การตรวจสอบบุคคลโดยอาศัยช่วงเวลาในการกดคีย์บอร์ด

AUTHENTICATION BY THE TIMING OF KEYPRESSES

กฤษฎาญชล สะดีวงศ์

หัสนัย พุทธวงค์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2550

ปริญญานิพนธ์ปีการศึกษา 2550

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การจดจำบุคคลโดยอาศัยช่วงเวลาในการกดคีย์บอร์ด

IDENTIFYING PERSON BY THE TIMING OF KEYPRESSES

ผู้จัดทำ

1. นายกฤษฎาญชล สะดีวงศ์ รหัสนักศึกษา 48015325
2. นายหัสนัย พุทธวงค์ รหัสนักศึกษา 48015363

_____ อาจารย์ที่ปรึกษา

(ผศ. เกียรติกูล เจียรนัยธนะกิจ)

การตรวจสอบบุคคลโดยอาศัยช่วงเวลาในการกดคีย์บอร์ด

นายกฤษฎาญชล สะดีวงค์ 48015325
นายหัสนัย พุทธวงค์ 48015363
ผศ. เกียรติกูล เจียรนัยธนะกิจ อาจารย์ที่ปรึกษา
ปีการศึกษา 2550

บทคัดย่อ

ในปัจจุบันนี้ ระบบป้องกันภัยส่วนมากนิยมใช้รหัสผ่านเป็นกุญแจในการเข้าระบบ ซึ่งระบบนี้ยังคงมีข้อเสียอยู่ เพราะระบบไม่สามารถตรวจสอบได้ว่ารหัสผ่านที่ใช้เข้าระบบนั้นเป็นของเจ้าของตัวจริงหรือไม่ ถ้าบุคคลอื่นล่วงรู้รหัสผ่านก็จะสามารถเข้าระบบได้เช่นกัน

โครงงานนี้เสนอการพัฒนาระบบการตรวจสอบบุคคล โดยใช้ช่วงเวลาในการพิมพ์รหัสผ่านของผู้ใช้ ข้อมูลค่าเวลาที่ได้จะนำไปใช้ในการฝึกสอนโครงข่ายประสาทเทียมให้สามารถรู้จำรูป แบบการพิมพ์รหัสผ่านข้อผู้ใช้ เพื่อนำไปใช้ในการตรวจสอบบุคคลที่ร้องขอเข้าระบบต่อไป

AUTHENTICATION BY THE TIMING OF KEYPRESSES

MR. Kritsadanshon Sadeewong 48015325

MR. Hasanai Phutthawong 48015363

ASST. PROF. Kietikul Jearanaitanakij Advisor

Academic Year 2007

ABSTRACT

Nowadays there are many security systems that use password as an only access key. This method still has the disadvantage, because the password can be easily know by another person, then system can be accessed by someone other than its owner.

This project proposes a development of a prototype of an authentication system that applies the neural network theory to identify a person from his or her keystrokes. We have used time intervals between keystrokes as an input to train the neural network and identify the person later.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้คงไม่อาจสำเร็จได้ด้วยดี หากไม่ได้รับความช่วยเหลือ และความร่วมมือจากหลายๆฝ่ายด้วยกัน บุคคลแรกที่ต้องกล่าวถึง เพราะเป็นบุคคลสำคัญที่ทำให้ปริญญานิพนธ์ฉบับนี้สำเร็จได้ด้วยดี ก็คือ ผศ.เกียรติกูล เจียรนัยธนะกิจ ที่ให้เกียรติเป็นอาจารย์ที่ปรึกษาคอยช่วยแนะนำ แนะแนวความรู้ และให้ความช่วยเหลือเสมอมา ต้องขอกราบขอบพระคุณเป็นอย่างยิ่งครับ และต้องขอขอบคุณบุคคลท่านอื่นๆ ที่ได้ให้ความช่วยเหลือ ทั้งทางด้านแนวคิดก็ดี ทางด้านเทคนิคใหม่ๆ ในการเขียนโปรแกรมก็ดี หรือแม้แต่บุคคลที่คอยเป็นกำลังใจให้ ซึ่งมิอาจที่จะกล่าวถึงได้หมด

และที่จะขาดเสียมิได้ ซึ่งเป็นบุคคลที่สำคัญที่สุดในชีวิต ที่ทำให้ข้าพเจ้ามีวันนี้ ก็คือ บิดามารดา อันเป็นที่เคารพรักยิ่ง ซึ่งได้เลี้ยงดูข้าพเจ้ามาเป็นอย่างดี พร้อมทั้งให้โอกาสทางการศึกษาอย่างเต็มที่ และยังให้กำลังใจ เอาใจใส่เสมอมาในทุกๆ ด้าน ข้าพเจ้าขอระลึกถึงพระคุณอันสุดประมาณ และขอกราบขอบพระคุณมา ณ. ที่นี้

กฤษฎาญชล สะดีวงค์

หัสนัย พุทธวงค์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

รูปที่ **หน้า**

สารบัญภาพ (ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาของปัญหา

"ภัยคุกคามจากเทคโนโลยี" ปัจจุบันถือเป็นภัยคุกคามที่ร้ายแรง อันเนื่องมาจากความก้าวหน้าของเทคโนโลยี และความเสื่อมโทรมของจิตใจคน ภัยคุกคามจากเทคโนโลยีมีหลากหลายรูปแบบ แต่สิ่งหนึ่งที่เป็นปัญหาร้ายแรงมากก็คือ ภัยคุกคามจากการถูกจารกรรมข้อมูล ไม่ว่าจะเป็นการจารกรรมข้อมูลส่วนบุคคล ไปจนถึงการจารกรรมข้อมูลสำคัญๆระดับประเทศ ต่างก็ส่งผลเสียต่อผู้ถูกกระทำทั้งสิ้น

ระบบรักษาความปลอดภัยส่วนมากมักใช้ รหัสผ่าน หรือบัตรผ่านเพื่อเข้าสู่ระบบ ซึ่งยังคงมีข้อเสียอยู่มาก เช่นระบบไม่สามารถตรวจสอบได้ว่ารหัสผ่าน หรือบัตรผ่านที่ใช้เข้าระบบนั้นเป็นของเจ้าของจริงหรือไม่ ยังผลให้เกิดความสูญเสียและส่งผลร้ายตามมา

โครงงานนี้จัดทำขึ้นเพื่อเสริมระบบป้องกันข้อมูลที่ใช้รูปแบบของรหัสผ่าน โดยนำเอาทฤษฎีไบโอเมตริกซ์(Biometrics) มาใช้ ไบโอเมตริกเป็นการนำลักษณะทางกายภาพ (Physiological Feature) และ ลักษณะทางพฤติกรรม (Behavioral feature) มาใช้ในการทดสอบบุคคล (Personal verification) เพื่อยืนยันหรือปฏิเสธว่าเป็นบุคคลที่กล่าวอ้างหรือไม่ หรือการระบุบุคคล (Personal identification) เพื่อระบุว่าเป็นบุคคลใดในระบบ

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคล จากบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูล

1.2.2 เพื่อแก้ปัญหาการจารกรรมข้อมูล หรือทรัพย์สินส่วนบุคคล อันเนื่องมาจากการถูกล่วงรู้รหัสผ่านที่ใช้ในการป้องกันการเข้าถึงข้อมูล

1.3 ประโยชน์ที่คาดว่าจะได้รับ

ระบบป้องกันการเข้าถึงข้อมูลหรือทรัพย์สินส่วนบุคคล ที่ถึงแม้ว่าผู้ที่ทำการพิมพ์รหัส ผ่านจะล่วงรู้ถึงรหัสก็ตาม แต่ถ้าหากมิใช่เจ้าของข้อมูลที่ได้ทำการลงทะเบียนไว้ ก็จะไม่สามารถเข้าถึงข้อมูล หรือทรัพย์สินส่วนบุคคล นั้นๆ ได้

1.4 ขอบเขตของโครงงาน

1.4.1 สร้างหน้าต่างจำลองการทำงานของการล็อกอินยูสเซอร์(User login) ซึ่งสามารถ สร้าง, ลบ และแก้ไข ข้อมูลของผู้ใช้ได้

1.4.2 โปรแกรม(Application) สามารถระบุตัวบุคคลที่ทำการล็อกอินได้ แสดงออกมาในรูปแบบของการให้สิทธิเข้าถึงข้อมูล และปฏิเสธการเข้าถึงข้อมูล

1.4.3 การเก็บข้อมูลของผู้ใช้ จัดเก็บในรูปแบบของ เท็กซ์ไฟล์(Text files)

1.4.4 การระบุตัวบุคคลที่ทำการล็อกอิน จะใช้ระบบโครงข่ายประสาทเทียม โดยใช้แบคพรอพเกชั่นเน็ตเวิร์ค และ ซิกมอยด์ฟังก์ชั่น ในการฝึกสอนโครงข่ายประสาทเทียม

1.5 ส่วนประกอบของปริญญานิพนธ์

อธิบายเนื้อหาของรายงานฉบับนี้ในแต่ละบทอย่างคร่าวๆ ดังนี้

เนื้อหาในบทที่ 1 กล่าวถึงความเป็นมาของปัญหา วัตถุประสงค์ของโครงงาน ประโยชน์ที่คาดว่าจะได้รับ ขอบเขตของโครงงาน และส่วนประกอบของรายงาน

เนื้อหาในบทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในโครงงาน

- ทฤษฎี ไบโอเมตริกซ์ (Biometrics)
- ทฤษฎี เครือข่ายประสาทเทียม(Artificial Neural Network)
- ทฤษฎี แบคพรอพเกชั่นเน็ตเวิร์คโมเดล(Back-propagation Network model)

เนื้อหาในบทที่ 3 กล่าวถึงแนวคิด และวิธีการทำงานของระบบ โดยแยกเป็นส่วนของแอพลิเคชั่น (Application) และ ส่วนประมวลผล (Processing)

เนื้อหาในบทที่ 4 กล่าวถึงการทดลอง และผลการทดลอง โดยจำลองการทำงานทั้งหมดบนเครื่อง PC

เนื้อหาในบทที่ 5 กล่าวถึงการสรุปผลของโครงงานโดยจะบอกถึงปัญหาที่เกิดขึ้นกับการทำงานและแนวทางในการพัฒนาต่อ

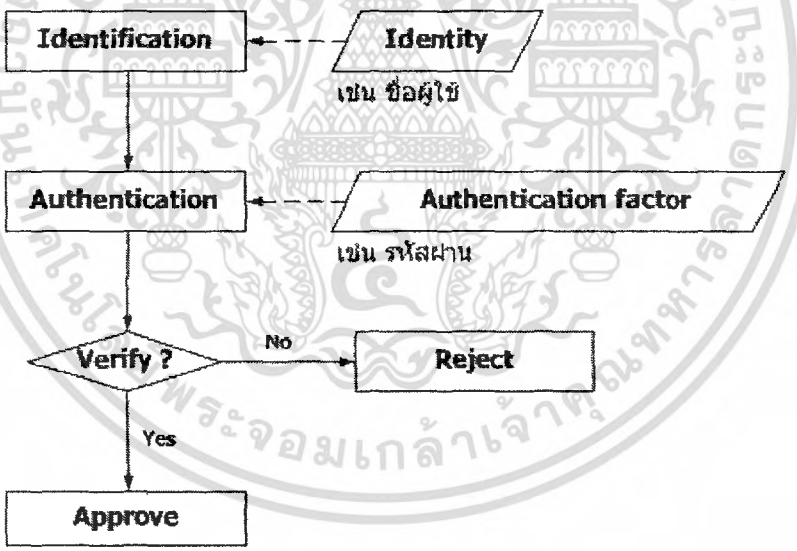
บทที่ 2
หลักและวิธีการตรวจสอบบุคคล

2.1 การตรวจสอบบุคคล

2.1.1 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)
- การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง



รูปที่ 2.1 แผนผังแสดงกระบวนการพิสูจน์ตัวตน

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ

หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิดคือ

- Actual identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร
- Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

- สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น
- สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs) เป็นต้น
- สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ อาจจะถูกดักฟัง, เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็นจัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

ดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (Multi-factor authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

2.1.1.1 การกำหนดสิทธิ (Authorization)

การกำหนดสิทธิ์ คือขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

2.1.1.2 การเข้ารหัส (Encryption)

การเข้ารหัส คือการเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือ ถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าวอ้างนั้นเป็นใคร และ ได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่เข้ารหัสแล้วได้

2.1.1.3 การรักษาความสมบูรณ์ (Integrity)

การรักษาความสมบูรณ์ คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (Source) ไม่ว่าจะเป็นโดยบังเอิญหรือดัดแปลงโดยเจตนาที่อาจส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูลคือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะเข้าควบคุมการจัดการของข้อมูลได้

2.1.1.4 การตรวจสอบ (Audit)

การตรวจสอบ คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่นการตรวจสอบบัญชีชื่อผู้ใช้โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

2.1.2 ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

- การพิสูจน์ตัวตน (Authentication) คือส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง
- การกำหนดสิทธิ์ (Authorization) คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
- การบันทึกการใช้งาน (Accountability) คือการบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

จากที่ได้กล่าวไปข้างต้นว่าการพิสูจน์ตัวตนมีความสำคัญที่สุดกับการเข้าใช้ระบบ จึงสามารถแจกแจงชนิดของการพิสูจน์ตัวตน ที่ใช้กันอยู่ในปัจจุบันว่ามีอะไรบ้างและแต่ละชนิดมีลักษณะอย่างไรได้ดังนี้

2.1.2.1 ไม่มีการพิสูจน์ตัวตน (No Authentication)

ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น ถ้าเงื่อนไขต่อไปนี้เป็นจริง

- ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้
- ข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้นๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

2.1.2.2 การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)

รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ แต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป วิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

2.1.2.3 การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN)

PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่างๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

2.1.2.4 การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens (Authentication by Password Authenticators or Tokens)

ออเทนติคาเตอร์(Authenticator) หรือ โทเค็น (Token) เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัส และอะซิงโครนัส

- การพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ

การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication) เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกดโทเค็น เพื่อให้โทเค็น สร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกดโทเค็น ใส่ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อน ว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบ

การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุกๆ หนึ่งนาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่

รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (รหัส ผ่านจะถูกสร้างขึ้นมาจาก โทเค็น) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่โทเค็น สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ

- การพิสูจน์ตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่างหนึ่งว่า "challenge-response" ถูกพัฒนาขึ้น เป็นลำดับแรกๆ ของระบบการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้" ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้ต้องการจะเข้าสู่ระบบ ผู้ใช้จะต้องทำการร้องของไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง challenge string มาให้ผู้ใช้ เพื่อให้ผู้ใช้ใส่ลงในโทเค็น ที่ผู้ใช้ถืออยู่ จากนั้นโทเค็น จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้ ผู้ใช้จึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้
การพิสูจน์ตัวตนแบบซิงโครนัสทั้งไคลเอ็นต์ และ เซิร์ฟเวอร์จะมีรหัสผ่านเก็บเอาไว้ แต่แบบอะซิงโครนัส ไคลเอ็นต์จะต้องติดต่อเซิร์ฟเวอร์ก่อน ก่อนจะได้รับรหัสผ่านจริง ทำให้การพิสูจน์ตัวตนแบบอะซิงโครนัสมีขั้นตอนที่ซับซ้อนกว่าแบบซิงโคนัส

ตัวอย่างของฮาร์ดแวร์พิเศษที่ใช้ในการสร้างรหัสผ่านซึ่งเปลี่ยนแปลงได้ ของการพิสูจน์ตัวตนโดยใช้ พาสเวิร์ดออเทนติคาเตอร์(Password authenticator) หรือ โทเค็น

รูปที่ 2.2 ฮาร์ดแวร์ที่ใช้สร้างรหัสผ่านที่สามารถเปลี่ยนแปลงได้

2.1.2.5 การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล

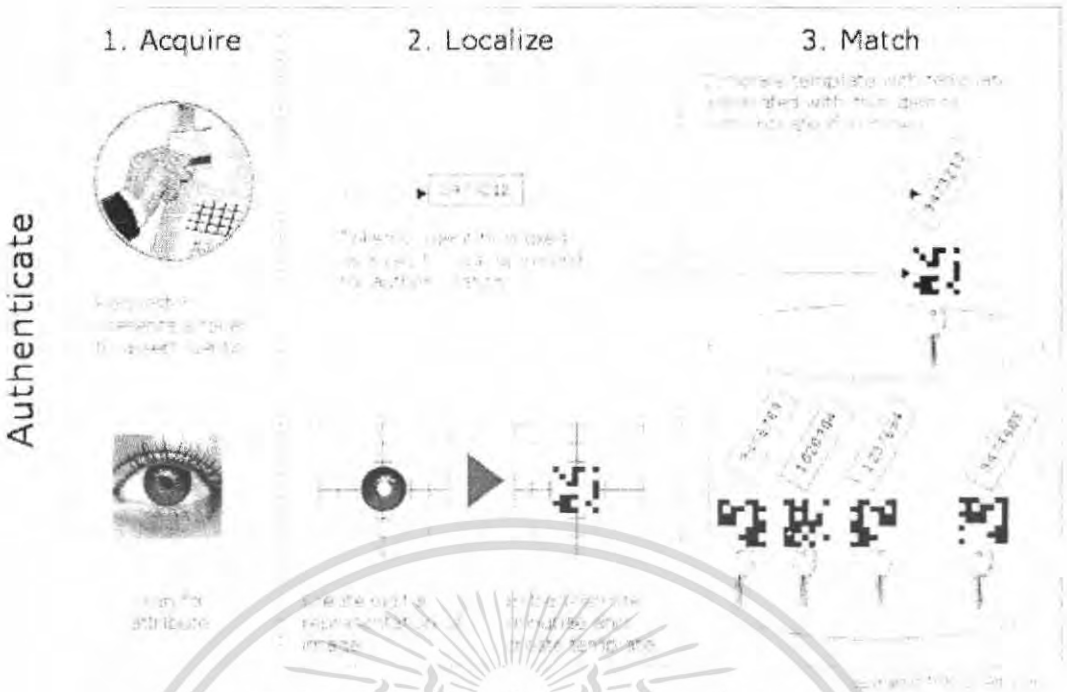
(Authentication by Biometric traits)

ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่น การใช้ควบคู่กับการใช้รหัสผ่าน

ตัวอย่างการใช้งานของการพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพร่วมกับการใช้โทเค็นการ์ด หรือสมาร์ทการ์ด

รูปที่ 2.3 ขั้นตอนของการเก็บหลักฐานทางชีวภาพ

ในขั้นตอนของการเก็บหลักฐานทางชีวภาพ จากตัวอย่างของรูปที่ 2.4 ในขั้นแรกระบบจะทำการเก็บภาพของเรตินาจากบุคคลที่ถือ โทเค็นการ์ด หรือสมาร์ทการ์ด จากนั้นจะนำภาพเรตินาที่ได้มาแยกแยะเพื่อหาลักษณะเด่นของแต่ละบุคคลเพื่อไม่ให้ซ้ำกับบุคคลอื่น แล้วเก็บไว้เป็น แม่แบบ ซึ่ง แม่แบบ ที่ได้จะถูกบันทึกเป็นกุญแจคู่กับรหัสผ่านที่มีอยู่ใน โทเค็นการ์ด หรือสมาร์ทการ์ดของแต่ละบุคคล



รูปที่ 2.4 ขั้นตอนของการตรวจสอบหลักฐานทางชีวภาพ

ในขั้นตอนของการตรวจสอบหลักฐาน ผู้ใช้ที่ถือ โทเค็นการ์ด หรือสมาร์ทการ์ด จะนำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินา ให้เครื่องเก็บภาพ เมื่อเครื่องอ่านบัตร อ่านค่าเลขที่ได้จากบัตรแล้ว ก็จะนำไปหากุญแจ ซึ่งในขณะเดียวกันภาพเรตินาที่เครื่องเก็บไว้ได้ ก็จะนำไปแยกแยะเพื่อหาลักษณะเด่น แล้วเก็บค่าไว้เป็นแม่แบบ และนำแม่แบบที่ได้ไปตรวจสอบกับแม่แบบ ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าผู้ที่ถือบัตรกับผู้ใช้เป็นคนเดียวกัน จึงอนุญาตให้เข้าสู่ระบบได้

2.1.2.6 การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP)

One-Time Password ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆกัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง ชาเลจน์สตริง(challenge string) กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ ชาเลจน์สตริง และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า ตอบสนอง(response) ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

2.1.2.7 การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography)

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้ จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัสคือ

- กุญแจสาธารณะ (public key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้

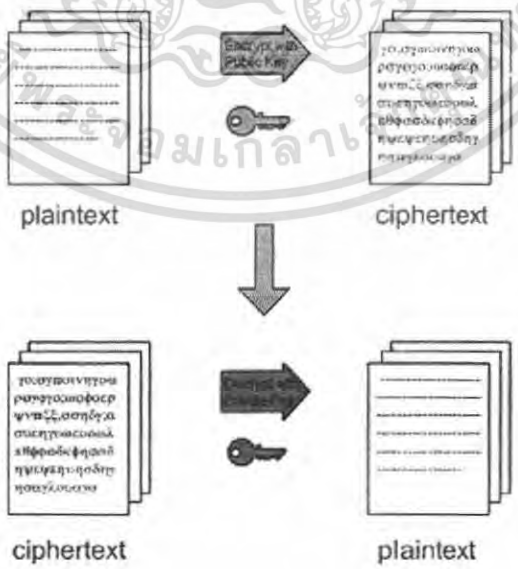
- กุญแจส่วนตัว (private key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

กระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัสกุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะ ก่อนถูกส่งออกไปเมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา

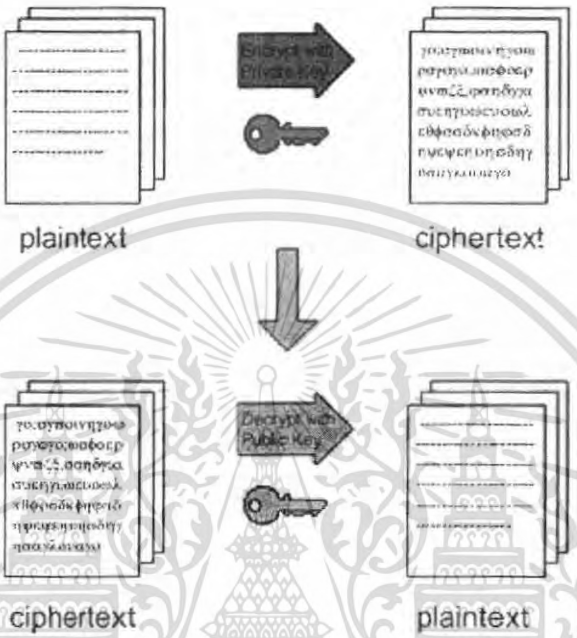
การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส และการพิสูจน์ตัวตน

การประยุกต์ใช้ในการเข้ารหัสข้อมูล เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้



รูปที่ 2.5 ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจ

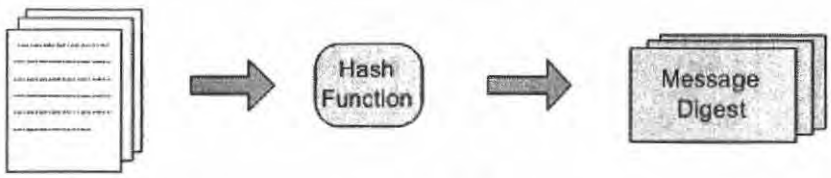
การประยุกต์ใช้ในการพิสูจน์ตัวตน เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง แล้วนำข้อมูลนั้นส่งไปยังผู้รับ ซึ่งผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัสออกมา ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง



รูปที่ 2.6 ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตน

2.1.2.8 การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจ เพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

1. เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชั่นทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" ได้เมสเซส ไดเจสต์ (Message Digest) ออกมา

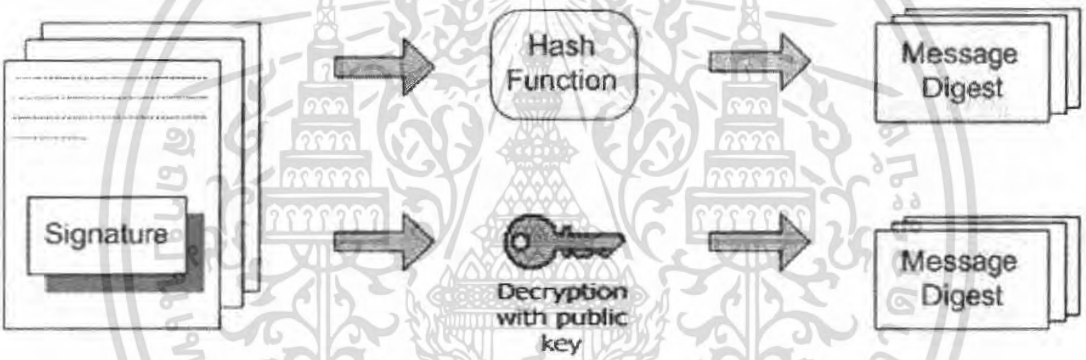


รูปที่ 2.7 การส่งข้อมูลเข้าไปในแฮชฟังก์ชั่น

2. การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

รูปที่ 2.8 การเข้ารหัสเมสเซสไดเจสต์ด้วยกุญแจส่วนตัวเพื่อเป็นการลงลายเซ็น

3. การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และ ถอดรหัสลายเซ็นอิเล็กทรอนิคส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง



รูปที่ 2.9 ขั้นตอนการเปรียบเทียบความถูกต้อง

ลายเซ็นอิเล็กทรอนิคส์นิยมใช้ในระบบรักษาความปลอดภัยในการชำระเงินผ่านระบบอินเตอร์เน็ต ซึ่งในปัจจุบันนี้การทำธุรกรรมการเงินอิเล็กทรอนิกส์ได้รับความนิยมเป็นอย่างมาก

2.1.2.9 การพิสูจน์ตัวตนโดยใช้การถาม - ตอบ (zero-knowledge proofs)

เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม - ตอบ เมื่อผู้ใช้เข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้คนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่างๆมีมากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่าน อาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้

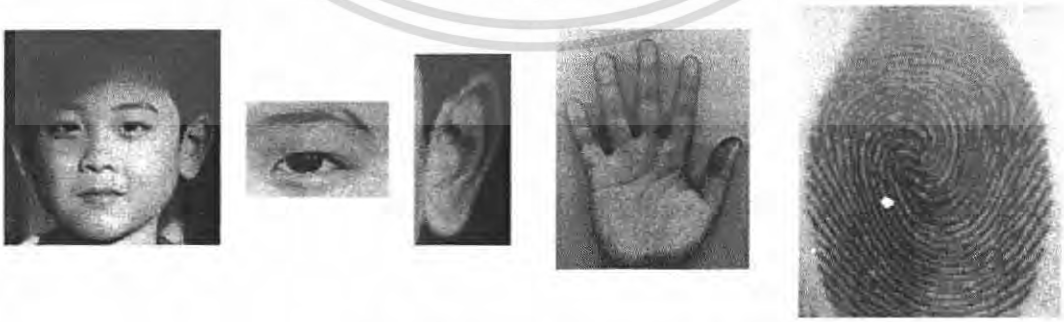
การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริง นั่นก็คือระบบจะใช้การถาม - ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม - คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อผู้ใช้คนนั้นๆเข้าสู่ระบบได้ ระบบจะถามสุ่ม

คำถามเหล่านั้นที่ผู้ใช้คนนั้นๆ สร้างขึ้นมา ถามผู้ใช้คนนั้นๆก่อนที่จะยอมให้เข้าใช้ระบบได้จริง การให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบ นั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ ยกตัวอย่างเช่น นาย ก. กับ นาย ข. รู้จักกันมานานละสนิทกัน นาย ก. และ นาย ข. ย่อมมีความสนิทกันเป็นส่วนตัวเมื่อนาย ก. และนาย ข. เล่น MSN กัน ต่างฝ่ายต่างจะแน่ใจได้อย่างไรว่า คนที่ตนคุยอยู่เป็นบุคคลเดียวกันกับที่ตนรู้จัก เพราะว่านาย ก. หรือ นาย ข. อาจจะทำการเข้าระบบทิ้งไว้ หรือ อาจจะมีบุคคลอื่นสามารถดักจับหลักฐานและข้อมูลที่สามารถเข้าสู่ระบบของคนใดคนหนึ่งไว้ได้ แล้วทำการสวมรอยแทน นั่นก็คือการใช้คำถามและคำตอบที่มีเพียงนาย ก. และนาย ข. เท่านั้นที่ทราบ

วิธีการพิสูจน์ตัวตนวิธีนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้ เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ อาจจะเรียกระบบนี้ได้ว่าเป็นการนำความรู้ด้าน AI (Artificial Intelligence) มาใช้นั่นเอง

2.2 ไบโอเมตริกซ์ (Biometrics)

ไบโอเมตริกซ์ หรือ ไบโอเมทรี (Biometry) เป็นศาสตร์ด้านหนึ่งในการนำเอาวิธีการทางคณิตศาสตร์ หรือวิธีการทางสถิติ มาใช้ในการวิเคราะห์แก้ไขปัญหาทางด้านชีววิทยาต่างๆ เช่น การใช้วิธีทางสถิติวิเคราะห์ผลกระทบของมลพิษที่มีผลต่อสุขภาพของบุคคล, การวิเคราะห์ข้อมูลสภาพอากาศที่มีผลต่อการเพาะปลูก เป็นต้น และไบโอเมตริกซ์ก็ยังมีอีกความหมายหนึ่งคือ เป็นศาสตร์ที่เกี่ยวข้องกับการใช้กระบวนการ ในการระบุตัวบุคคลหรือ ตรวจสอบตัวบุคคล โดยใช้ลักษณะทางกายภาพที่แตกต่างกันแต่ละบุคคล เช่น รูปแบบของลายนิ้วมือ (Fingerprint) , รูปลักษณ์ของมือ (Hand Geometry) , ลักษณะของเรตินา (Retina Pattern) , ลักษณะของม่านตา (Iris Pattern) , รูปลักษณ์ใบหน้า (Facial) หรือใช้ลักษณะทางพฤติกรรมของแต่ละบุคคล เช่น เสียง (Voice) , เอกลักษณ์ในการพิมพ์ (Keystroke Dynamics) , ลักษณะท่าทางในการเดิน (Gait recognition) เป็นต้น



รูปที่ 2.10 ลักษณะทางกายภาพของมนุษย์

2.2.1 ประเภทของไบโอเมตริกซ์

ไบโอเมตริกซ์สามารถแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือ การใช้ลักษณะทางกายภาพ (Physiological Biometrics) และการใช้ลักษณะทางพฤติกรรม (Behavioural Biometrics) ในการระบุตัวบุคคล

2.2.1.1 ลักษณะทางกายภาพ (Physiological Biometrics)

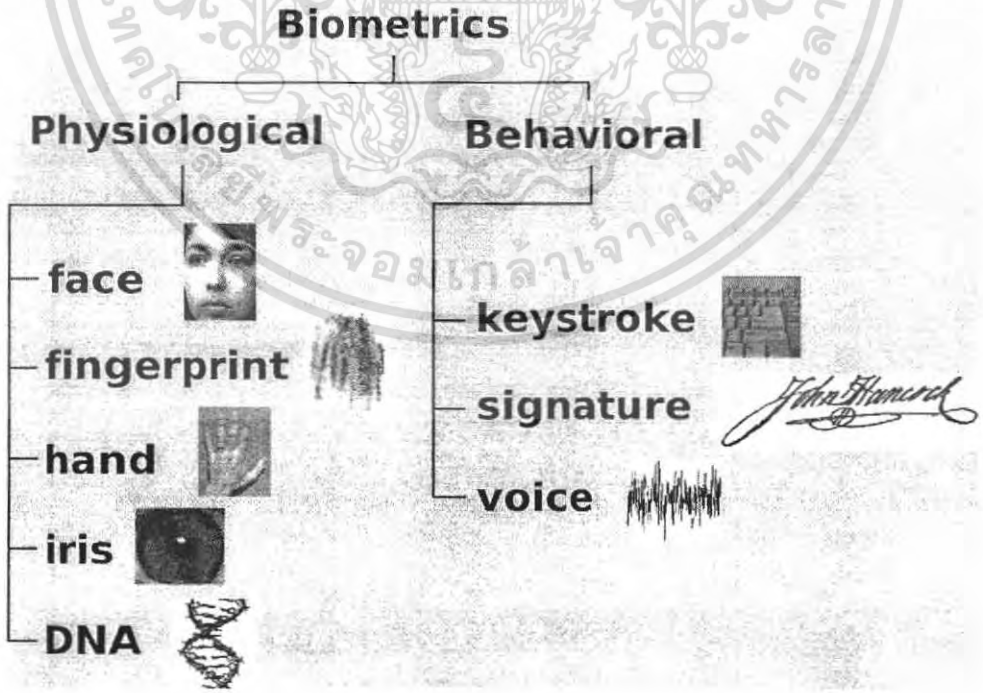
ลักษณะทางกายภาพ เป็นสิ่งที่ติดตัวมนุษย์มาตั้งแต่เกิด เช่น

- ลายนิ้วมือ
- ลักษณะของร่างกายต่างๆ เช่น ใบหน้า, รูปร่างมือ, ลักษณะของใบหู
- ไอรีส และ เรตินา ภายในดวงตา
- กลิ่นของร่างกาย
- ลักษณะทางพันธุกรรม (DNA)

2.2.1.2 ลักษณะทางพฤติกรรม (Behavioural Biometrics)

ลักษณะทางพฤติกรรม เป็นความเคยชิน หรือเป็นสิ่งที่มนุษย์ทำอยู่เป็นประจำ เช่น

- เอกลักษณ์ในการพิมพ์
- ลักษณะท่าทางในการเดิน
- เสียงพูด
- ลายมือชื่อ หรือการเซ็นชื่อ



รูปที่ 2.11 ประเภทของไบโอเมตริกซ์

กระบวนการในการตรวจสอบ หรือ ระบุบุคคลด้วยไบโอเมตริกซ์ไม่ว่าจะเป็นการใช้ลักษณะเฉพาะแบบใดก็ตาม จะมีขั้นตอนเหมือนๆ กันดังต่อไปนี้

ผู้ใช้ระบบต้องทำการให้ตัวอย่าง (Samples) ของลักษณะทางไบโอเมตริกซ์ ที่จะใช้ หรือเป็นการลงทะเบียนเริ่มต้นก่อนที่จะทำการใช้ระบบ ตัวอย่างทางไบโอเมตริกซ์ที่ถูกเก็บมาในขั้นตอนแรก จะถูกทำการแปลงและจัดเก็บให้เป็นแม่แบบ(Template) ที่จะใช้ในการเปรียบเทียบเมื่อผู้ใช้ต้องการที่จะใช้ระบบก็จะถูกตรวจสอบหรือระบุผู้ใช้ โดยทำการเก็บตัวอย่างทางไบโอเมตริกซ์ ของผู้ใช้และทำการเปรียบเทียบกับ แม่แบบที่เก็บไว้ แล้วทำการตรวจสอบความเหมือนกันของตัวอย่างกับแม่แบบ จากนั้นก็จะทำการอนุญาต หรือปฏิเสธ การเข้ามาใช้งานระบบของผู้ใช้ เราเรียกขั้นตอนที่ 1 และ 2 ว่าเป็นขั้นตอนของการลงทะเบียน (Enrollment) ซึ่งจะเป็นการทำเพียงครั้งเดียว ก่อนการที่จะเริ่มใช้งาน ส่วนขั้นตอนที่ 3 เป็นกระบวนการตรวจสอบ (Authentication) หรือระบุตัวผู้ใช้ (Identification) ซึ่งผลของการตรวจสอบหรือระบุตัวผู้ใช้นี้มีผลออกมาได้ 4 กรณีดังนี้

- **Correct Accept**: อนุญาตให้ผู้ใช้ที่มีสิทธิใช้ระบบ เข้าใช้ระบบ
- **Correct Reject**: ปฏิเสธผู้ที่ไม่มีสิทธิใช้ระบบ ไม่ให้เข้าใช้ระบบ
- **False Accept**: อนุญาตให้ผู้ที่ไม่มีสิทธิใช้ระบบ เข้าใช้ระบบ จำนวนของ False Accept ถ้าคำนวณออกมาเป็นเปอร์เซนต์ จะเรียกว่า อัตราการอนุญาตผิดพลาด (False Accept Rate หรือ FAR)
- **False Reject** : ปฏิเสธผู้ใช้ที่มีสิทธิใช้ระบบ ไม่ให้เข้าใช้ระบบ จำนวนของ False Reject ถ้าคำนวณออกมาเป็นเปอร์เซนต์ จะเรียกว่า อัตราการปฏิเสธผิดพลาด (False Reject Rate หรือ FRR)

2.2.2 ข้อเปรียบเทียบเทคโนโลยีไบโอเมตริกซ์แต่ละประเภท

โดยเปรียบเทียบไบโอเมตริกซ์แต่ละประเภท ตามหัวข้อต่างๆ ดังนี้

- ความแพร่หลายในการใช้งาน(Universality)
- ความเป็นเอกลักษณ์ มีลักษณะเฉพาะ (Uniqueness)
- ความคงทนของเอกลักษณ์ (Permanence)
- ความง่ายของการเก็บข้อมูล (Collect ability)
- สมรรถนะของเทคโนโลยี (Performance)
- ระดับการรับรอง (Acceptability)
- ความง่ายต่อการนำมาใช้ (Circumvention)

ตารางที่ 2.1 ตารางแสดงการเปรียบเทียบตัวแปลทางไบโอเมตริกซ์

Comparison of various biometric technologies, according to A. K. Jain[2] (H=High, M=Medium, L=Low)

Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

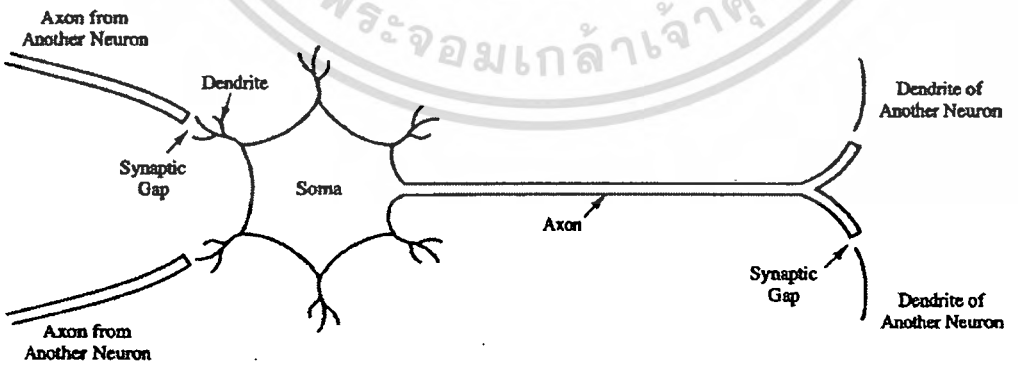
บทที่ 3
โครงข่ายประสาทเทียม

โครงข่ายประสาทเทียม (Artificial Neural Network)

โครงข่ายประสาทเทียม คือแบบจำลองทางคณิตศาสตร์สำหรับประมวลผลสารสนเทศ โดยจำลองการทำงานของระบบเครือข่ายประสาทในสมองของมนุษย์ นำมาพัฒนาให้คอมพิวเตอร์มีความสามารถในการเรียนรู้(Learning) การจดจำรูปแบบ (Pattern Recognition) และการอุปมานความรู้ (Knowledge deduction) เช่นเดียว กับความสามารถที่มีในสมองมนุษย์

3.1 ระบบเครือข่ายประสาทในสมองของมนุษย์ทำงานอย่างไร

สมองมนุษย์ประกอบด้วยเซลล์สมองที่เรียกว่า นิวรอล(Neuron) นับล้านๆ เซลล์ เชื่อมกันเป็นเครือข่าย โดยแต่ละเซลล์ประกอบด้วยปลายในการรับกระแสประสาท เรียกว่า "เดนไดรท์" (Dendrite) ซึ่งเป็นเสมือนอินพุต(Input) และปลายในการส่งกระแสประสาทเรียกว่า "แอคซอน" (Axon) ซึ่งเป็นเสมือนเอาท์พุต(output) ของเซลล์ เซลล์เหล่านี้ทำงานด้วยปฏิกิริยาไฟฟ้าเคมี เมื่อมีการกระตุ้นด้วยสิ่งเร้าภายนอก หรือกระตุ้นด้วยเซลล์ด้วยกัน กระแสประสาทจะวิ่งผ่านเดนไดรท์เข้าสู่นิวเคลียส ซึ่งจะเป็นตัวตัดสินว่าต้องกระตุ้นเซลล์อื่นๆ ต่อหรือไม่ ถ้ากระแสประสาทแรงพอนิวเคลียสก็จะกระตุ้นเซลล์อื่นๆ ต่อไปผ่านทางแอคซอนของมัน นักวิทยาศาสตร์เชื่อกันว่าผลการกระตุ้นด้วยสิ่งเร้าที่เหมือนหรือมีลักษณะพิเศษบางอย่างเหมือนกัน จะให้ผลลัพธ์สุดท้ายเป็นค่าที่ค่อนข้างแน่นอน เราจึงสามารถรู้จำ และแยกแยะสิ่งต่างๆ ได้

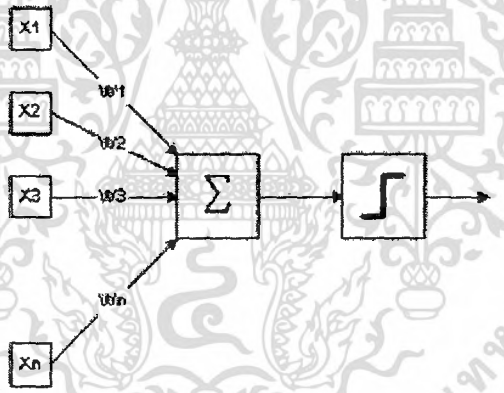


รูปที่ 3.1 นิวรอลในสมองของมนุษย์

การออกแบบสร้างโครงข่ายประสาทเทียมนั้นมีสมมติฐานขั้นแรกจากคุณสมบัติของระบบประสาทชีวภาพ ดังที่กล่าวมา กล่าวคือ ชุดรับสัญญาณข้อมูล อินพุทของเซลล์ประสาทหนึ่งได้จาก

สัญญาณเอาท์พุทของเซลล์ประสาทอื่นๆ ผ่านทางจุดประสานประสาทและเดนไดรท์ ข้อมูลแต่ละค่าที่รับมาจะถูกลดขนาดด้วยจุดประสานประสาท ซึ่งภายในประกอบด้วยสารเคมีประเภท K^{+}, Ca^{++}, Na^{+}, Cl^{-} ซึ่งจะมีลักษณะทางความนำพัลส์ (Pulse) สัญญาณไฟฟ้าเคมีที่แตกต่างกันด้วยเหตุนี้โมดุลโครงข่ายประสาทเทียมที่สร้างขึ้น จะต้องมีการถ่วงน้ำหนักให้กับโมดุลก่อนที่จะนำเข้าสู่โมดุลประสาทเทียม จุดนี้เรียกว่า ซินแนปติกส์เวจท์(Synapstic weight) ปริมาณของข้อมูลที่เข้าสู่นิวรอลจะถูกนำมารวมกัน และตัดสินใจด้วยระดับความสนใจของนิวรอล (Activation level) แล้วจะส่งเป็นเอาท์พุทออกที่แอกซอนไปยังนิวรอลอื่นๆ

โครงข่ายประสาทเทียมมีโครงสร้างแตกต่างจากข่ายงานในสมอง แต่ก็ยังเหมือนสมอง ในแง่ที่ว่าโครงข่ายงานประสาทเทียม การรวมกลุ่มแบบขนานของหน่วยประมวลผลย่อย ๆ และการเชื่อมต่อนี้เป็นส่วนสำคัญที่ทำให้เกิดสติปัญญาของข่ายงาน เมื่อพิจารณาขนาดแล้วสมองมีขนาดใหญ่กว่าข่ายงานประสาทเทียมอย่างมาก รวมทั้งเซลล์ประสาทยังมีความซับซ้อนกว่าหน่วยย่อยของข่ายงาน อย่างไรก็ดีหน้าที่สำคัญของสมอง เช่น การเรียนรู้ยังคงสามารถถูกจำลองขึ้นอย่างง่ายด้วยโครงข่ายประสาทนี้



รูปที่ 3.2 ไดอะแกรมของนิวรอล

จากภาพแสดงถึงโมดุลที่สร้างขึ้นโดยแนวความคิดจากเซลล์สมองชีวภาพ สัญญาณอินพุท คือ $X_1, X_2, \ldots, X_n$ จะถูกป้อนเข้าไปยังนิวรอลที่สร้างขึ้น ซึ่งเปรียบเทียบได้กับสัญญาณที่ป้อนเข้ายังซินแนปส์ของนิวรอลชีวภาพ สัญญาณอินพุทนี้จะนำไปคูณกับค่าซินแนปติกส์เวจท์ที่มีค่าตั้งแต่ 0-1 $W_1, W_2, \ldots, W_n$ ก่อนที่จะเข้าสู่บล็อกซัมเมชั่น ซึ่งค่าถ่วงน้ำหนักนี้จะสอดคล้องกับค่าสเตรงท์ (Strength) ของจุดต่อซินแนปส์ชีวภาพแต่ละจุด (Single biological synaptic connection)

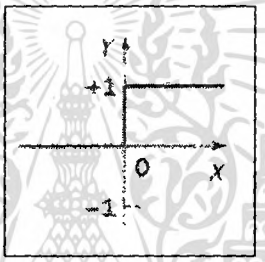
บล็อคซัมเมชั่นนี้ก็จะทำหน้าที่สอดคล้องคล้ายกับตัวเซลล์สมองชีวภาพ ผลรวมทางคณิตศาสตร์ของอินพุตและเวจท์จะได้เป็นเอาท์พุท เราเรียกว่าเน็ต (NET) ซึ่งเราจะรวมกันในรูปของเวกเตอร์ได้ดังนี้

$$NET = X_1 W_1 + X_2 W_2 + \ldots + X_n W_n \tag{3.1}$$

3.2 ฟังก์ชั่นกระตุ้นความสนใจ (Activation Function)

เมื่อได้สัญญาณ NET แล้วกระบวนการต่อมาที่นิวรอลต้องทำคือตัดสินใจ เราจึงต้องกำหนดฟังค์ชันการตัดสินใจ เพื่อใช้เป็นระดับของการตัดสินใจให้กับนิวรอล เพื่อให้ได้สัญญาณเอาท์พุทของนิวรอลออกมา ซึ่งเชื่อมต่อไปยังนิวรอลตัวอื่นๆ เป็นโครงข่าย OUT

3.2.1 สเตปฟังค์ชัน (Step function)



รูปที่ 3.3 กราฟที่ได้จากฟังก์ชั่นสเตปฟังก์ชั่น

สเตปฟังค์ชัน หรือลีเนียร์เทรชโฮลฟังค์ชั่น(linear threshold function) นั้นจะนำสัญญาณที่เข้ามาคูณกับค่าถ่วงน้ำหนัก (Weight) ค่าผลรวมจะมาเทียบกับค่าเทรชโฮล หากผลรวมมากกว่าค่าเทรชโฮลแล้วค่าระดับความสนใจของนิวรอลเท่ากับ +1 ถ้าค่าน้อยกว่าเทรชโฮลนั้นค่าระดับความสนใจของนิวรอลจะเป็น -1 (อาจแทนด้วย 0 ในบางระบบ)

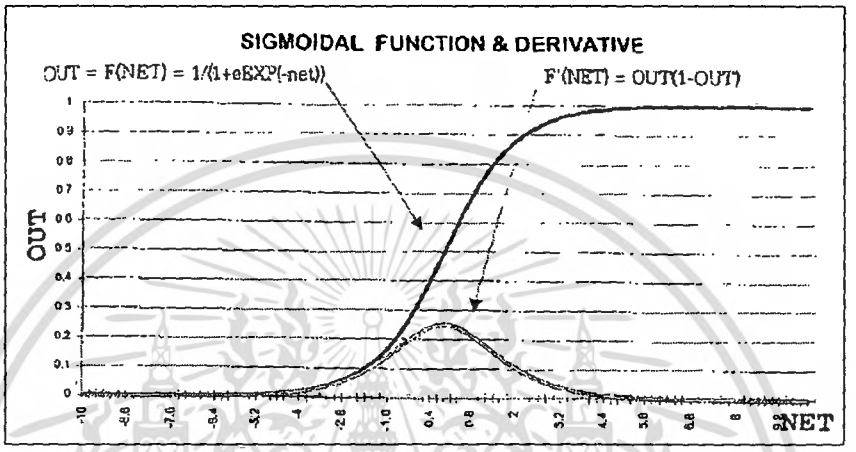
$$X = \sum_{i=1}^{n} w_i x_i \tag{3.2}$$

โดย X เป็นค่าผลรวมระหว่างค่าถ่วงน้ำหนักกับอินพุต

$$Y = \begin{cases} +1 \; for \; X > t \\ 0 \; for \; X \le t \end{cases} \tag{3.3}$$

โดย Y เป็นค่าระดับความสนใจของนิวรอล และ t เป็นค่าเทรชโฮลดงที่ หรืออาจเป็นฟังค์ชันอื่นๆ ที่เลียนแบบคุณสมบัติที่ไม่เป็นเชิงเส้นของเซลล์ประสาทชีวภาพได้อย่างใกล้เคียงกว่า และใช้เป็นฟังค์ชันให้กับโครงข่ายทั่วไปได้

3.2.2 ซิกมอยด์ฟังค์ชัน (Sigmoid function)



รูปที่ 3.4 กราฟที่ได้จากฟังก์ชั่นซิกมอยด์ฟังก์ชั่น

ลักษณะของเทรชโฮลฟังค์ชันมีลักษณะเป็นนอลลีเนียร์ฟังค์ชัน (Non-linear function) เช่น เอสเคิร์ฟว (S-Curve) เราจะได้ค่าเอาท์พุทที่มีความไวต่อสัญญาณอินพุทที่มีขนาดเล็กๆ และเฉลี่ยต่อสัญญาณแรงๆ ซึ่งสัญญาณอ่อนๆไปทางบวกเพียงเล็กน้อยก็จะให้ผลใกล้เคียง "1" กระตุ้นหรือสัญญาณอ่อนๆ ทางลบเพียงเล็กน้อยก็จะทำให้ผลใกล้เคียง "0" (ยับยั้ง) ขณะที่สัญญาณแรงๆ ทางบวกก็ยังคงให้ผลใกล้เคียง "1" และสัญญาณทางลบแรงๆ ก็ยังคงให้ผลใกล้เคียง "0" เช่นกัน 00 จะมีอัตราขยายแบบนอลลีเนียร์ (non- linear gain) ซึ่งคุณลักษณะแบบนี้สามารถแก้ปัญหานอยซแซซทูเรชันดิเลมมา (Noise-saturation dilemma) ได้ และทำให้นิวรอลเทียมที่สร้างขึ้นสามารถทำงานกับขนาดของอินพุทได้กว้างมากขึ้น โดยครอบคลุมอินพุตในช่วง - ∞ ถึง + ∞

โดยฟังค์ชันของซิกมอยด์ฟังค์ชันคือ $$\sigma(x) = \frac{1}{1+e^{-x}} \qquad (3.4)$$

3.3 การฝึกสอนให้แก่โครงข่ายประสาทเทียม(Training of Artificial Neural Networks)

ค่าถ่วงน้ำหนัก มีความสัมพันธ์กับอะไร? เปลี่ยนแปลงอย่างไร? นั้นก็เช่นเดียวกับเด็กที่คลอดออกมาก็มีสมองแล้วแต่สมองยังไม่เจริญเติบโตเพียงพอ และยังไม่ได้รับการฝึกสอน และเรียนรู้ เด็กจึงไม่สามารถทำกิจกรรมใดๆด้วยตนเอง เว้นแต่กิจกรรมที่ธรรมชาติสร้างมาพร้อมกับการกำเนิดที่เรียกว่า "สัญชาติญาณ" ซึ่งธรรมชาติใส่คุณลักษณะบางอย่างให้เซลล์สมองบางส่วนตั้งแต่ทารก เจริญเติบโตอยู่ในครรภ์มารดา เช่น ระบบควบคุมการหายใจ, ความรู้สึก, การเรียกร้องเมื่อหิว, การตอบสนองต่อสิ่งเร้า ฯลฯ เด็กจะพัฒนาการเรียนรู้ไปตามขั้นตอน หลังจากนั้นสมองของเขาจะได้รับการฝึกสอน และเจริญเติบโตไปพร้อมๆกัน เซลล์สมองจะได้รับการปรับคุณลักษณะสอดคล้องกับการฝึกสอน และจะเจริญเป็นโครงข่ายสอดคล้องกัน

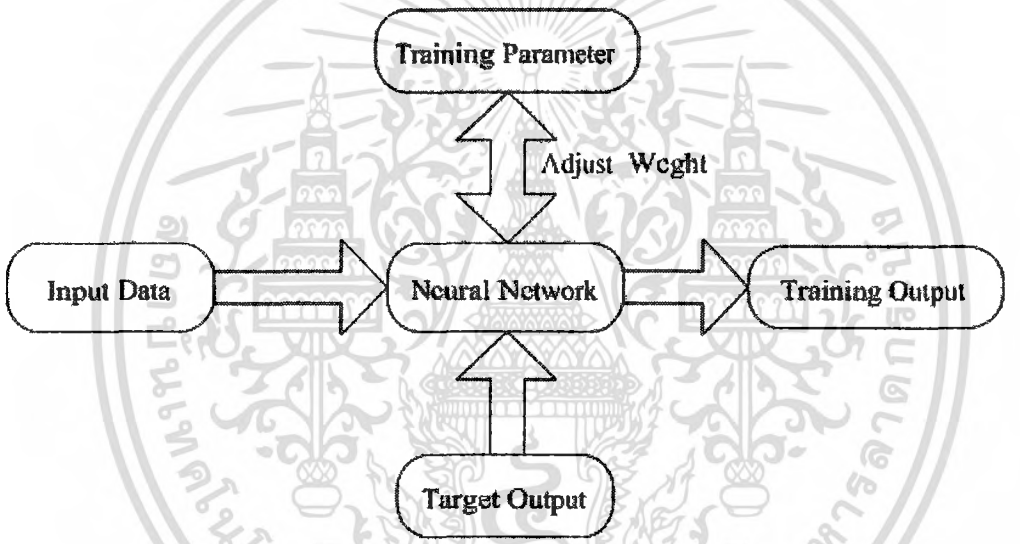
โครงข่ายประสาทเทียมที่สร้างขึ้นมีลักษณะเช่นเดียวกัน คือ เมื่อสร้างเสร็จ แต่ละเซลล์ประสาทที่สร้างขึ้นมานั้น จะยังไม่มีคุณลักษณะใดเลย เนื่องจากยังไม่มีการกำหนดค่าซินแนปติกส์เวจท์ที่เหมาะสมกับงานที่ต้องการให้กับมัน จึงต้องมีการฝึกสอนเพื่อให้โครงข่ายที่สร้างขึ้นมีคุณลักษณะตามที่ต้องการ การฝึกสอนของโครงข่ายประสาทเทียม จะกระทำโดยการปรับเปลี่ยนค่าซินแนปติกส์เวจท์เพื่อให้โครงข่ายจดจำรูปแบบความสัมพันธ์ระหว่างอินพุทกับเอาท์พุทได้ โดยในขั้นแรกกำหนดเป็นค่าสุ่มใดๆ (Random weight) ก่อนแล้วถึงปรับเปลี่ยนค่าถ่วงน้ำหนักไปตามอัลกอริทึมสมมติฐานหลายๆรอบจนกว่าจะได้ผลลัพธ์ของโครงข่าย เหมือนกับผลลัพธ์ที่ต้องการในเงื่อนไขความผิดพลาดที่ยอมรับได้

3.4 วัตถุประสงค์ของการฝึกฝน (Objective of Training)

เนื่องจากค่าถ่วงน้ำหนักที่ให้เป็นค่าสุ่มใดๆ โครงข่ายจึงไม่แสดงคุณลักษณะใดออกมาการฝึกสอน (Training) ให้โครงข่ายก็คือการปรับค่าค่าถ่วงน้ำหนักทุกๆจุดให้สอดคล้องกับอินพุทหลายๆแบบ เพื่อให้ได้เอาท์พุทตามต้องการนั่นเอง การฝึกสอนโครงข่าย จะต้องบรรลุถึงกระบวนการเข้าใจพื้นฐานเสียก่อน คือการเรียนรู้ในโครงข่ายประสาทเทียมนั้นมีขีดจำกัด ปัญหาต่างๆ ผู้ใช้คงต้องแก้ไขให้มันก่อน แล้วนำผลนั้นไปอ้างอิงสำหรับการปรับปรุงค่าค่าถ่วงน้ำหนัก หลังจากปรับค่าถ่วงน้ำหนักจนได้ค่าผิดพลาดที่เอาท์พุทเทียบกับเป้าหมายน้อยลงเป็นที่พอใจแล้ว โครงข่ายประสาทเทียมนั้นก็พร้อมที่จะวิเคราะห์อินพุทและให้เอาท์พุทตามลักษณะตัวอย่างที่มันเคยเรียนรู้มาการเรียนรู้จะมีการปรับค่าถ่วงน้ำหนักหลายๆรอบ จนค่าถ่วงน้ำหนักสอดคล้องกับตัวอย่างหลายๆตัวอย่าง และให้เอาท์พุทตามต้องการ พบว่าโครงข่ายได้ตัวอย่างสำหรับการฝึกฝนมากๆ โครงข่ายก็จะมีความแม่นยำสูงขึ้น แต่ก็จะใช้เวลาในการฝึกฝนเพิ่มขึ้นเช่นกัน หากพิจารณาต่อไปจะพบว่า โครงข่ายประสาทเทียมที่สร้างขึ้นจะมีพฤติกรรมคล้ายกับระบบการเรียนรู้ของมนุษย์มากเป็นเพราะมีต้นแบบมาจากระบบประสาทชีวภาพนั่นเอง

3.4.1 การฝึกฝนแบบควบคุม (Supervised Training)

วิธีการฝึกฝนถูกจัดเป็น 2 ประเภท คือ แบบควบคุม และแบบอิสระ (Unsupervised training) โดย การฝึกฝนแบบควบคุม จะต้องการคู่ของการฝึกฝนระหว่างอินพุทกับเป้าหมายที่ต้องการที่เรียกว่า คู่การฝึกฝน (Training pairs) โครงข่ายจะถูกเทรนไปตามจำนวนของคู่ที่ฝึกฝน (จำนวนคู่ของอินพุทกับเอาท์พุทที่ต้องการให้โครงข่ายรู้จัก) เอาท์พุทที่คำนวณได้จากโครงข่ายจะถูกเปรียบเทียบกับความสอดคล้องกับเป้าหมาย ค่าผิดพลาดที่เกิดขึ้นจะถูกป้อนกลับไปยังโครงข่ายและเปลี่ยนแปลงค่าถ่วงน้ำหนักให้สอดคล้องกับวิธีการ ที่ทำให้แนวโน้มของค่าผิดพลาดที่เกิดขึ้นระหว่างผลลัพธ์กับเป้าหมายโดยเฉลี่ยมีค่าลดต่ำลง ตัวอย่างการฝึกฝนแบบนี้ ได้แก่ การฝึกฝนแบบแพร่กลับ (Back-propagation) ซึ่งการฝึกฝนแบบควบคุมนั้นจะต้องทำการฝึกฝนโครงข่ายก่อนที่จะนำข้อมูลที่ไม่เคยจำแนกในโครงข่าย



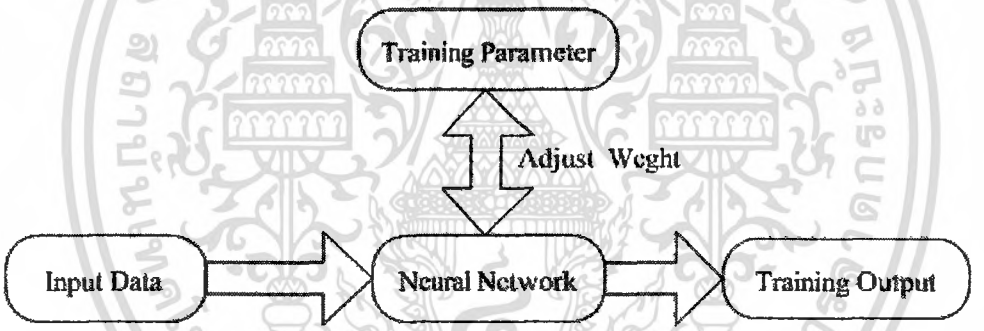
รูปที่ 3.5 แผนผังการฝึกฝนโครงข่ายแบบควบคุม

3.4.2 การฝึกฝนแบบอิสระ

ถึงแม้ว่าวิธีการแบบควบคุมสามารถจะประยุกต์ใช้เพื่อปรับคุณลักษณะของโครงข่ายได้สำเร็จ แต่ก็ยังมีข้อวิจารณ์อยู่ คือ มันเป็นไปอย่างชีวภาพไม่ได้ และยากที่จะเชื่อได้ว่า กลไกการฝึกฝนของสมองจะต้องการ การเปรียบเทียบระหว่างค่าที่ต้องการกับผลลัพธ์จริง โดยกระบวนการป้อนกลับไปแก้ไขคุณลักษณะของโครงข่าย และถ้าสมมติว่า ถ้าสมองมีกลไกเช่นนี้ ต้องมีผู้หาผลลัพธ์ที่ต้องการเพื่อนำมาเป็นเป้าหมายตลอดเวลา และจะเอามาจากที่ใดสรุปคือ ต้องมีผู้คิดเป้าหมายให้กับโครงข่ายก่อน โครงข่ายไม่สามารถคิดและปรับคุณลักษณะได้ก่อนด้วยตนเอง ในทางตรงกันข้ามหากพิจารณาทารกแรกเกิดสมองของเขาสามารถจัดระบบเองได้อย่างไร

การฝึกฝนแบบอิสระที่สร้างขึ้นคงยังห่างไกลความเป็นไปได้ ที่จะมีลักษณะการฝึกฝนแบบระบบของสมอง จนกระทั่งมีการพัฒนาการฝึกฝนแบบอิสระนี้ขึ้นปี 1984 ได้เสนอแนวคิดที่เป็นการฝึกฝนแบบไม่ต้องการเป้าหมายไม่มีการตัดสินใจด้วยเหตุผลในอุดมคติมาก่อน

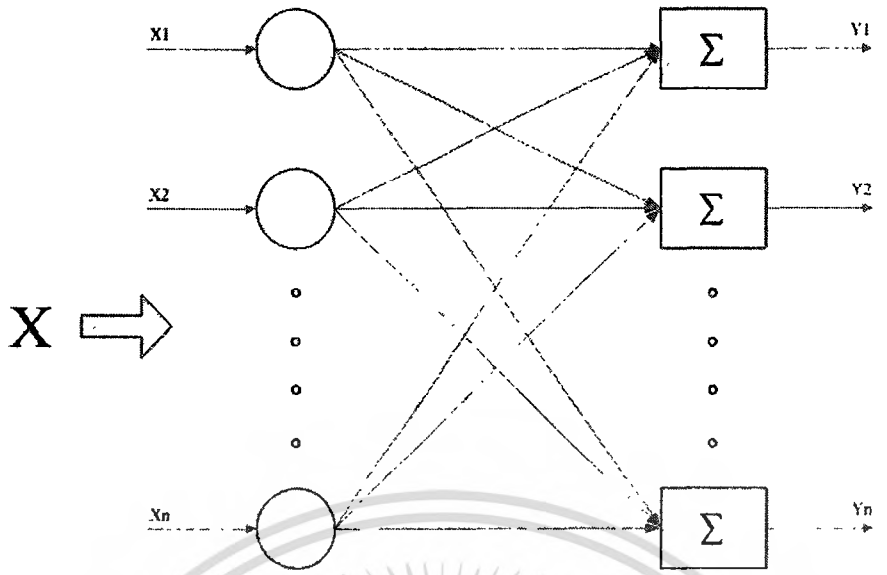
ชุดข้อมูลของการฝึกฝน จะมีเพียงอินพุทเวกเตอร์เท่านั้น ฝึกฝนอัลกอริทึมจะเปลี่ยนแปลงค่าถ่วงน้ำหนักของโครงข่าย เพื่อสร้างเอาท์พุทที่มีความคงที่ ยกตัวอย่างเช่น หากให้โครงข่ายรู้จำภาพหน้าคนหนึ่ง หากภาพหน้าคนคนนั้นเปลี่ยนแปลงไปเล็กน้อย (ภาพอาจมีสัญญาณรบกวนรวมอยู่บ้าง) โครงข่ายนั้นก็ยังสามารถบอกได้ว่าคนคนนั้นเป็นคนเดิม เป็นต้น การฝึกฝนจะไม่มีการตัดสินใจมาก่อน ไม่มีการกำหนดแบบเอาท์พุทมาก่อน (อาจกล่าวได้ว่าแบบเอาท์พุทจะถูกกำหนดโดยอินพุทเวกเตอร์นั่นเอง) ดังนั้น เอาท์พุทของโครงข่ายก็เช่นกัน ส่วนใหญ่จะถูกแปรรูปซึ่งจะเข้าใจได้ภายหลังกระบวนการฝึกฝน ดังนั้นจึงไม่สามารถแก้ปัญหาที่เคร่งครัดสำคัญได้ แต่มักนิยมใช้โครงข่ายแบบนี้กับงานง่ายๆ ประเภทการเปรียบเทียบเอกลักษณ์ รูปแบบที่สัมพันธ์กันระหว่างอินพุท-เอาท์พุท ที่ถูกกำหนดโดยโครงข่าย



รูปที่ 3.6 แผนผังการฝึกฝนเครือข่ายแบบอิสระ

3.5 โครงข่ายประสาทเทียมแบบชั้นเดียว (Single Layer Artificial Neural Networks)

ที่กล่าวมาจะถึงจุดนี้ เป็นการกล่าวถึงหลักการและเหตุผลในการสร้างเซลล์ประสาทเทียมเพียงหนึ่งเซลล์ โดยใช้แนวความคิดจากเซลล์ประสาทชีวภาพ การจะนำเซลล์ประสาทเทียมมาใช้งานได้นั้นต้องใช้เซลล์ประสาทเทียมที่มีคุณลักษณะต่างๆกัน (ค่าถ่วงน้ำหนักจะทำให้คุณสมบัติของเซลล์ประสาทเทียมแต่ละเซลล์มีคุณลักษณะแตกต่างกันไป) มาเชื่อมโยงเป็นโครงข่ายในลักษณะเดียวกับเซลล์สมองชีวภาพเสียก่อน ซึ่งลักษณะการเชื่อมโยงมีหลายชนิด แต่ละชนิดก็มีคุณลักษณะเด่นที่แตกต่างกันไป

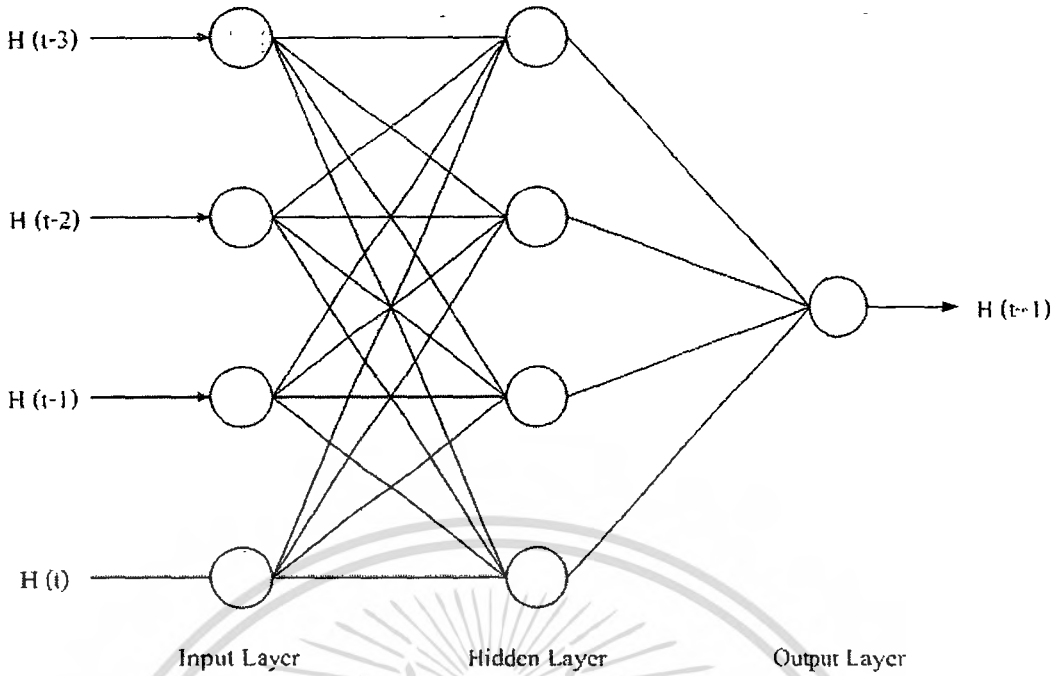


รูปที่ 3.7 ลักษณะโครงข่ายประสาทเทียมแบบชั้นเดียว (Single-Layer Neural Networks)

จากรูป เป็นโครงข่ายประสาทเทียมแบบชั้นเดียว ที่ประกอบด้วยเซลล์ประสาทเทียมง่ายๆ หลายชุด ความสามารถในการคำนวณของโครงข่ายประสาทเทียมได้มาจากลักษณะการเชื่อมต่อเป็นโครงข่ายประสาทเทียม โครงข่ายง่ายๆเป็นกลุ่มโมดุลประสาทเทียมที่เชื่อมต่อกันเป็นชั้นๆ (Layer) อย่างไรก็ดีลักษณะการเชื่อมโยงระหว่างโครงข่ายไม่ได้มีแบบเดียว การเชื่อมโยงระหว่างชั้นอาจมีการเชื่อมโยงย้อนกลับมาที่ชั้นอินพุทอีก ซึ่งโครงข่ายประสาทชีวภาพก็มีลักษณะดังกล่าวเช่นกัน สำหรับค่าน้ำหนัก มีวิธีการพิจารณาในรูปของ เวจท์เมตริก (Weight matrix) ซึ่งหากโครงข่ายมีหลายชั้น จะช่วยให้ระบุค่าถ่วงน้ำหนักได้ง่ายขึ้น และเพื่อหลีกเลี่ยงความสับสนจะกำหนดเป็นมิติ (dimensions) ของเมตริก โดยให้ m แทนจำนวนแถว หรือจำนวนของอินพุท และ n แทน จำนวนของนิวรอล ที่สร้างขึ้น ตัวอย่างเช่น ค่าถ่วงน้ำหนักที่เชื่อมระหว่างอินพุทตัวที่ 4 กับนิวรอลตัวที่ 2 คือ $W_{4,2}$

3.6 โครงข่ายประสาทเทียมแบบหลายชั้น (Multilayer Artificial Neural Networks)

โครงข่ายที่ซับซ้อนจะมีความสามารถในการคำนวณที่ดีขึ้นมันจะเป็นโครงข่ายที่มีโครงสร้างเป็นจินตนาการที่น่าเป็นไปได้โดยการจัดการเชื่อมโยงนิวรอลมีโครงสร้างเป็นชั้นๆ คล้ายส่วนหนึ่งของสมองและมีการพัฒนาวิธีการเกี่ยวกับการฝึกสอนให้โครงข่ายแบบหลายชั้นทำงานได้ ตามความต้องการแล้วเมื่อไม่นานมานี้โครงข่ายแบบหลายชั้นอาจจะสร้างจากกลุ่มของโครงข่ายแบบชั้นเดียวเอาท์พุทของชั้นหนึ่ง จะใช้เป็นอินพุทของชั้นถัดไป

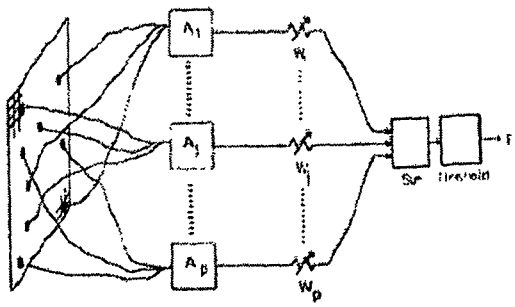


รูปที่ 3.8 แผนภาพของโครงข่ายแบบฟีดฟอร์เวิร์ด (feed-forward network)

จากภาพเป็น โครงข่ายแบบฟีดฟอร์เวิร์ดโดยชั้นแรกเป็นอินพุตเลเยอร์ (Input layer) แต่ละโหนดในชั้นนี้ได้รับสัญญาณจากภายนอก ซึ่งชั้นนี้อาจไม่ใช่นิวรอลก็ได้ แล้วส่งสัญญาณนี้ไปยังชั้นถัดไปคือ ฮิดดันเลเยอร์ (Hidden layer) ในชั้นนี้ประกอบด้วยนิวรอล สัญญาณที่รับเข้ามาจะถูกส่งไปยังเอาท์พุตเลเยอร์ (Output layer) เพื่อส่งสัญญาณที่ได้ออกไป เมื่อ โครงข่ายแบบฟีดฟอร์เวิร์ดผ่านการฝึกฝนแล้วสถานะจะไม่เปลี่ยนถ้าข้อมูลใหม่เข้ามา กล่าวคือระบบนี้ไม่มีหน่วยความจำ

สาเหตุที่เรียกว่าฟีดฟอร์ดเวิร์ดเนื่องจากข้อมูลที่ได้รับมาจากอินพุตโหนด (Input node) จะถูกส่งไปยังเอาท์พุตโหนด (Output node) โดยไม่มีการส่งข้อมูลบางส่วนของเอาท์พุตโหนด กลับมายังอินพุตโหนดระบบที่มีการส่งข้อมูลบางส่วนของเอาท์พุตโหนดกลับมานั้นเรียกว่า recurrent network

3.7 เพอร์เซ็ปตรอน (Perceptrons)



รูปที่ 3.9 แผนภาพของเพอร์เซ็ปตรอน

เพอร์เซ็ปตรอนเป็นโมเดลแรกของโครงข่ายประสาทเทียมที่เป็นแบบควบคุม (Rosenblatt, 1958) ซึ่งเป็นสามารถแยกข้อมูลที่รับมาแบ่งได้เป็นสองประเภท โดยสามารถนำไปใช้เพื่อจำแนกรูปและในงานจำพวกการรู้จำต่างๆได้

เพอร์เซ็ปตรอนใช้สเตปฟังค์ชัน ถ้าค่าผลลัพธ์เป็น +1 แสดงว่าผลรวมระหว่างการคูณของข้อมูลที่รับมาและค่าถ่วงน้ำหนักมีค่ามากกว่า เทรชโฮล และในทางกลับกันถ้าค่าน้อยกว่าค่าผลลัพธ์จะเป็น -1

ฟังค์ชันของ Step สามารถเขียนได้ดังนี้

$$Step(X) = \begin{cases} +1 \; for \; X > t \\ -1 \; for \; X \le t \end{cases} \tag{3.5}$$

ฟังค์ชันกระตุ้นความสนใจของเพอร์เซ็ปตรอนสามารถเขียนได้ดังนี้

$$Y = Step\left(\sum_{i=0}^{n} w_i x_i\right) \tag{3.6}$$

การสอนเพอร์เซ็ปตรอนนั้นสามารถสังเกตจากผลลัพธ์ที่ได้จากการแบ่งแยก ถ้าผลลัพธ์ไม่ถูกต้องต้องทำการเปลี่ยนแปลงค่าถ่วงน้ำหนักเพื่อทำให้ใกล้กับข้อมูลที่รับมา

$$w_i \longleftarrow w_i + (a \times x_i \times e) \tag{3.7}$$

เมื่อ e คือ ค่าความผิดพลาดของผลลัพธ์

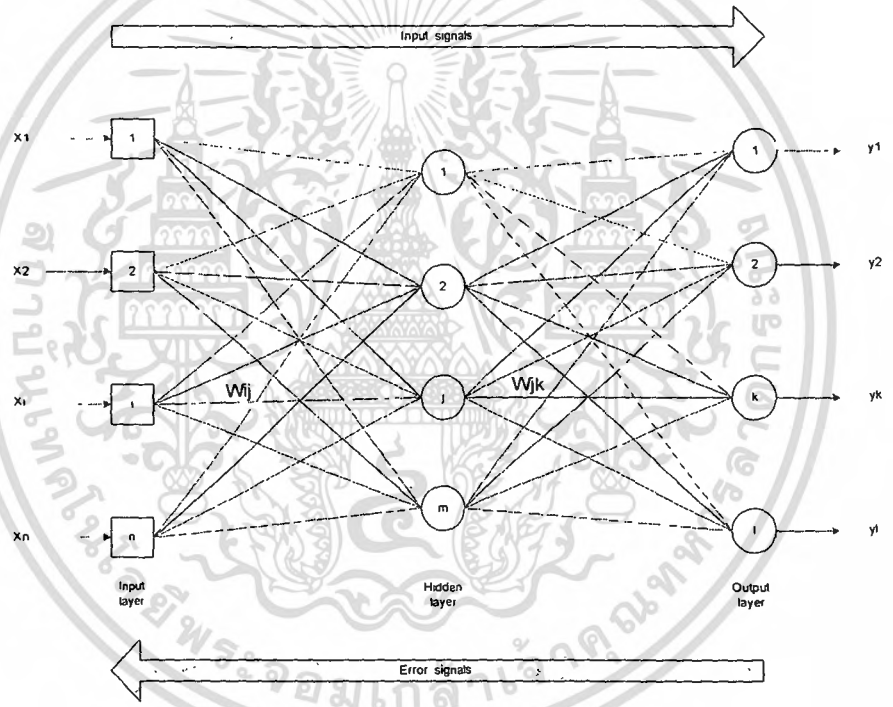
a คือ ค่าอัตราการเรียนรู้ ($0 < a < 1$).

ถ้าค่าความผิดพลาดของผลลัพธ์เป็นศูนย์แสดงว่าผลลัพธ์นั้นถูกต้อง ถ้าผลลัพธ์มีค่ามากจะทำการลดค่าถ่วงน้ำหนักสำหรับค่าของข้อมูลที่รับมาที่มีค่าเป็นบวก และการสอนถ้าทำในครั้งแรกไม่ถูกต้องก็จะใช้วิธีเดิมสอนจนกระทั่งได้ผลที่ถูกต้อง เรียกวิธีว่า epoch

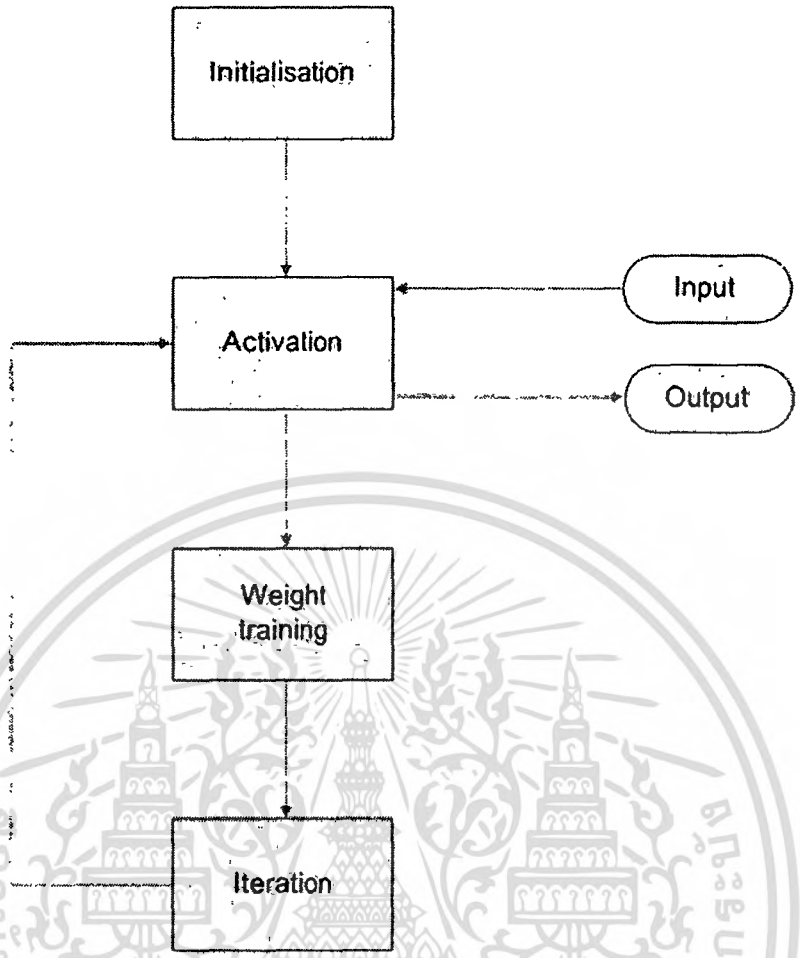
3.8 แบคพรอพเกชั่น

แบคพรอพเกชั่นเป็นโครข่ายที่มีโครงสร้างแบบมัลติเลเยอร์ (Multilayer network) การเรียนรู้ควบคุมโดยแต่ละนิวรอลมีค่าถ่วงน้ำหนักช่วยกับอินพุต และค่าถ่วงน้ำหนักจะถูกปรับเปลี่ยนเมื่อมีค่าความผิดพลาดจากฝึกฝน โดยส่วนใหญ่ใน มัลติเลเยอร์แบคพรอพเกชั่นเน็ตเวิร์ค จะนิยมใช้ซิกมอยด์ฟังค์ชัน

วิธีการแบคพรอพเกชั่นจะกำหนดค่าเริ่มต้นของค่าถ่วงน้ำหนักโดยการสุ่มค่า จากนั้นจะนำข้อมูลเข้าโครงข่ายจนกระทั้งได้ผลลัพธ์ แล้วนำค่าความผิดพลาดจากผลลัพธ์ส่งกลับเป็นข้อมูลทำให้ค่าถ่วงน้ำหนักเปลี่ยนไป ทำวิธีการนี้จนกระทั่งได้ผลลัพธ์ใกล้ค่าตามที่ต้องการ หรือจนกระทั่งค่าความผิดพลาดมีค่าน้อยมากๆ



รูปที่ 3.10 แผนภาพของโครงข่ายแบบแบคพรอพเกชั่นแบบทรีเลเยอร์



รูปที่ 3.11 แผนผังการฝึกสอนโครงข่ายประสาทเทียม

ขั้นตอนแรกของการฝึกสอนโครงข่ายประสาทเทียมต้องทำการ กำหนดค่าน้ำหนัก (Weight) และค่าเทรชโฮลด์ (Threshold) ให้แต่ละชั้นของโครงข่ายก่อน โดยค่าน้ำหนัก และเทรชโฮลด์ จะได้มาจากการสุ่มค่า ในช่วงของตัวเลขที่กำหนดไว้ จากสูตร $(-\frac{2.4}{Fi}, +\frac{2.4}{Fi})$ ที่ Fi คือจำนวนอินพุตทั้งหมดที่เข้ามาในโครงข่ายประสาทเทียม การสุ่มค่าน้ำหนัก และเทรช-โฮลด์ จะทำในครั้งแรกที่เริ่มทำการฝึกสอนโครงข่ายเท่านั้น ค่าน้ำหนัก และเทรชโฮลด์ในครั้งต่อไปของการฝึกสอนจะได้มาจากการปรับปรุงค่าน้ำหนัก และเทรชโฮลด์ จากการเรียนรู้ของโครงข่ายในครั้งที่ผ่านมา

ขั้นตอนที่สองเมื่อได้รับอินพุตเข้ามาแล้ว จะทำการคำนวณหาค่าเอาต์พุต เนื่องจากโครงข่ายที่เราใช้ เป็นโครงข่ายแบบ 3 ชั้น จึงต้องทำการคำนวณหาค่าเอาต์พุต 2 ครั้ง ที่ชั้นฮิดเด้น และชั้นเอาต์พุต

(a) การหาค่าเอาต์พุตในชั้นฮิดเด้นจะคำนวณหาได้จากสูตร

$$Yj(P) = \text{sigmoid}\left[\sum_{i=1}^{n} Xi(P) * Wij(P) - \theta j\right] \quad *** \qquad (3.8)$$

โดยที่ Y คือ เอาต์พุต

X คือ อินพุต

P คือ หมายเลขประจำเส้นของโครงข่าย

n คือ จำนวนอินพุตที่ได้รับเข้ามาของนิวรอล j ในชั้นฮิดเด้น

Sigmoid คือ ฟังก์ชั่นที่เป็นตัวตัดสินใจส่งข้อมูลไปยังเลเยอร์ถัดไป

θ คือ ค่าเทรชโฮลด์

W คือ ค่าน้ำหนัก

i , j คือ ชื่อเรียกประจำตัวของนิวรอล

(b) การหาค่าเอาต์พุตในชั้นเอาต์พุตจะคำนวณหาได้จากสูตร

$$Yk(P) = \text{sigmoid}\left[\sum_{j=1}^{m} Xjk(P) * Wjk(P) - \theta k\right] \quad *** \qquad (3.9)$$

โดยที่ Y คือ เอาต์พุต

X คือ อินพุต

P คือ หมายเลขประจำเส้นของโครงข่าย

m คือ จำนวนอินพุตที่ได้รับเข้ามาของนิวรอล j ในชั้นฮิดเด้น

Sigmoid คือ ฟังก์ชั่นที่เป็นตัวตัดสินใจส่งข้อมูลไปยังเลเยอร์ถัดไป

θ คือ ค่าเทรชโฮลด์

W คือ ค่าน้ำหนัก

j , k คือ ชื่อเรียกประจำตัวของนิวรอล

*หมายเหตุ *** เป็นสูตรที่ได้อ้างอิงมาจากรูปที่ 3.10*

ขั้นตอนที่สามคือการปรับปรุงค่าน้ำหนัก (Weight training) การปรับปรุงค่าน้ำหนักก็แบ่งเป็น 2 ครั้งเช่นกัน ซึ่งในแต่ละครั้งจะมีการคำนวณ ค่าความผิดพลาด ค่าน้ำหนักที่ถูก ต้อง (ในแต่ละอินพุต) และค่าน้ำหนักที่ได้ปรับปรุง

(a) การปรับปรุงค่าน้ำหนักที่ชั้นเอาท์พุต

- คำนวณหาค่าความผิดพลาด หาได้จากสูตร :

$$\delta k(P) = Yk(P) * [1 - Yk(P)] * Ek(P) \quad *** \quad (3.10)$$

โดยที่ $Ek(P) = Yd,k(P) - Yk(P)$ (3.11)

เมื่อ Yd คือ ค่าเอาท์พุตที่ต้องการ

- คำนวณหาค่าน้ำหนักที่ถูกต้อง หาได้จากสูตร :

$$\Delta Wjk(P) = \alpha * Yj(P) * \delta k(P) \quad *** \quad (3.12)$$

- ปรับปรุงค่าน้ำหนัก จากสูตร :

$$Wjk(P+1) = Wjk(P) + \Delta Wjk(P) \quad *** \quad (3.13)$$

(b) การปรับปรุงค่าน้ำหนักในชั้นฮิดเด้น

- คำนวณหาค่าความผิดพลาด หาได้จากสูตร :

$$\delta j(P) = Yj(P) * [1 - Yj(P)] * \sum_{k=1}^{1} \delta k(P) * Wjk(P) \quad *** \quad (3.14)$$

- คำนวณหาค่าน้ำหนักที่ถูกต้อง หาได้จากสูตร :

$$\Delta Wij(P) = \alpha * Xi(P) * \delta j(P) \quad *** \quad (3.15)$$

- ปรับปรุงค่าน้ำหนัก จากสูตร :

$$Wij(P+1) = Wij(P) + \Delta Wij(P) \quad *** \quad (3.16)$$

ขั้นตอนที่สี่ เพิ่มค่าชี้ตำแหน่ง P ขึ้นหนึ่งค่าแล้ววนกลับไปทำที่ขั้นตอนที่สอง จนกระทั่งค่าความผิดพลาดอยู่ในเกณฑ์ที่พอใจ หรือเท่ากับศูนย์

ขั้นตอนทั้งสี่ที่ได้กล่าวมาข้างต้นทั้งหมด คือการฝึกสอนโครงข่ายประสาทเทียมให้สามารถรู้จำช่วงเวลาในการพิมพ์รหัสของผู้ใช้ โดยที่เมื่อทำครบแล้วนับเป็นการเรียนรู้หนึ่งครั้ง เราจะต้องทำการพิมพ์รหัสหลายๆครั้ง เพื่อฝึกสอนให้โครงข่ายมีประสิทธิภาพมากขึ้น

*หมายเหตุ *** เป็นสูตรที่ได้อ้างอิงมาจากรูปที่ 3.10*

3.8.1 การพัฒนาประสิทธิภาพของแบคพรอพเกชั่น

เนื่องจากวิธีการแบคพรอพเกชั่นเมื่อนำไปแก้ปัญหานั้นพบว่ามีแนวโน้มค่อนข้างช้า ในบางปัญหาอาจทำร้อยหรือพันครั้งของ Epoch จึงทำให้ได้ค่าความผิดพลาดที่เป็นที่พอใจได้ จึงได้มีการรวมแรงกระตุ้น (momentum) ในสูตรเพื่อช่วยแก้ค่าถ่วงน้ำหนัก โดยคิดเฉพาะค่าถ่วงน้ำหนักที่เปลี่ยนในรอบที่ผ่านมา เมื่อ t แทนรอบปัจจุบันและ t-1 แทนรอบที่ผ่านมา เราสามารถเขียนกฎการเรียนรู้ได้ดังนี้

$$\Delta w_{ij}(t) = \alpha . x_i . \delta_j + \beta \Delta w_{ij}(t-1) \tag{3.17}$$

$$\Delta w_{jk}(t) = \alpha . y_j . \delta_k + \beta \Delta w_{jk}(t-1) \tag{3.18}$$

เมื่อ $\Delta w_{ij}(t)$ เป็นผลรวมการเพิ่มค่าถ่วงน้ำหนักของการเชื่อมต่อระหว่างโหนด i และ j

β แทนค่าแรงกระตุ้นมีค่าระหว่าง 0 ถึง 1 หากค่าเป็น 0 แสดงว่าไม่มีการใช้แรงกระตุ้น

กฎที่มีการเพิ่มค่าแรงกระตุ้นเรียกว่า Generalized delta rule และการเพิ่มแรงกระตุ้นนั้นยังทำให้วิธีการแบคพรอพเกชั่นหลีกเลี่ยงจาก local minima และทำให้เคลื่อนผ่านพื้นที่ที่มีค่าความผิดพลาดที่เกือบไม่มีการเปลี่ยนแปลงได้เร็วขึ้น

อาจมีการใช้ไฮเปอร์โบลิกแทนเจนฟังค์ชันแทนซิกมอยด์ฟังค์ชันเพื่อให้เพอร์เซ็ปตรอนทำงานได้เร็วยิ่งขึ้น สมการของไฮเปอร์โบลิกแทนเจนฟังค์ชัน คือ

$$\tanh(x) = \frac{2a}{1+e^{-bx}} - a \tag{3.19}$$

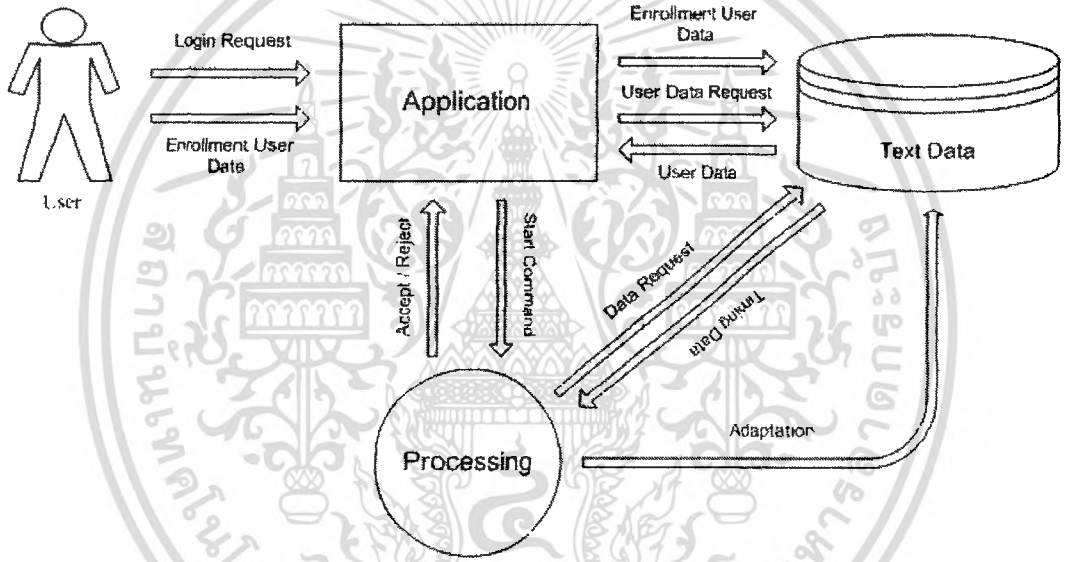
เมื่อ a และ b เป็นค่าคงที่ เช่น a = 1.7 และ b = 0.7

บทที่ 4
หลักการทำงานและโครงสร้างระบบ

4.1 โครงสร้างของระบบ

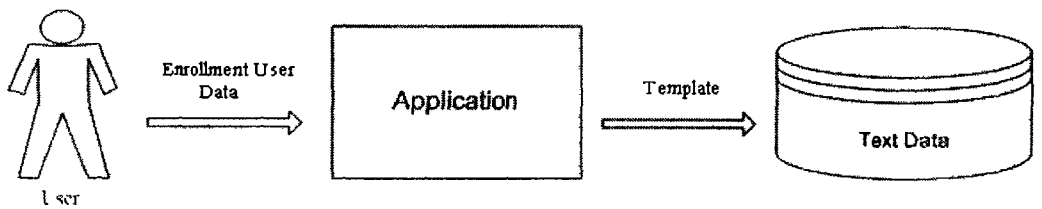
โครงสร้างของระบบประกอบด้วย 3 ส่วนหลักๆ คือ

- ส่วนโปรแกรมหลัก (Main application)
- ส่วนประมวลผล (Processing)
- ส่วนเก็บข้อมูล (Storage)



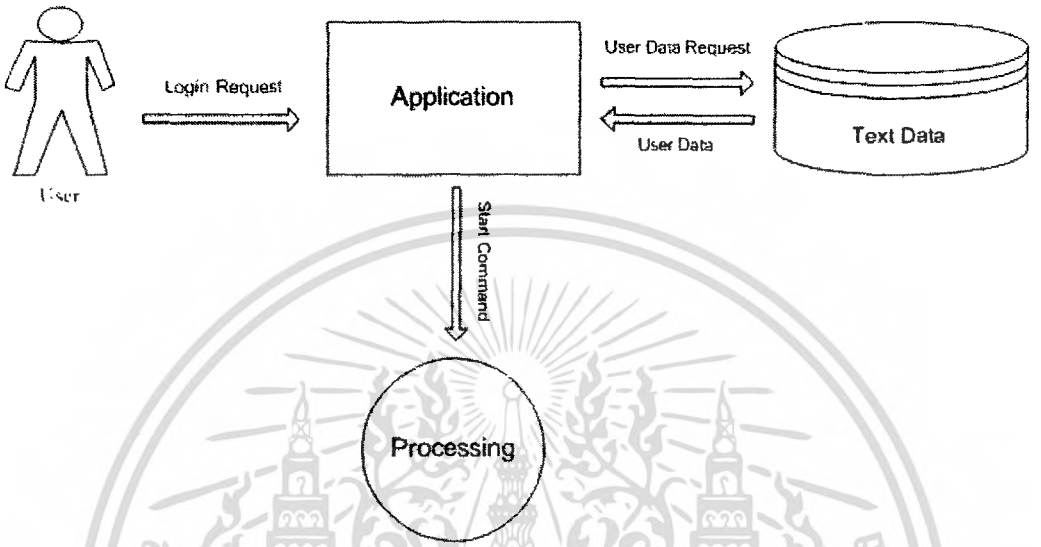
รูปที่ 4.1 โครงสร้างของระบบ

4.1.1 ส่วนโปรแกรมหลัก



รูปที่ 4.2 ภาพรวมการทำงานของขั้นตอนการลงทะเบียน

การใช้งานระบบนั้น ขั้นตอนแรกต้องทำการลงทะเบียนเพื่อสร้างชื่อผู้ใช้งาน (Account) ก่อน โดยข้อมูลที่ผู้ใช้ต้องป้อนให้ระบบ ได้แก่ ชื่อ, นามสกุล, ชื่อผู้ใช้งาน และ รหัสผ่าน หลังจากได้รับข้อมูลของผู้ใช้มาแล้ว ตัวโปรแกรมจะทำการเก็บข้อมูลไว้ในฐานข้อมูล โดยเก็บในรูปแบบของเท็กซ์ไฟล์ เพื่อใช้เป็นแม่แบบในการเปรียบเทียบในครั้งต่อไป



รูปที่ 4.3 ภาพรวมการทำงานในขั้นตอนของการร้องขอเข้าระบบ

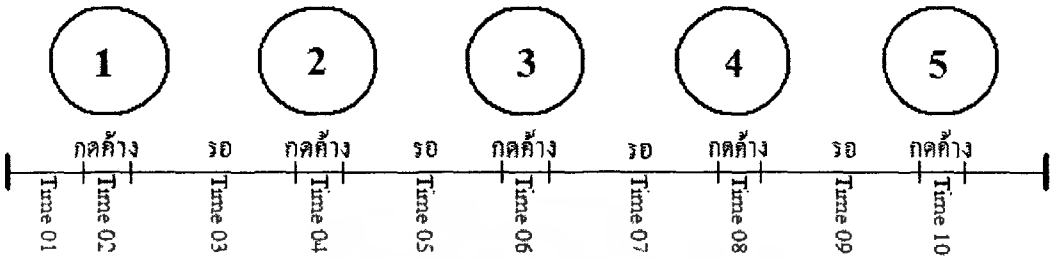
หลังจากผ่านขั้นตอนของการลงทะเบียนแล้ว เมื่อผู้ใช้ทำการร้องขอเข้าระบบ ผู้ใช้จะต้องทำการพิมพ์ ชื่อผู้ใช้ และรหัสผ่าน โปรแกรมจะทำการดึงข้อมูลรหัสผ่านของผู้ใช้จากฐานข้อมูลนำมาเปรียบเทียบกับ รหัสผ่านที่ผู้ทำการร้องของเข้าระบบป้อนเข้ามา เป็นการตรวจสอบผู้ใช้ในขั้นต้น ถ้าหากว่ารหัสที่ผู้ร้องขอเข้าระบบป้อนเข้ามา ไม่ตรงกับรหัสผ่านที่ได้ทำการลงทะเบียนไว้ในครั้งแรก ระบบจะปฏิเสธการเข้าระบบของผู้ร้องขอเข้าระบบ แต่ถ้ารหัสผ่านที่ป้อนเข้ามาตรงกันกับรหัสผ่านที่ได้ทำการบันทึกไว้ ก็จะเข้าสู่การตรวจสอบในขั้นที่สองคือส่วนของ การประมวลผล (Processing)

4.1.1.1 วิธีการเก็บข้อมูลช่วงเวลาในการพิมพ์รหัสผ่านเพื่อนำไปใช้งาน

ข้อมูลที่จะนำไปใช้ฝึกสอนให้แก่โครงข่ายประสาทเทียม จะตรวจเช็คจากช่วงเวลาในการพิมพ์รหัสโดยมีวิธีการตรวจสองช่วงเวลาคือ

- ช่วงเวลาตั้งแต่มีการกดแป้นคีย์บอร์ดไปจนถึงปล่อยแป้นคีย์บอร์ด
- ช่วงเวลาตั้งแต่ปล่อยแป้นคีย์บอร์ดไปจนถึงการกดอีกครั้งหนึ่ง

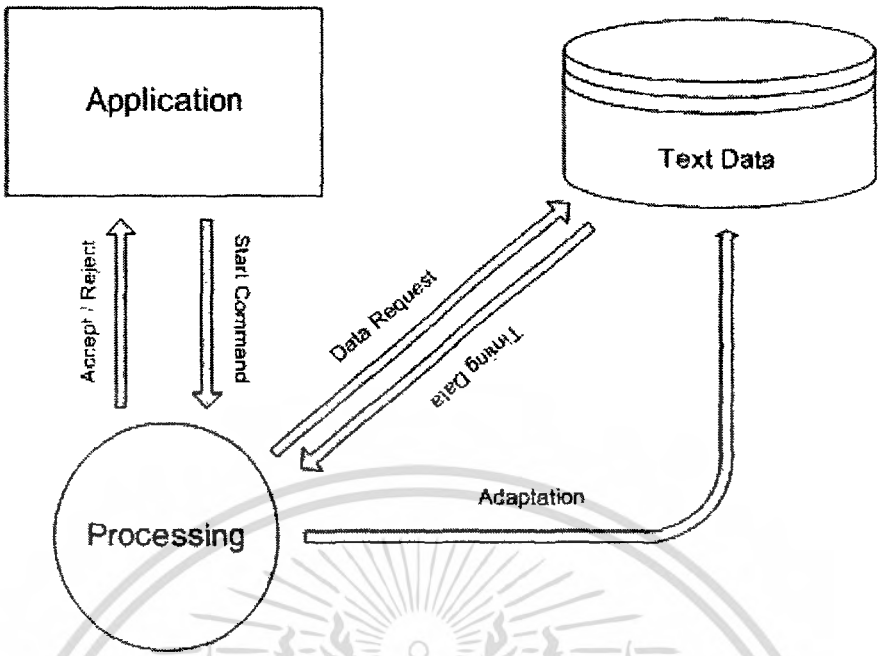
ซึ่งช่วงเวลาที่ได้จะแปรผันตามจำนวนของรหัสผ่าน เป็นจำนวนสองเท่า เช่นถ้าหากว่ารหัสผ่าน มีจำนวน 3 ตัวอักษร คือ 123 จะทำให้ได้ ข้อมูลช่วงเวลา (Timing Data) เป็นจำนวนเท่ากับจำนวนตัวอังษรของรหัสผ่าน ข้อมูลที่ได้ก็จะเป็นเอกลักษณ์ในการพิมพ์ของผู้ใช้



รูปที่ 4.4 วิธีการเก็บช่วงเวลาในการพิมพ์รหัสผ่าน

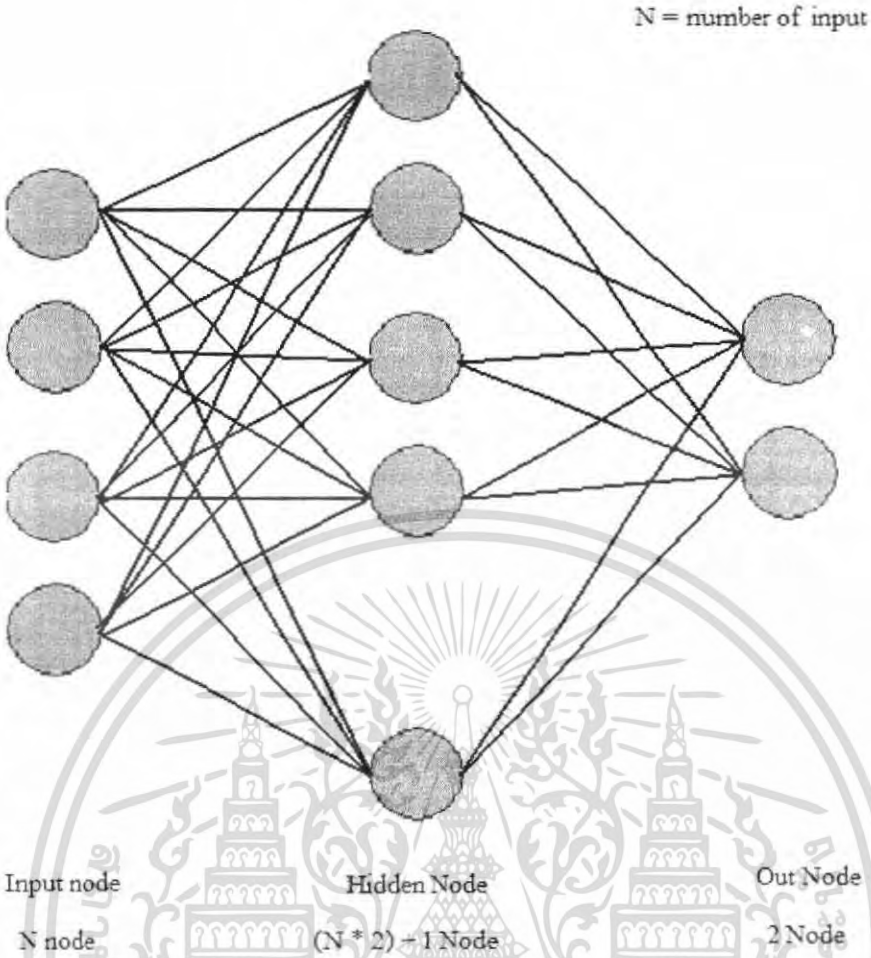
4.1.2 ส่วนประมวลผล

ส่วนประมวลผลจะรับข้อมูลจากฐานข้อมูล โดยอ่านข้อมูลเท็กซ์ไฟล์นำมาเป็นอินพุตเพื่อประมวลผล แล้วส่งค่าที่ได้ซึ่งแสดงอยู่ในรูปการให้สิทธิและการปฏิเสธการเข้าระบบ กลับคืนไปให้แก่โปรแกรมเพื่อแสดงผลให้ผู้ใช้ทราบ และ ทำการปรับปรุงข้อมูลในเท็กซ์ไฟล์ส่งกลับคืนไปเก็บยังฐานข้อมูล การทำงานของส่วนประมวลผลแสดงได้ดังรูป



รูปที่ 4.5 ภาพรวมการทำงานของส่วนประมวลผล

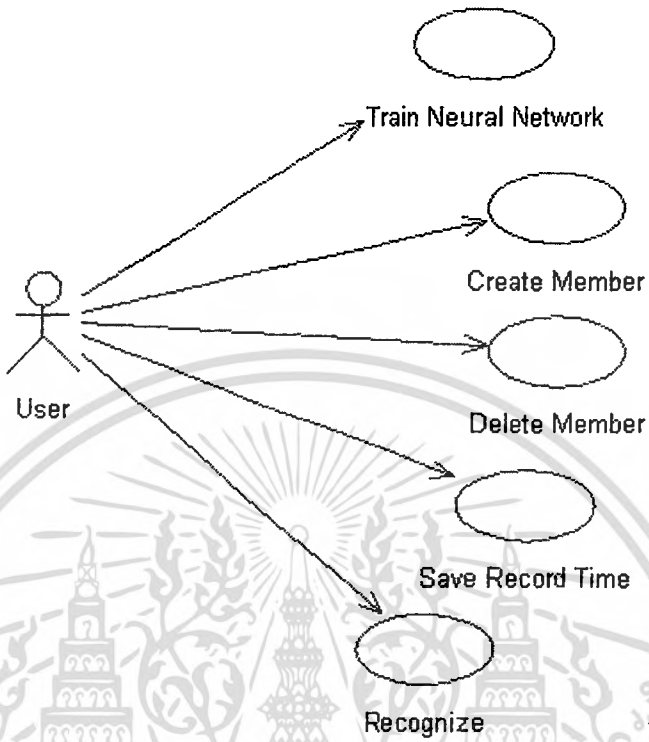
โดยที่ส่วนประมวลผลจะอาศัยหลักการของ อาร์ติฟิเชียลนิวรอลเน็ตเวิร์ค ในการระบุบุคคลที่ทำการล็อกอินเข้าระบบ โดยใช้โมเดล แบบแบคพรอพเกชั่นเน็ตเวิร์ค ซึ่งเป็น ระบบเน็ตเวิร์คแบบมัลติเลเยอร์ กำหนดจำนวนเลเยอร์ให้มี 3 เลเยอร์คือ อินพุตเลเยอร์ , ฮิดเด้นเลเยอร์ และเอาท์พุตเลเยอร์ การเรียนรู้ของโครงข่ายเป็นแบบ ซุปเปอร์ไวด์เลิร์นนิ่ง เป็นการเรียนรู้แบบที่มีการฝึกสอนมาก่อน โดยใช้อินพุตที่รับเข้ามาจากโปรแกรมหลักเป็นข้อมูลในการฝึกสอนโครงข่าย และใช้ฟังก์ชั่นซิกมอย์ด เป็นแอคทิเวชั่นฟังก์ชั่น



รูปที่ 4.6 สถาปัตย์กรรมโครงข่ายประสาทเทียมที่ใช้

จำนวนโหนดในอินพุตเลเยอร์จะเท่ากับจำนวณอินพุตที่ได้รับเข้ามา จำนวณโหนดในฮิดเด้นเลเยอร์ในที่นี้กำหนดให้เท่ากับจำนวนอินพุตเลเยอร์หารด้วยสอง และจำนวนโหนดในเอาท์พุต เลเยอร์เท่ากับสอง โดยกำหนดชุดเอาท์พุตดีไซน์(Output desire)ไว้คือ เอาท์พุตโหนดที่หนึ่งเป็นหนึ่งและเอาท์พุตโหนดที่สองเป็นศูนย์ ให้ทำการให้สิทธิเข้าระบบ และถ้าชุดเอาท์พุตดีไซน์เป็นเอาท์พุตโหนดที่หนึ่งเท่ากับศูนย์และเอาท์พุตโหนดที่สองเท่ากับหนึ่ง ให้ทำการปฏิเสธการเข้าระบบ ดังนั้นหลังจากการตรวจสอบแล้วถ้าค่าเอาท์พุตที่ออกมาคือ เอาท์พุตโหนดที่หนึ่งเท่ากับหนึ่งหรือเข้าใกล้เลขหนึ่งและเอาท์พุตโหนดที่สองเท่ากับศูนย์หรือเข้าใกล้เลขศูนย์แล้วแสดงว่าผู้ทำการร้องขอเข้าระบบเป็นบุคคลคนเดียวกับที่ได้ทำการลงทะเบียนไว้ และจะอนุญาตให้เข้าระบบ แต่ถ้าหากผ่านการตรวจสอบแล้วปรากฏว่าเอาท์พุตโหนดที่หนึ่งเป็นศูนย์หรือเข้าใกล้เลขศูนย์ และเอาท์พุตโหนดที่สองเป็นหนึ่งหรือเข้าใกล้เลขหนึ่ง จะหมายความว่าผู้ที่ทำการร้องขอเข้าระบบ มิใช่บุคคลที่ได้ทำการลงทะเบียนไว้ และไม่อนุญาตให้เข้าระบบ

4.2 Use Case Diagram และ Sequence Diagram



รูปที่ 4.7 Use Case Diagram

4.3 วิธีการฝึกสอนโครงข่ายประสาทเทียม

การฝึกสอนโครงข่ายประสาทเทียม ให้สามารถจดจำเอกลักษณ์ในการพิมพ์ของแต่ละบุคคลได้นั้น จะเริ่มทำการฝึกสอนหลังจากได้รับข้อมูลของผู้ใช้เป็นจำนวนตั้งแต่ 50 ชุดข้อมูลขึ้นไป หลังจากนั้นทุกๆ ครั้งที่มีการร้องขอเข้าระบบ ระบบจะทำการเก็บค่า ความถูกต้องของการเข้าระบบ และค่าความผิดพลาดของการเข้าระบบไว้ จากกระบวนการการตรวจสอบผู้ร้องขอเข้าระบบ และ ทำการเก็บค่าเวลาในการเข้าระบบครั้งสุดท้ายไว้ด้วย เพื่อใช้ในการตรวจสอบตัวบุคคล (ค่าเวลาที่เก็บมานั้น เก็บมาจากเวลาจริงซึ่งเรียกเก็บมาจากไบออส (Bios) ของเครื่องคอมพิวเตอร์)

4.3.1 การตรวจเช็คการจดจำบุคคลของโครงข่าย

วิธีการตรวจเช็คว่าระบบสามารถจดจำบุคคลได้แล้วหรือไม่นั้น จะใช้วิธีการตรวจเช็คด้วยค่าความแม่นยำ (Accuracy) โดยที่ค่าความแม่นยำหาได้จาก

(ค่าความถูกต้องของการเข้าระบบ / จำนวนครั้งในการร้องขอเข้าระบบ)*100

ใช้ระบบสามารถผ่านเข้าใช้ระบบได้

จำนวนครั้งในการร้องขอเข้าระบบ คือ จำนวนครั้งที่ผู้มีสิทธิเข้าระบบ ทำการร้องขอเข้าระบบ โดยจะเริ่มคิดตั้งแต่ผู้มีสิทธิเข้าระบบทำการร้องขอเข้าระบบ ครั้งที่ 50 ขึ้นไปหลังจากการให้ข้อมูลแม่แบบ แล้ว ดังนั้นการตรวจสอบว่าระบบสามารถจดจำผู้ใช้ได้หรือไม่นั้น จะเริ่มขึ้นตั้งแต่การร้องขอเข้าระบบ ครั้งที่ 100 ขึ้นไป (มาจากการให้แม่แบบ 50 ครั้ง และการร้องขอเข้าระบบอีก 50 ครั้ง) เมื่อค่าความแม่นยำ มีค่ามากกว่า 95% จะถือว่าระบบสามารถจดจำผู้ใช้ได้และผู้ใช้สามารถเริ่มใช้ระบบตรวจสอบบุคคลโดยอาศัยช่วงเวลาในการกดคีย์บอร์ดได้แล้ว

บทที่ 5
ผลการทดลองและการวิเคราะห์ข้อมูล

5.1 หน้าตาโปรแกรมหลัก

รูปที่ 5.1 หน้าตาของโปรแกรมหลัก

โดยจะมีเมนูของโปรแกรมเพื่อใช้ในการทดและทดสอบดังนี้

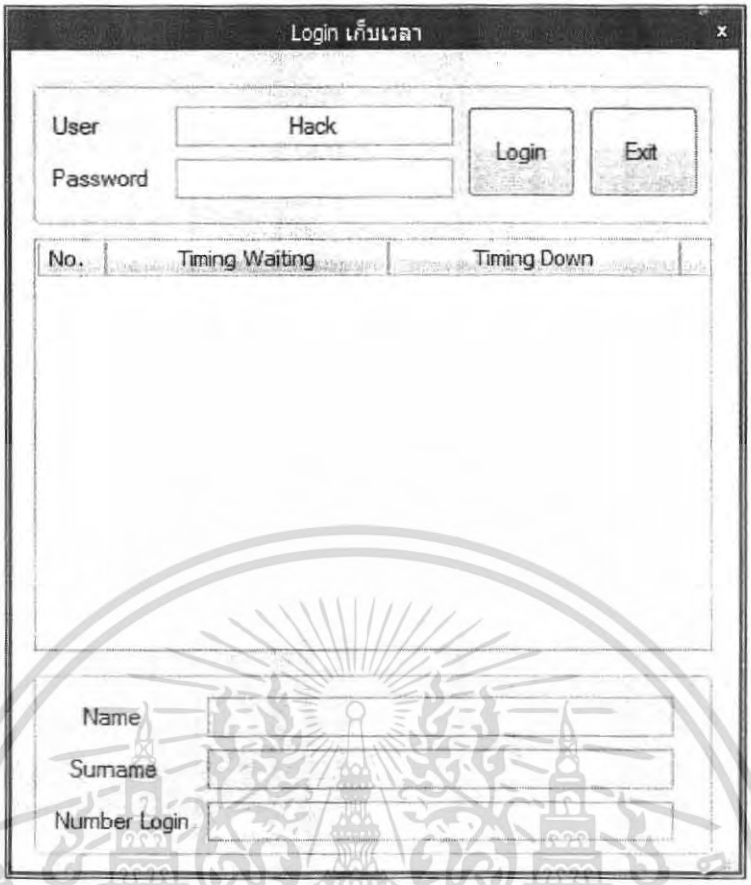
- รายการ โดยจะมีเมนูย่อยเพื่อแยกการทำงานเป็นส่วนดังนี้
  - สมัครสมาชิก ทำหน้าทำการลงทะเบียนเพื่อสร้างข้อมูลเริ่มแรงให้สมาชิกนั้น โดยมีหน้าตาดังรูป

รูปที่ 5.2 ส่วนของการลงทะเบียนสมาชิก

- ลบสมาชิก ทำหน้าที่ลบสมาชิกในระบบ โดยมีหน้าตาดังนี้

รูปที่ 5.3 ส่วนของการลบสมาชิก

- เก็บข้อมูลเวลา ทำหน้าที่ทำการให้สมาชิกนั้น ทำการล็อคอินเพื่อทำการบันทึกเวลาเพื่อใช้เป็นข้อมูลในการฝึกสอนโครงข่ายประสาทเทียม โดยมีหน้าตาดังนี้

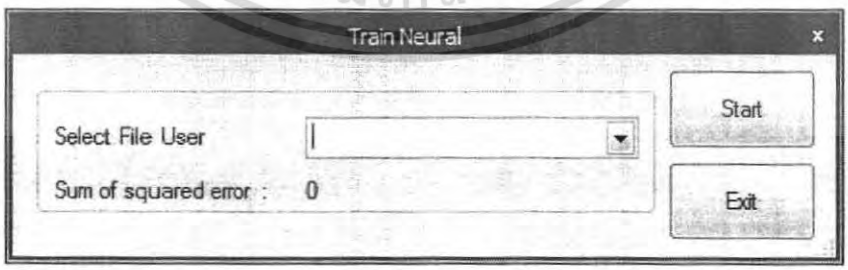


รูปที่ 5.4 ส่วนของการทำการล็อคอินเพื่อทำการบันทึกเวลาสมาชิก

- ออกโปรแกรม ทำหน้าออกจากโปรแกรม

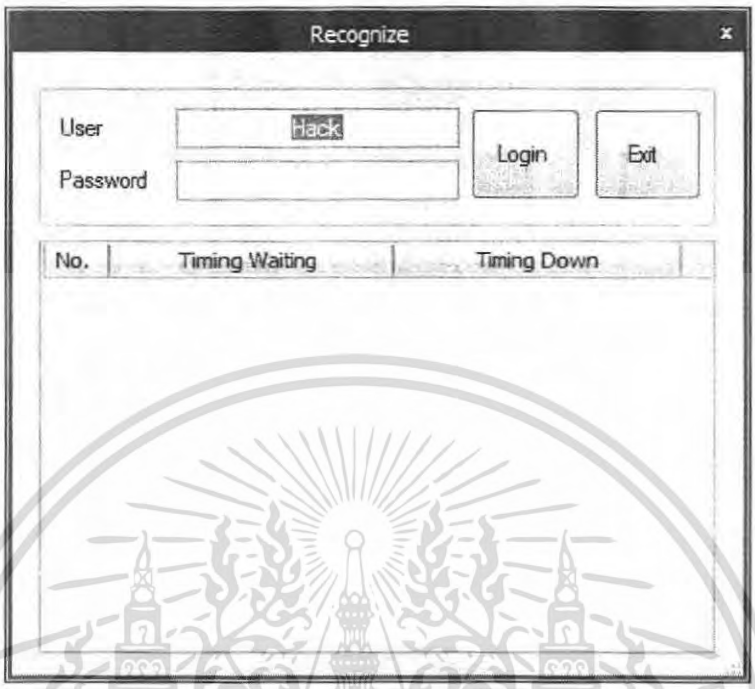
- Neural Network โดยจะมีเมนูย่อยเพื่อแยกการทำงานเป็นส่วนดัง

  - Train Neural ทำหน้าที่ใช้ในการเลือกไฟล์สมาชิกเพื่อฝึกสอนนิวรอลของสามาชิกนั้น โดยมีหน้าตาดังนี้



รูปที่ 5.5 ส่วนของการเลือกไฟล์สมาชิกเพื่อฝึกสอนนิวรอล

- Recognize ทำหน้าที่ใช้ในการตรวจสอบช่วงเวลาที่สมาชิกได้ทำการล็อคอินเข้ามาเวลาถูกต้องหรือไม่ โดยมีหน้าตาดังนี้



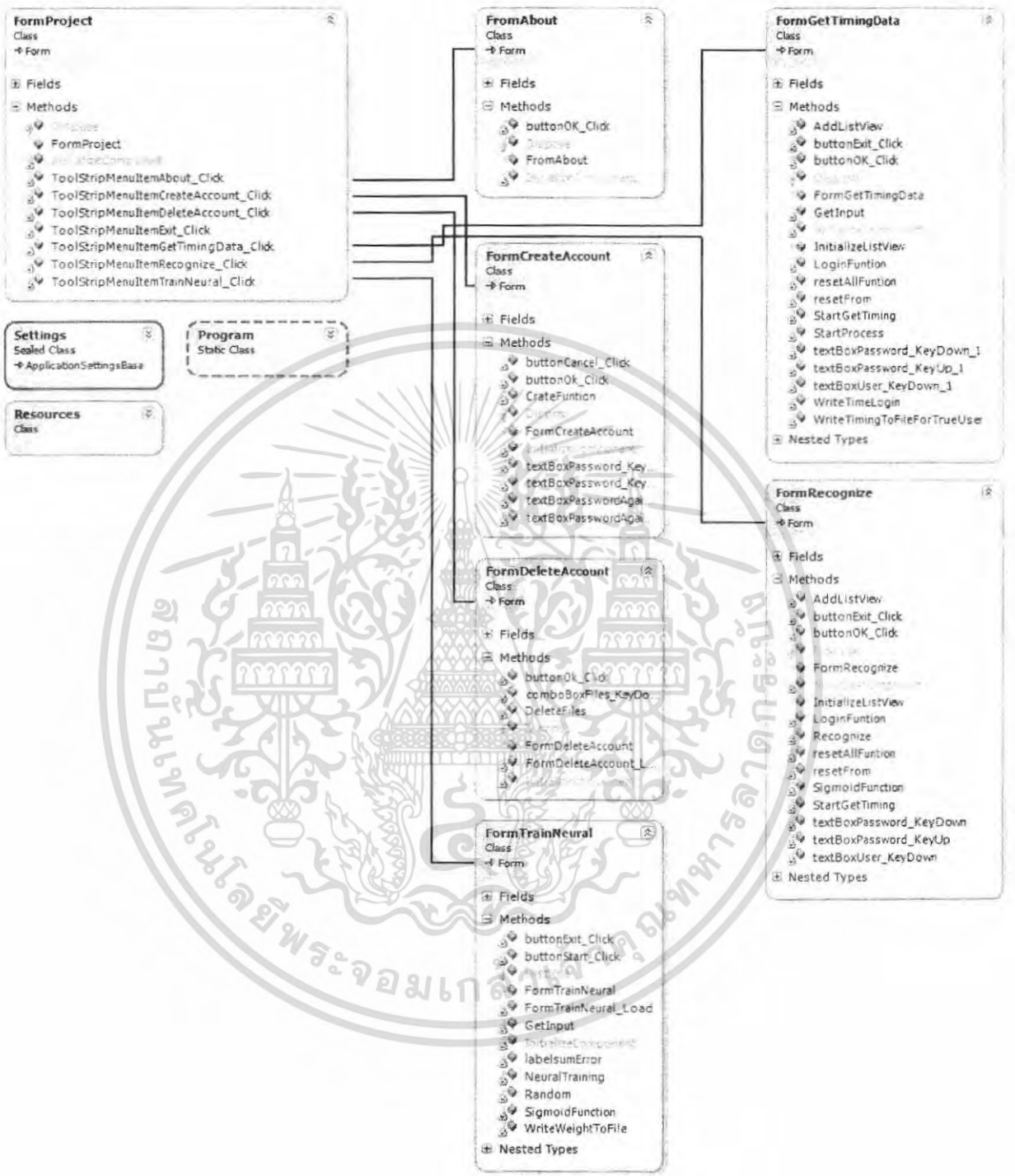
รูปที่ 5.6 ส่วนของการการตรวจสอบช่วงเวลาที่สมาชิก

5.2 เมธอด(Method) ที่สำคัญที่ใช้ในโปรแกรม

- AddListview เป็น เมธอด ที่ทำการเซ็ตค่าในกับ Listview ที่ใช้ในการแสดงค่าเวลาที่ตรวจจับได้
- GetInput เป็น เมธอด ที่ทำการอ่านค่าของมูลจากไฟล์นำมาใช้งาน
- NeuralProcessing เป็น เมธอด ที่ใช้ในการเรียกใช้โครงข่ายประสาทเทียมในการตรวจสอบช่วงเวลาผู้ใช้งาน
- NeuralTraining เป็น เมธอด ที่ใช้ในการฝึกสอนโครงข่ายประสาทเทียม
- ResetAllFunction เป็น เมธอด ที่ใช้ในการเคลียร์ ค่าทั้งหมดของโปรแกรม
- ResetForm เป็น เมธอด ที่ใช้ในการเคลียร์ ค่า Form ที่แสดงผลอยู่ทั้งหมด
- SigmoidFuuction เป็น เมธอด ที่ใช้ในการสร้างค่าเพื่อนำไปใช้ในโครงข่ายประสาทเทียม
- Random เป็น เมธอด ที่ใช้ในการสุ่มค่าเพื่อนำไปใช้ในโครงข่ายประสาทเทียม
- StartGetTiming เป็น เมธอด ที่รับค่าของเวลาที่จับได้มาจัดเก็บลง File ตามชื่อของชื่อผู้ใช้นั้น ๆ

- StartProcess เป็น เมธอด ที่ใช้ในการตรวจจำนวนในการล็อกอินครบที่กำหนดแล้วหรือยัง เมื่อครบจะทำการฝึกสอนโครงข่าย
- WriteTimeLogin เป็น เมธอด ที่ใช้เขียนเพิ่มค่าจำนวนครั้งในการล็อกอิน
- WriteWeightToFile เป็น เมธอด ที่ใช้ในการเขียนค่าน้ำหนัก ที่ได้จากการฝึกสอนมาบันทึกลง File

5.3 คลาสไดอะแกรม (Class Diagram)



รูปที่ 5.7 คลาสไดอะแกรมของระบบ

5.4 ผลการทดลอง

จากการทดลองโดยการทดลองป้อนชุดข้อมูลเพื่อทำการฝึกสอนให้กับโครงข่ายประสาทเทียมโดยใช้ชุดข้อมูลที่ได้ทำการเก็บตัวอย่างช่วงเวลาโดยมีรูปแบบที่จัดเก็บลงไฟล์ดังรูป

|Password|123456|Surname|สะดีวงศ์|Name|กฤษฎาญชล

|Login|214

|True|0

|Flase|0

|Train|1

|Weight_IH|0

|Weight_HO|0

|Threshold_H|0

|Threshold_O|0

|Time|

|0.0000|0.1467|0.2860|0.0847|0.2382|0.0955|0.2605|0 1594|0.3024|0.1167|0.2336|0.1113|1.0000|0.0000

|0.0000|0.1166|0.3039|0.1140|0 3018|0 1276|0.2666|0.1114|0.2592|0 1062|0.2525|0.1085|1.0000|0 0000

|0 0000|0.1115|0 3231|0.1113|0.3272|0.1438|0 3413|0 1383|0.2759|0.1168|0.2924|0.1008|1.0000|0.0000

|0.0000|0.1115|0.3576|0 1061|0 3747|0.1168|0.3071|0.1244|0.2825|0 1115|0.2725|0.1008|1.0000|0.0000

|0.0000|0.1115|0.3348|0.1221|0.3380|0.1487|0.3321|0.1112|0 2586|0.1063|0.6074|0 0978|1.0000|0.0000

|0.0000|0.1307|0.2728|0.1274|0.3157|0.1170|0.2941|0.1274|0.2941|0.1223|0 3124|0.0925|1.0000|0 0000

|0.0000|0.1058|0.3204|0.1142|0.3343|0 1328|0 2648|0.1008|0.2847|0.1275|0.3294|0.1381|1.0000|0.0000

|0.0000|0 1112|0.3073|0 1060|0 2904|0.1116|0.2818|0.1168|0.2754|0.1168|0.2918|0.1114|1.0000|0 0000

รูปที่ 5.8 แสดงชุดข้อมูลที่จัดเก็บลงไฟล์

เข้าสู่โครงข่ายประสาทเทียมที่ได้ออกมาโดยมีโดยมีพารามิเตอร์ดังต่อไปนี้

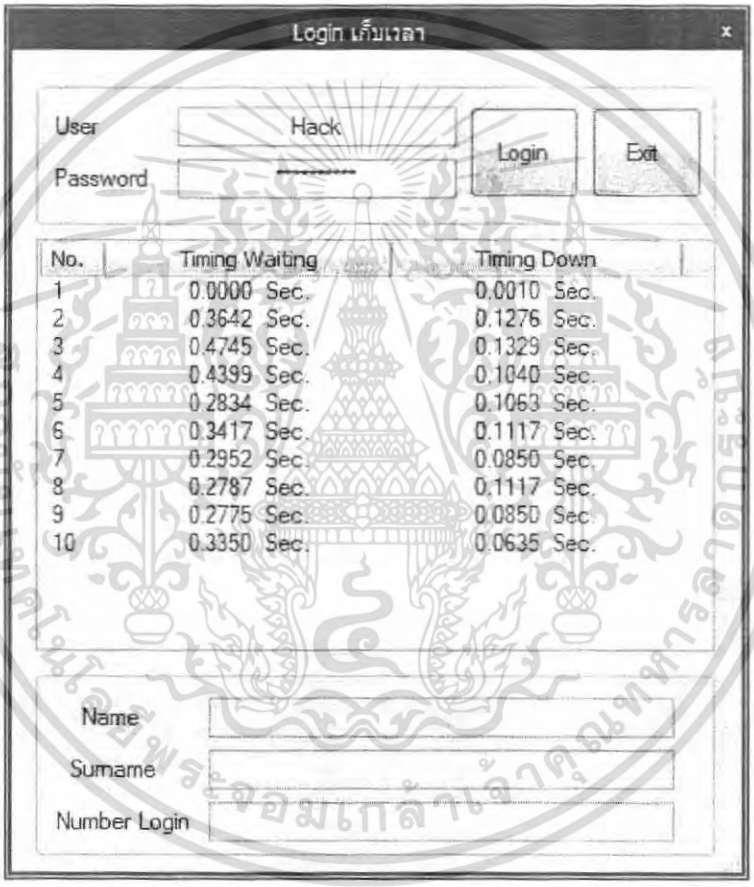
- จำนวนชุดข้อมูลมีตั้งแต่ 10, 20, 50, 100, 200 ชุด ของแต่ละผู้ใช้
- Input Node มีจำนวนเท่ากับจำนวนตัวอักษรของรหัสผ่านคูณด้วยสอง
- Hidden Node มีจำนวนเท่ากับจำนวนตัวอักษรของรหัสผ่านคูณด้วยสองแล้วบวกด้วยหนึ่ง
- Output Node มีจำนวนเท่ากับสองโหนด
- Learning Rate มีค่าเท่ากับ 0.15
- กำหนดค่า Sum Square Error ต้องมีค่าน้อยกว่า 0.0001

โดยผลที่ออกมาลักษณะการทำงานของโครงข่ายประสาทเหมือนจะทำงานได้แต่เมื่อนำไปทดลองส่วนที่ทำการตรวจสอบบุคลกับพบว่ายังไม่สามารถตรวจสอบบุคคลได้ ซึ่งจากข้างต้นตั้งสมมุติฐานว่าเกิดจากส่วนของโครงข่ายประสาทเทียม และการกำหนดค่าพารามิเตอร์บางส่วนผิด

บทที่ 6
บทสรุป

สรุป

จากการทดลองตามส่วนต่าง ๆ ที่ได้วางแผนในช่วงแรกได้ทำการทดลองสร้างโครงข่ายประเทียมขนาดเล็ก ๆ โดยทำการฝึกสอน AND OR GATE ขนาด 2 อินพุต อย่างง่าย ๆ ซึ่งผมที่ได้เป็นน่าพอใจต่อมาทดลองการใช้เมธอด HiPerfTimer ซึ่งเป็นการใช้เรียกใช้คำสั่งจาก APIs ที่จัดเก็บอยู่ใน Kernel32.dll เพื่อทดสอบการจับช่วงเวลาของการพิมพ์ โดยได้ผลออกมาดังรูป



รูปที่ 6.1 แสดงการจับช่วงเวลาการพิมพ์ของโปรแกรม

โดยช่วงเวลาที่ได้ทำการจับออกมานั้นจะทำการบันทึกลงไฟล์ตามชื่อผู้ใช้นั้น ๆ โดยผลออกมาได้ถูกต้องตามที่ได้วางแผนไว้โดยลักษณะของมูลตามแบบฟอร์มที่ได้กำหนดไว้แล้วบันทึกลงไฟล์ลักษณะดังรูป

|Password|123456|Surname|สะดีวงศ์|Name|กฤษฎาญชล

|Login|214

|True|0

|Flase|0

|Train|1

|Weight_IH|0

|Weight_HO|0

|Threshold_H|0

|Threshold_O|0

|Time|

|0.0000|0.1467|0.2860|0.0847|0.2382|0.0955|0.2605|0 1594|0.3024|0.1167|0.2336|0.1113|1.0000|0 0000

|0.0000|0.1166|0.3039|0.1140|0.3018|0.1276|0.2666|0.1114|0.2592|0.1062|0.2525|0 1085|1.0000|0.0000

|0.0000|0 1115|0.3231|0.1113|0.3272|0.1438|0.3413|0.1383|0.2759|0.1168|0 2924|0.1008|1 0000|0.0000

|0.0000|0 1115|0.3576|0 1061|0.3747|0.1168|0.3071|0.1244|0.2825|0.1115|0.2725|0.1008|1.0000|0.0000

|0.0000|0.1115|0.3348|0.1221|0.3380|0.1487|0.3321|0 1112|0.2586|0.1063|0.6074|0 0978|1.0000|0 0000

|0.0000|0.1307|0.2728|0.1274|0.3157|0.1170|0.2941|0.1274|0.2941|0.1223|0 3124|0.0925|1.0000|0.0000

|0.0000|0.1058|0.3204|0.1142|0 3343|0.1328|0.2648|0.1008|0.2847|0.1275|0.3294|0.1381|1.0000|0.0000

|0.0000|0 1112|0.3073|0.1060|0 2904|0.1116|0.2818|0.1168|0.2754|0.1168|0.2918|0.1114|1.0000|0 0000

|0.0000|0.1307|0.2728|0.1274|0 3157|0.1170|0.2941|0.1274|0.2941|0.1223|0.3124|0.0925|1.0000|0 0000

|0.0000|0.1115|0.3576|0.1061|0 3747|0.1168|0.3071|0.1244|0.2825|0.1115|0.2725|0.1008|1.0000|0 0000

|0.0000|0.1467|0.2860|0.0847|0 2382|0.0955|0.2605|0.1594|0.3024|0.1167|0.2336|0.1113|1.0000|0.0000

รูปที่ 6.2 แสดงชุดข้อมูลที่จัดเก็บลงไฟล์

หลังจากนั้นได้ทำการทดลองนำข้อมูลที่ได้จัดเก็บมานั้นทำการฝึกสอนให้กับโครงข่ายประสาทเทียมที่ได้ทดลองสร้างขึ้นพบว่าการฝึกสอนเหมือนกันตัวโครงข่ายประสาทเทียมนั้นได้ทำการจดจำข้อมูลที่ส่งเข้าไปฝึกสอนได้แล้ว แต่เมื่อนำโครงข่ายนั้นมาทดลองทำการตรวจสอบผู้ใช้งานพบว่าไม่สามารถแยกแยะได้ว่าช่วงเวลาถูกต้องหรือไม่ โดยผู้จักทำได้ศึกษาข้อมูลเพิ่มเติมแล้วพบว่าตัวโครงข่ายปสาทเทียมนั้นยังไม่ถูกต้องทั้งหมด ซึ่งผู้จัดทำได้สันนิฐานเกิดจาก

- การหาจำนวนของชั้น Hidden Node ยังหาไม่สมกับสมมุติฐาน
- โครงสร้างโครงข่ายประสาทเทียม
- รูปแบบการฝึกสอนของโครงข่ายประสาทอาจจะยังไม่เหมาะสมกับสมมุติฐาน
- การจัดเก็บช่วงเวลาอาจจะยังไม่ดีพอทำให้การฝึกสอนทำได้ไม่ดีพอ

ซึ่งทั้งหมดนี้มีผลต่อการฝึกสอนให้แก่โครงข่ายประสาทเทียมทั้งหมด โดยต้องปรับปรุงตัวโครงสร้างโครงข่ายประสาทเทียมก่อนเป็นอันดับแรก เพราะปัญหาที่เกิดจากการพัฒนาที่เกิดขึ้นนั้นเกิดขึ้นที่ตัวโครงข่ายประสาทเทียม

บรรณานุกรม

ศุภชัย สมพานิช,& สัจจะ จรัสรุ่งรวีวร (บรรณาธิการ). (2546). **คู่มือการเขียนโปรแกรม Visual C# . NET ฉบับโปรแกรมเมอร์.** กรุงเทพฯ: ด่านสุทธาการพิมพ์.

Coppin, Ben. (2004). **Artificial intelligence illuminated.** 1st ed. United States of America: Jones and Bartlett Publishers, Inc.

Negnevitsky, Michael. (2005). **Artificial Intelligence: A Guide to Intelligence System.** 2nd ed. Great Britain: Biddles Ltd, King's Lynn.

สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์,& เลอศักดิ์ ลิ้มวิวัฒน์กุล (เรียบเรียง). (2547) **ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน.** ค้นข้อมูล 20 ธันวาคม 2550, จาก http://www.thaicert.nectec.or.th/paper/authen/authentication_guide.php.

IEEE Xplore. Retrieved September 2, 2007, from http://ieeexplore.ieee.org.

Wikipedia, the free encyclopedia. **Biometrics.** Retrieved November 15, 2007, from http://en.wikipedia.org/wiki/Biometrics.