) ซึ่งสามารถทำการเปลี่ยนพิกัดได้ จะใช้ในกรณีที่ผู้ใช้ต้องการใช้งานอุปกรณ์ eToken นอกบริเวณพื้นที่ของบริษัทหรือหน่วยงาน

  ซึ่งสามารถทำการค้นหา เพิ่ม ลบ และแก้ไขข้อมูลที่ได้กล่าวไว้ข้างต้น ตามความต้องการของผู้ดูแลระบบ หรือว่าอาจจะมีการร้องขอมาจากผู้ใช้ก็เป็นได้

4.2.4 หน้าจอการเปลี่ยนรหัสผ่านของผู้ดูแลระบบ

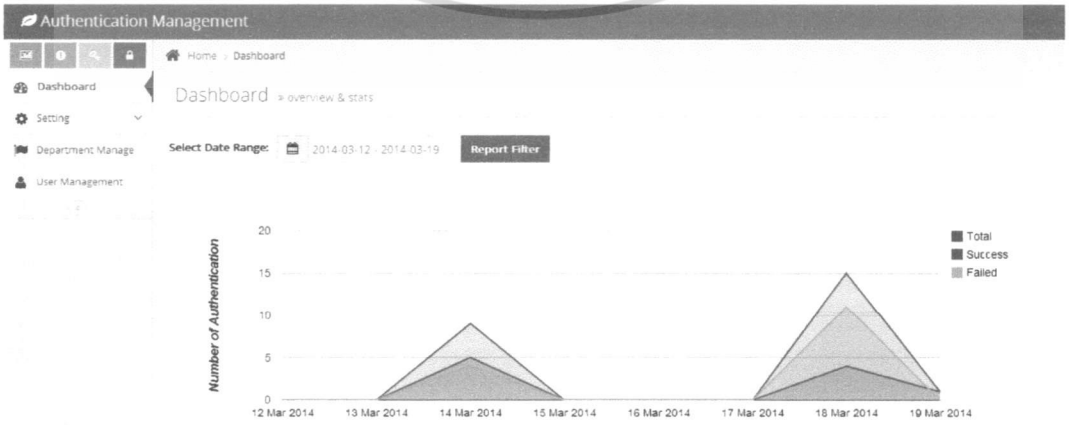
ผู้ดูแลระบบสามารถทำการเปลี่ยนรหัสผ่านได้ด้วยตนเอง เนื่องการใช้รหัสผ่านที่ใช้อยู่ ณ ปัจจุบันอาจจะทำให้ไม่ปลอดภัยเท่าที่ควร จึงจำเป็นต้องมีการเปลี่ยนรหัสผ่านอยู่เป็นประจำ สามารถทำการเปลี่ยนรหัสผ่าน โดยการระบุรหัสผ่านเดิมในช่อง Old Password พร้อมกับระบุรหัสผ่านใหม่ในช่อง New Password และทำการยืนยันรหัสผ่านอีกครั้งในช่อง Confirm Password ได้ดังรูปภาพที่ 4.5



รูปที่ 4.5 หน้าจอการเปลี่ยนรหัสผ่านของผู้ดูแลระบบ

4.2.5 หน้าจอ Dashboard

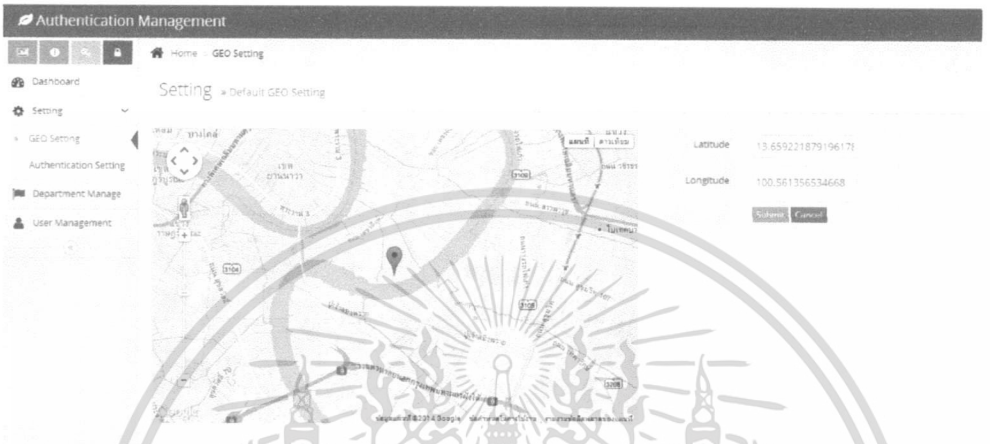
หน้าจอ Dashboard จะแสดงรายละเอียดการเข้าใช้งานระบบของผู้ใช้โดยจะถูกแบ่งออกเป็น 3 ส่วน ส่วนที่ 1 จะแสดงผลออกเป็นกราฟโดยมีสถานะ Total Success Failed จะมีการแสดงผลโดยแยกสีตามสถานะ ส่วนที่ 2 เป็นการแสดงพิกัดปัจจุบันที่ผู้ใช้ได้ทำการเข้าใช้ระบบ โดยสามารถเลือก Authen Location ก็จะทราบพิกัดที่ผู้ใช้อยู่ทันที ส่วนที่ 3 สามารถทำการรายงานผลการเข้าใช้ระบบ โดยระบุการรายงานผลเป็นช่วงเวลา เช่น รายวัน รายสัปดาห์ รายเดือน และรายปี ได้ดังรูปภาพที่ 4.6



รูปที่ 4.6 หน้าจอ Dashboard

4.2.6 หน้าจอแสดงการตั้งค่า Default GEO Setting

หน้าจอ Default GEO Setting เป็นการตั้งค่าพิกัดมาตรฐาน สำหรับการกำหนดพื้นที่การใช้งานของอุปกรณ์ eToken เช่น ที่ตั้งของบริษัทหรือหน่วยงานที่ต้องใช้งานเป็นประจำ โดยการเลื่อนจุดสีแดงไปยังเป้าหมายที่กำหนด หรือจะใส่ค่า Latitude และ longitude ลงในช่องรับค่าก็ได้ได้ดังรูปภาพที่ 4.7



รูปที่ 4.7 หน้าจอแสดงการตั้งค่า Default GEO Setting

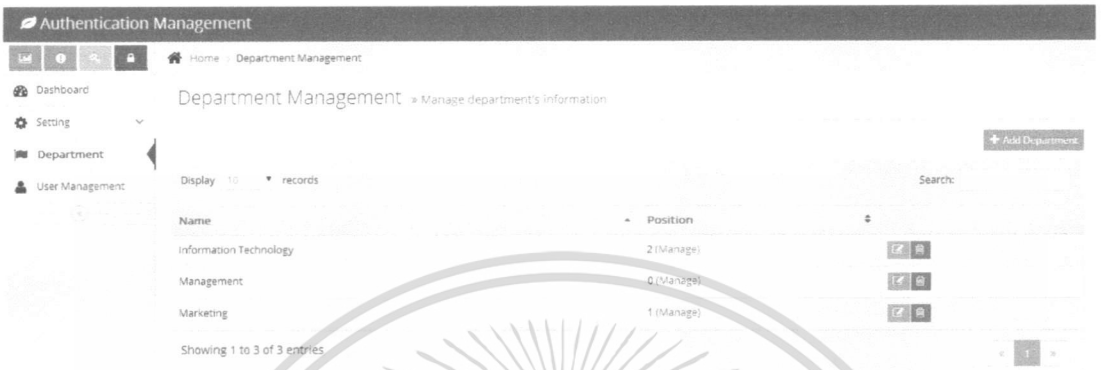
4.2.7 หน้าจอแสดงการตั้งค่า Authentication Setting

หน้าจอ Authentication Setting จะแบ่งการตั้งค่าเป็น 4 ส่วน คือ ส่วนที่ 1 เป็นการระบุ E-Mail Account ใช้สำหรับการรับพิกัดจากผู้ใช้ ส่วนที่ 2 เป็นการระบุเบอร์โทรศัพท์ ใช้สำหรับการรับพิกัดจากผู้ใช้ผ่านระบบข้อความ ส่วนที่ 3 ใช้สำหรับการกำหนดระยะรัศมีการเข้าใช้งานของอุปกรณ์ eToken ว่าสามารถใช้งานได้กี่กิโลเมตรจากจุดที่ Smartphone อยู่ ณ ปัจจุบัน ส่งนที่ 4 ใช้สำหรับการกำหนดเวลาในการยืนยันตัวตนเข้าระบบ ถ้าเกินจากเวลาที่ระบบได้กำหนดไหว้ ระบบจะให้ทำการยืนยันเข้าระบบใหม่อีกครั้ง หรือกว่าผู้ใช้งานจะทำการส่งพิกัดจาก Smartphone ไปยัง Server ได้ ดังรูปภาพที่ 4.8

รูปที่ 4.8 หน้าจอแสดงการตั้งค่า Authentication Setting

4.2.8 หน้าจอแสดงรายละเอียดของ Department และ Position

หน้าจอ Department และ Position ใช้สำหรับการค้นหา เพิ่ม ลบ และแก้ไขในส่วนของ Department และ Position เพื่อนำทั้ง 2 ส่วนไปใช้ในหน้าของ User Management ในกรณีที่มีการเพิ่มผู้ใช้ใหม่หรือมีการแก้ไขเกิดขึ้น ได้ ดังรูปภาพที่ 4.9



รูปที่ 4.9 หน้าจอแสดงรายละเอียดของ Department และ Position

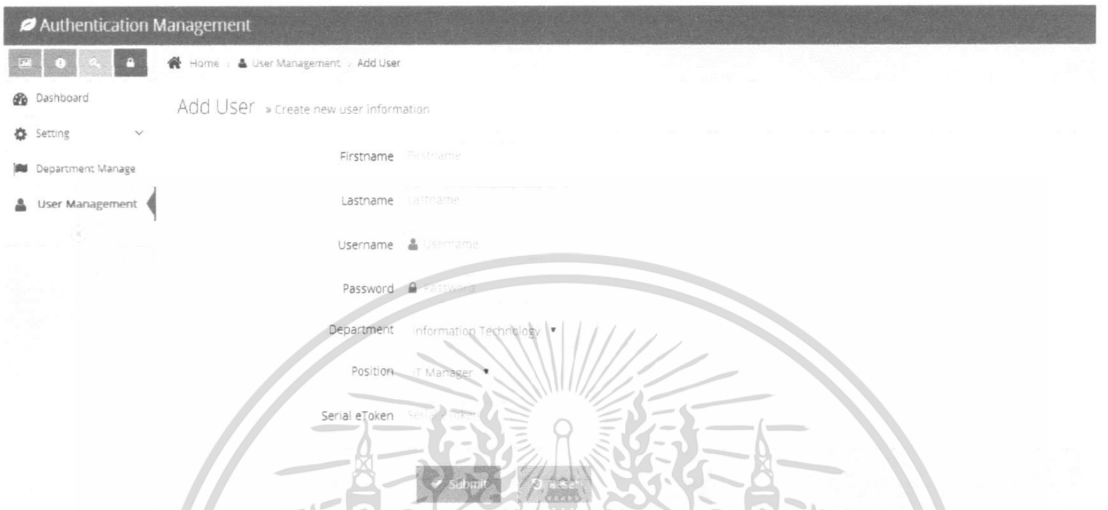
4.2.9 หน้าจอแสดงรายละเอียดของ User Management

หน้าจอ User Management ใช้สำหรับการแสดงข้อมูลโดยรวมของผู้ใช้ ซึ่งระบบสามารถทำการค้นหา เพิ่ม ลบ และแก้ไขข้อมูลของผู้ใช้ รวมถึงข้อมูล Smartphone (Device ID) ได้ ซึ่งข้อมูลพิกัดปัจจุบันของผู้ใช้ สามารถทำการเปลี่ยนแปลงได้อย่างเดียว ค่าที่มีการเปลี่ยนแปลงนั้นขึ้นอยู่กับผู้ใช้โดยตรงว่าจะนำอุปกรณ์ eToken ไปใช้งานที่ใด ดังรูปภาพที่ 4.10

รูปที่ 4.10 หน้าจอแสดงรายละเอียดของ User Management

4.2.10 หน้าจอแสดงการเพิ่มผู้ใช้

หน้าจอ Add User ใช้สำหรับทำการเพิ่มผู้ใช้งานเข้าสู่ระบบ ซึ่งจะประกอบด้วยรายละเอียดที่ต้องใส่ในช่องรับค่า คือ ชื่อ นามสกุล ชื่อเข้าใช้ระบบ รหัสผ่าน แผนก ตำแหน่ง และข้อมูลอุปกรณ์ eToken ดังรูปภาพที่ 4.11



รูปที่ 4.11 หน้าจอแสดงการเพิ่มผู้ใช้

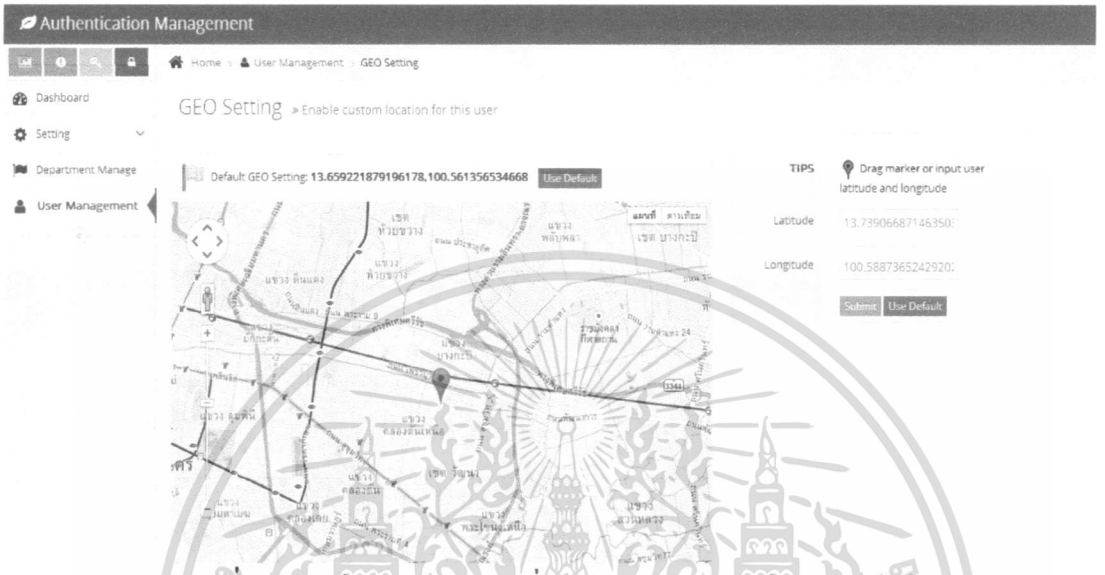
4.2.11 หน้าจอแสดงการเพิ่ม Device ID

หน้าจอ Device Management ใช้สำหรับทำการเพิ่ม ลบและแก้ไขข้อมูล Device ID ของผู้ใช้ ซึ่งจะประกอบด้วยรายละเอียดที่ต้องใส่ในช่องรับค่า คือ เลข EMI ของ Smartphone ในหน้าจอของ Device Management จะแสดง ชื่อของผู้ใช้ พิกัดล่าสุด พร้อมกับ Smartphone ที่ผู้ใช้มีการใช้งานร่วมกับอุปกรณ์ eToken ดังรูปภาพที่ 4.12

รูปที่ 4.12 หน้าจอแสดงการเพิ่ม Device ID

4.2.12 หน้าจอแสดงการเปลี่ยนแปลงพิกัดการใช้งานของผู้ใช้

หน้าจอ GEO Setting Enable custom location for this user ใช้สำหรับทำการเปลี่ยนแปลงพิกัดการเข้าใช้งาน ในกรณีที่ผู้ใช้มีการเปลี่ยนสถานที่การใช้อุปกรณ์ eToken ผู้ดูแลระบบสามารถทำการเปลี่ยนแปลงพิกัดตามความต้องการของผู้ใช้ได้ทันที ดังรูปภาพที่ 4.13



รูปที่ 4.13 หน้าจอแสดงการเปลี่ยนแปลงพิกัดการใช้งานของผู้ใช้

4.2.13 หน้าจอแสดงการแก้ไขข้อมูลผู้ใช้

หน้าจอ Edit User ใช้สำหรับแก้ไขข้อมูลของผู้ใช้ ซึ่งจะประกอบด้วยรายละเอียดที่สามารถแก้ไขในช่องรับค่า คือ ชื่อ นามสกุล แผนก ตำแหน่ง และ Serial ของอุปกรณ์ eToen ดังรูปภาพที่ 4.14

รูปที่ 4.14 หน้าจอแสดงการแก้ไขข้อมูลผู้ใช้

4.3 การใช้งานแอพพลิเคชั่นบน Smartphone ในส่วนของผู้ใช้

การใช้งานของผู้ใช้จะถูกแบ่งออกเป็น 2 ส่วน คือ ส่วนของการใช้แอพพลิเคชั่นบน Smartphone และส่วนของขั้นตอนการนำอุปกรณ์ eToken และค่าพิกัดที่ได้จาก Smartphone ไปใช้ในการยืนยันตัวตนเข้าระบบขององค์กร ซึ่งมีรายละเอียดดังนี้

4.3.1 ส่วนของการใช้งานแอพพลิเคชั่นบน Smartphone

การใช้แอพพลิเคชั่นบน Smartphone ซึ่งจะถูกแบ่งการทำงานออกเป็น 7 ส่วน แต่ละส่วนจะมีการใช้งานที่แตกต่างกันดังนี้

รูปที่ 4.15 แสดภาพหน้าจอการทำงานโดยรวมของผู้ใช้

4.3.1.1 หน้าจอล็อกอิน (Login)

ใช้สำหรับการยืนยันตัวตนเข้าระบบ เพื่อทำการเรียกใช้ข้อมูลของผู้ใช้ที่ถูกเก็บไว้ในฐานข้อมูลมาแสดงยังที่หน้าจอ Smartphone

4.3.1.2 User Information

ใช้สำหรับการแสดงข้อมูลต่าง ๆ ของผู้ใช้ที่หน้าจอ Smartphone ซึ่งผู้ใช้สามารถทำการเปลี่ยนรหัสผ่านของผู้ใช้ได้จากส่วนนี้

4.3.1.3 Current Location

ใช้สำหรับการแสดงสถานที่ปัจจุบันของผู้ใช้ที่หน้าจอ Smartphone ซึ่งผู้ใช้สามารถนำข้อมูลของสถานที่ไปอ้างอิงกับผู้ดูแลระบบได้ เพื่อใช้เป็นการยืนยันสถานที่ได้อีกด้วย

4.3.1.4 Send Your Location

ใช้สำหรับการส่งพิกัดปัจจุบันของผู้ใช้ไปยัง Server เพื่อนำค่าพิกัดที่ได้นั้น ไปทำการตรวจสอบเงื่อนไข ส่วนนี้จะใช้ก็ต่อเมื่อผู้ใช้จะต้องการยืนยันตัวตนเข้าระบบร่วมกับอุปกรณ์ eToken เท่านั้น

4.3.1.5 Change Password

ใช้สำหรับการเปลี่ยนรหัสผ่านของผู้ใช้

4.3.1.6 Sign Out

ใช้สำหรับสิ้นสุดการใช้งานของโปรแกรม

4.3.1.7 E-Mail และ SMS

ใช้สำหรับการส่งข้อความพร้อมกับพิกัดที่ผู้ใช้ต้องการใช้งาน ในกรณีที่มีการเปลี่ยนแปลงสถานที่การใช้งานอุปกรณ์ eToken ในรูปแบบ E-Mail และ SMS

4.3.2 ขั้นตอนการยืนยันตัวตนเข้าสู่ระบบองค์กร

ขั้นตอนการทดลองการยืนยันตัวตนด้วยอุปกรณ์ eToken และค่าพิกัดที่ได้จาก Smartphone มีหลักการทำงานดังนี้ ให้ผู้ใช้งานทำการเสียบอุปกรณ์ eToken เข้ากับเครื่องคอมพิวเตอร์หลังจากนั้น เปิดใช้งานระบบผ่านเว็บบราวเซอร์ขึ้นมา จากนั้นทำการยืนยันรหัสผ่านของอุปกรณ์ eToken เมื่อทำการยืนยันแล้วระบบจะมีข้อความแจ้งว่าให้ทำการส่งพิกัดจาก Smartphone ของผู้ใช้ไปยัง Server หลังจากที่ผู้ใช้ได้ส่งค่าไปที่ Server แล้ว ให้ทำการยืนยันที่ระบบผ่านเว็บบราวเซอร์ ระบบจะทำการตรวจสอบพิกัดของผู้ใช้ว่าตรงตามเงื่อนไขหรือไม่ ถ้าตรงตามเงื่อนไขก็สามารถเข้าใช้งานระบบได้ทันที

บทที่ 5
สรุปผลและแนวทางการพัฒนาต่อ

5.1 สรุปผลการทดลอง

จากการทดลองที่ได้กล่าวไว้ในหัวข้อ 4.1 และ 4.2 แสดงให้เห็นว่า ระบบที่ถูกพัฒนาขึ้นมานี้สามารถควบคุมและกำหนดพื้นที่การใช้งานอุปกรณ์ eToken ได้ เนื่องจากการยืนยันตัวตนแบบ 2 ระดับมีความแข็งแรงอยู่แล้ว แต่เมื่อมีการเพิ่ม การตรวจสอบพื้นที่ที่ผู้ใช้อยู่ปัจจุบันทำให้ระบบมีความแข็งแรงเพิ่มขึ้นอีกระดับ ทำให้ความเสียงต่อความเสียหายของข้อมูลในองค์กรลดน้อยลง ต่อให้อุปกรณ์ eToken สูญหายก็ไม่มีผลกระทบต่อระบบ

5.2 ผลประโยชน์ที่ได้รับหลังจากการทดลอง

- มีความรู้และความเข้าใจหลักการทำงานและการใช้งานของระบบ GPS
- ได้เรียนรู้การใช้งานและการประยุกต์ใช้งาน GPS
- มีความรู้และความเข้าใจในการเขียน Application Android และมีความเข้าใจวิธีการสื่อสารข้อมูลและการประมวลผลข้อมูล
- สามารถควบคุมการใช้งานอุปกรณ์ eToken ตามพื้นที่ ที่กำหนด
- สามารถค้นหาอุปกรณ์ eToken จากตำแหน่งที่ Smartphone อยู่ได้
- อุปกรณ์ eToken มีความปลอดภัยในการใช้งานเพิ่มขึ้น

5.3 แนวทางการพัฒนาต่อ

นำวงจรการทำงานของอุปกรณ์ eToken ผนวกรวมกับไมโครคอนโทลเลอร์ (Microcontroller) และ GPS Module เป็นชิ้นเดียวกัน (Build-in device) เพื่อให้สะดวกต่อการใช้งานและลดขั้นตอนของการทำงานของระบบที่ถูกพัฒนาขึ้นมา ซึ่งปัจจุบันยังไม่สามารถนำมาใช้งานได้ เนื่องจากอุปกรณ์ที่กล่าวมาข้างต้นนั้น ยังมีขนาดที่ค่อนข้างใหญ่ทำให้ยากต่อการนำมาใช้งาน ซึ่งผู้พัฒนามีความคิดเห็นว่า เทคโนโลยีมีการเปลี่ยนแปลงอยู่ตลอดเวลาอาจทำให้อุปกรณ์ที่กล่าวมาข้างต้นนั้นมีขนาดเล็กลงและสมารถนำไปพัฒนาต่อก็เป็นได้

บรรณานุกรม

กัลยาณี เปลี่ยนผัน. 2552. ระบบระบุตำแหน่งผู้ใช้โทรศัพท์เคลื่อนที่ด้วย GPS ผ่านทาง SMS ปริญญานิพนธ์ วิศวกรรมโทรคมนาคม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

จตุชัย แพงจันทร์. 2553. Master in Security 2nd Edition นนทบุรี : ไอดีซีฯ.

นันทวัฒน์ เพชรมณี. 2546. การออกแบบพิกัดบนแผนที่โดยใช้จีพีเอส. ปริญญานิพนธ์ วิศวกรรมอิเล็กทรอนิกส์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

ปรัชญา ไชยเมือง และสมนึก พ่วงพรพิทักษ์, "การยืนยันตัวตนสองปัจจัย ณ จุดเดียวบนเว็บแอปพลิเคชั่นโดยใช้เทคโนโลยีเว็บเซอร์วิสและเจทูเอมอี" ,ECTI-CARD2010, MAY'10, Pataya, Thailand, หน้า 450-455.

พร้อมเลิศ หล่อวิจิตร. 2556. คู่มือเขียนแอพ Android ฉบับสมบูรณ์.กรุงเทพฯ : โปรวิชั่น.

วิกิพีเดีย – จีพีเอส [Online]: http://th.wikipedia.org/wiki/จีพีเอส#cite_note-1

วิกิพีเดีย – สมาร์ทโฟน [Online]: http://th.wikipedia.org/wiki/สมาร์ทโฟน

J.Paek, J.Kim, and R.Govindan, "Energy-Efficient Rate-Adaptive GPS-based Positioning for Smartphons," ACM 978-1-60558-985 5/10/06. MobiSys' 10, June 15-18,2010.

SafeNet Inc – eToken Pro Authentication Token [Online]: http://www.safenet-inc.com/product/data-protection/two-factor-authentication/etoken-pro/

Security Concepts – Somewhere are you [Online]: http://www.subspacefield.org/security/security_concepts/index.html#toc-Subsection-11.8

Z.Feng, Kondoro, A. and S.Muftic, "Location-Based Authentication and Authorization Using Smartphones" Trust, Security and Privacy in Computer and Communications (TrustCom), *2012 IEEE 11th International Conferrence on.*

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายวัลลภ มั่นน้อย
วัน เดือน ปีเกิด	26 ตุลาคม 2526
ที่อยู่	21/272 หมู่ที่ 18 หมู่บ้านรัชธานี 2 ถนนเทพารักษ์ ตำบลบางพลีใหญ่ อำเภอบางพลี จ.สมุทรปราการ 10540
อีเมล	wanlop_munnoi@hotmail.com

ประวัติการศึกษา

2553	วิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี วิทยาลัยเซาธ์อีสท์บางกอก