นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็วและการเข้ารหัสแบบทางเดียว

นางสาวนันทวัน สันทศนะสุวรรณ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาธุรกิจเทคโนโลยีและการจัดการนวัตกรรม (สหสาขาวิชา)
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2554

INNOVATION OF CREDIT CARD CUSTOMER AUTHENTICATION BASED ON QR-CODE AND ONE-WAY ENCRYPTION

MISS NUNTAWAN SANTASANASUWAN

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Technopreneurship and Innovation Management

(Interdisciplinary Program)

Graduate School

Chulalongkorn University

Academic Year 2011

หัวข้อวิทยานิพนธ์	นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็วและการเข้ารหัสแบบทางเดียว
โดย	นางสาวนันทวัน สันทศนะสุวรรณ
สาขาวิชา	ธุรกิจเทคโนโลยีและการจัดการนวัตกรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร. ศุภกานต์ พิมลธเรศ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ศาสตราจารย์ กิตติคุณ ดร.อัจฉรา จันทร์ฉาย

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

…….. คณบดีบัณฑิตวิทยาลัย
(รองศาสตราจารย์ ดร.พรพจน์ เปี่ยมสมบูรณ์)

คณะกรรมการสอบวิทยานิพนธ์

……ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.พงศ์พันธ์ อนันต์วรณิชย์)

……... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร. ศุภกานต์ พิมลธเรศ)

……อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม
(ศาสตราจารย์ กิตติคุณ ดร.อัจฉรา จันทร์ฉาย)

……กรรมการ
(อาจารย์ ดร.วัชรา จันทาทับ)

……กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.สาธิษฐ์ นากกระแสร์)

นันทวัน สันทศนะสุวรรณ: นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็วและการเข้ารหัสแบบทางเดียว. (INNOVATION OF CREDIT CARD CUSTOMER AUTHENTICATION BASED ON QR-CODE AND ONE-WAY ENCRYPTION) อ. ที่ปรึกษาวิทยานิพนธ์หลัก:อ.ดร.ศุภกานต์ พิมลธเรศ, อ. ที่ปรึกษาวิทยานิพนธ์ร่วม : ศ.กิตติคุณ ดร.อัจฉรา จันทร์ฉาย, 135 หน้า.

บัตรเครดิตเป็นบัตรที่ใช้แทนเงินสดเพื่อซื้อสินค้าและรับบริการต่างๆ ซึ่งการโจรกรรมหรือการปลอมแปลงบัตรเครดิตเป็นอาชญากรรมชนิดหนึ่งที่สามารถเกิดขึ้นได้ทุกที่ทุกเวลา ดังนั้นงานวิจัยนี้จึงมีจุดประสงค์เพื่อการศึกษาความต้องการของผู้บริโภคต่อความปลอดภัยในการใช้บัตร การพัฒนานวัตกรรมที่นำเสนอในงานวิจัยนี้ ประกอบด้วยสองส่วนหลัก ส่วนแรกคือการใช้ตัวอ่านคิวอาร์โค้ดเพื่ออ่านภาพที่ถูกแสดงไว้ที่บัตร ส่วนที่สองประกอบด้วยการเข้ารหัสแบบทางเดียวเพื่อยืนยันรหัสผ่านที่ผู้ใช้กำหนดไว้ โดยเมื่อนำเอาทั้งสองส่วนประกอบกันก็จะสามารถยืนยันตัวตนของผู้ใช้ได้ ทำให้การใช้บัตรเครดิตมีความปลอดภัยมากขึ้น จากการทดสอบประสิทธิภาพของนวัตกรรม และการยอมรับของผู้บริโภค พบว่าระบบที่เสนอสามารถใช้งานได้อย่างมีประสิทธิภาพ และผู้บริโภคอยู่ในระดับที่พึงพอใจ

สาขาวิชา ธุรกิจเทคโนโลยีและการจัดการนวัตกรรม ลายมือชื่อนิสิต ……..
ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก……..
ปีการศึกษา .....2554.....ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์ร่วม……

5287184820 : MAJOR TECHNOPRENEURSHIP AND INNOVATION MANAGEMENT
KEYWORDS : Credit Card / QR Code / One-Way Encryption

NUNTAWAN SANTASANASUWAN : INNOVATION OF CREDIT CARD CUSTOMER AUTHENTICATION BASED ON QR-CODE AND ONE-WAY ENCRYPTION. ADVISOR : SUPHAKANT PHIMOLTARES,Ph.D.,
CO-ADVISOR : EMERITUS PROF. ACHARA CHANDRACHAI,Ph.D., 135 pp.

A credit card is used for buying goods and getting services instead of cash. Stealthy and forgery are kinds of credit card crimes that would happen from time to time. The purpose of this research is to study customer's need towards security card usage. The development of innovation proposed in this research consists of two main parts. Firstly, QR Code reader is used for reading the code embedded in a card. The other part is using one way encryption for indentifying user via predefined password. If the results of those two parts are passed, the identity of the user can be confirmed. From the analysis of innovation efficiency and customer response it has been found that the proposed system can be efficiently operated in satisfactory level from users.

Field of Study : Technopreneurship and Innovation Management Student's Signature .....
Advisor's Signature .....
Academic Year : 2011 Co-advisor's Signature .....

กิตติกรรมประกาศ

ขอกราบขอบคุณ อาจารย์ ดร. ศุภกานต์ พิมลธเรศ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และศาสตราจารย์ กิตติคุณ ดร.อัจฉรา จันทร์ฉาย อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ที่คอยช่วยเหลือ และให้คำปรึกษา คำแนะนำต่างๆ ในเรื่องการทำวิจัย จนผลงานออกมาเสร็จสมบูรณ์

ขอกราบขอบคุณ ผู้ช่วยศาสตราจารย์ ดร.พงศ์พันธ์ อนันต์วรณิชย์ อาจารย์ ดร.วัชรา จันทาทับ และผู้ช่วยศาสตราจารย์ ดร.สาธิษฐ์ นากกระแสร์ ที่กรุณามาเป็นกรรมการสอบวิทยานิพนธ์ ช่วยติ-ชม และให้คำแนะนำ ในจัดทำวิทยานิพนธ์เพื่อให้ผลงานออกมาได้อย่างสมบูรณ์

ขอขอบคุณครอบครัว ที่เป็นกำลังใจในวันที่รู้สึกท้อถอย และคอยช่วยเหลือ สนับสนุนในทุกๆเรื่อง

ขอขอบคุณเพื่อนๆทุกคน ที่ให้กำลังใจ และมีส่วนสำคัญที่ทำให้งานนี้ออกมาได้ดี

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคสมัยที่มีการแข่งขันทางธุรกิจสูง และด้วยเทคโนโลยีที่ก้าวหน้าในปัจจุบันทำให้มีเครื่องอำนวยความสะดวกเพื่อตอบสนองความต้องการให้กับมนุษย์หลากหลาย ในด้านการเงินการธนาคารสถาบันการเงินหลายแห่งต่างมีกลยุทธ์และวิธีการในการกำหนดขั้นตอนและรูปแบบในการเพิ่มช่องทางในการให้ความสะดวกแก่ลูกค้าในการทำธุรกรรมทางการเงิน ซึ่งบัตรเครดิตก็เป็นช่องทางหนึ่งที่จะอำนวยความสะดวกในเรื่องการใช้จ่าย ซื้อสินค้าต่างๆ รวมทั้งการชำระค่าบริการโดยที่สถาบันการเงินจะออกบัตรให้ภายใต้ข้อจำกัดในการใช้ เช่น ใช้ซื้อสินค้าตามห้างสรรพสินค้าทั่วไป หรือ ใช้ชำระค่าบริการต่างๆ โดยต้องเป็นกรณีที่เจ้าของบัตรเอง ถือบัตรของตนไปชำระเงินที่แคชเชียร์ โดยไม่ต้องใช้เงินสด การใช้งานส่วนมากมีลักษณะคล้ายกันคือ ใช้งานบัตรเครดิตโดยที่แคชเชียร์จะรูดบัตรตามยอดเงินที่ต้องชำระ และออกสลิปให้เป็นหลักฐานในการใช้จ่าย จากนั้นเจ้าของบัตรลงลายมือชื่อกำกับ แสดงความเป็นเจ้าของ และความรับผิดชอบในการชำระเงิน เมื่อถึงกำหนดเวลา ก็จะมีหนังสือแจ้งการชำระหนี้ให้จ่ายหนี้ตามยอดนั้น

บัตรเครดิตถือได้ว่าเป็นเครื่องมือในการใช้จ่ายซื้อสินค้าแทนเงินสดที่มีจำนวนเพิ่มมากขึ้นทุกปี โดยตั้งแต่ปี พ.ศ. 2550-2553 มียอดการใช้จ่ายผ่านบัตรเครดิตประมาณ 703,910 ล้านบาท และมีแนวโน้มที่จะเพิ่มขึ้นในปี พ.ศ. 2554 ประมาณ 817,550-825,000 ล้านบาท ซึ่งขยายตัวร้อยละ 13.9-14.9 [1] จากรายงานของธนาคารแห่งประเทศไทย พบว่าจำนวนบัตรเครดิตในทุกกลุ่มผู้ประกอบการในเดือนมกราคม – กุมภาพันธ์ ปี พ.ศ. 2554 มีประมาณ 14,247,721 บัตร เติบโตร้อยละ 6.3 เมื่อเทียบกับช่วงเดียวกันของปีก่อน เพิ่มขึ้นจากที่ขยายตัวร้อยละ 5.2 ในปี พ.ศ. 2553 [2] และจากการสำรวจพฤติกรรมการใช้จ่าย และความคิดเห็นเกี่ยวกับหนี้บัตรเครดิตของประชาชนของศูนย์พยากรณ์เศรษฐกิจและธุรกิจ มหาวิทยาลัยหอการค้าไทย โดยได้สอบถามความคิดเห็นของประชาชน จากการสำรวจกลุ่มตัวอย่าง 1,203 ตัวอย่างทั่วประเทศจากกลุ่มผู้ใช้บัตรเครดิต จากการสำรวจพฤติกรรมการใช้จ่าย ตามลักษณะการใช้บัตรนั้น พบว่าจะใช้แทนเงินสดในการซื้อสินค้าคิดเป็นร้อยละ 32.7 ใช้ผ่อนสินค้าร้อยละ 35.6 และใช้เบิกเป็นเงินสดร้อยละ 31.7 และเมื่อสอบถามถึงเหตุผลการใช้บัตรเครดิต พบว่า กลุ่มตัวอย่างส่วนใหญ่จะใช้บัตรเครดิตเพราะได้นำเงินสดที่มีอยู่ไปหมุนใช้ก่อน คิดเป็นร้อยละ 30.8 รองลงมาคือมีความสะดวกในการใช้ ร้อยละ 28.4 ของจำนวนผู้แจกแบบสอบถาม [3] ซึ่งแสดงให้เห็นว่าบัตรเครดิตมีความจำเป็นต่อประชาชนมากขึ้นเรื่อยๆ เนื่องด้วยความสะดวกในการใช้จ่ายนั่นเอง

แต่เนื่องจากสภาพปัญหาสังคมในปัจจุบันเกิดอาชญากรรมหลายรูปแบบ ยิ่งเทคโนโลยีมีความสะดวกมากเท่าใด ก็เป็นเหมือนดาบสองคมที่เพิ่มช่องทางให้มิจฉาชีพมีโอกาสก่อเหตุได้มากเท่านั้น ซึ่งปัจจุบันมีผู้ไม่หวังดี (มิจฉาชีพ) นำบัตรเครดิตที่ได้โดยทุจริตไปใช้ (บัตรเครดิตหาย หรือถูกโจรกรรม) เป็นจำนวนมาก โดยวิธีการปลอมแปลงลายเซ็นเมื่อรูดซื้อสินค้า หรือการใช้เลขหมายบนหน้าบัตรซื้อขายผ่านระบบอินเทอร์เน็ต

จากข้อมูลสถิติการรับแจ้งและจับกุมกลุ่มคดีอาญาทั่วราชอาณาจักร ช่วงปี พ.ศ. 2544-2553 [4] ซึ่งการกระทำผิดเกี่ยวกับบัตรเครดิตจัดอยู่ในกลุ่มการยักยอกทรัพย์ จากตารางที่ 1-1 แสดงให้เห็นว่าการกระทำผิดในกลุ่มการยักยอกทรัพย์ มีการจับกุมผู้กระทำผิดได้มีไม่ถึง ร้อยละ 50 ของยอดที่ได้รับแจ้งความ

ตารางที่ 1-1 ข้อมูลเรื่องการยักยอกทรัพย์

รับแจ้ง										
ยักยอกทรัพย์	2544	2545	2546	2547	2548	2549	2550	2551	2552	2553
	14,733	17,453	11,903	11,386	12,077	12,834	12,993	12,706	11,734	10,764
จับกุม										
ยักยอกทรัพย์	2544	2545	2546	2547	2548	2549	2550	2551	2552	2553
	4,655	5,221	1,581	1,777	1,823	2,751	2,993	2,726	2,882	2,721

ข้อมูลจาก : สถิติการรับแจ้งและจับกุมกลุ่มคดีอาญาที่น่าสนใจ จำแนกตามประเภทคดีที่รับแจ้งทั่วราชอาณาจักร พ.ศ. 2544-2553, สำนักงานตำรวจแห่งชาติ

นอกจากนั้นข้อมูลที่เกี่ยวกับการประทุษร้ายต่อทรัพย์ทั่วราชอาณาจักร พ.ศ.2544-2553 [5] การกระทำผิดเกี่ยวกับบัตรเครดิตจัดอยู่ในกลุ่มของลักทรัพย์ที่มีผลสืบเนื่องมาจากการปลอมแปลงเอกสาร หรือเจตนาลักไปโดยทุจริตทำให้ผู้เสียหายสูญเสียทรัพย์ ดังตารางที่ 1-2

ตารางที่ 1-2 ข้อมูลเรื่องการลักทรัพย์

รับแจ้ง										
ลักทรัพย์	2544	2545	2546	2547	2548	2549	2550	2551	2552	2553
	56,029	57,413	52,988	54,457	60,881	63,649	62,007	57,457	50,412	48,790
จับกุม										
ลักทรัพย์	2544	2545	2546	2547	2548	2549	2550	2551	2552	2553
	27,461	24,992	18,065	18,142	19,427	22,155	24,934	25,150	19,945	21,682

ข้อมูลจาก : สถิติการรับแจ้งและจับกุมกลุ่มคดีประทุษร้ายต่อทรัพย์ จำแนกตามประเภทคดีที่รับแจ้งทั่วราชอาณาจักร พ.ศ. 2544-2553, สำนักงานตำรวจแห่งชาติ

จากตารางที่ 1-2 พบว่าการกระทำผิดในกลุ่มของลักทรัพย์ จำนวนที่รับแจ้งความกับจำนวนที่จับกุมได้มีจำนวนที่ต่างกันอย่างเห็นได้ชัดเช่นเดียวกับตารางที่ 1-1 คือ จำนวนที่จับกุมได้มีอยู่ไม่ถึงครึ่งหนึ่งของจำนวนที่ได้รับการแจ้งความ ดังนั้นการคิดหาทางป้องกันปัญหาจึงเป็นสิ่งที่สำคัญเพื่อที่จะได้ลดความเสี่ยงในการเกิดความเสียหายดังกล่าวได้

นอกจากปัญหาอาชญากรรมที่มีมากขึ้นตามตารางสถิติคดีต่างๆข้างต้น ยังพบว่าบัตรเครดิตยังมีจุดอ่อนของการใช้จ่ายบัตรเครดิตลักษณะต่างๆที่ใช้อยู่ในปัจจุบันอีก เช่น บัตรเครดิตที่ใช้แถบแม่เหล็กในการจัดเก็บข้อมูล จะมีข้อจำกัดในการใช้งานเป็นอย่างมาก เพราะเก็บข้อมูลได้จำนวนน้อย ทั้งยังก่อให้เกิดปัญหาการทุจริตและปลอมแปลงได้ง่าย หรือบัตรเครดิตที่มีการฝังชิพคอมพิวเตอร์ (Computer Chip) ที่เรียกว่า สมาร์ทการ์ด (Smart Card) ก็มีข้อบกพร่องสำคัญคือ การรวมศูนย์ข้อมูลหลายอย่างมากเกินไปจึงเป็นการจูงใจ ผู้ไม่หวังดีอย่างมากที่จะเจาะระบบเอาข้อมูลเอาไปใช้อย่างไม่ถูกต้อง ดังนั้นการศึกษาเรื่องนี้จึงน่าสนใจในการหาหนทางคิดเทคโนโลยีใหม่ๆที่ป้องกันข้อบกพร่องดังกล่าว

การใช้รหัสแถบ 1 มิติ หรือที่เรียกว่า บาร์โค้ด ในการเก็บข้อมูลต่างๆ เช่น รหัสของสินค้านั้นเป็นที่นิยมเป็นอย่างมากเพราะสะดวกในการเก็บข้อมูล ต้นทุนไม่สูงนัก และสามารถใช้กับสินค้าได้หลากหลาย แต่บรรจุข้อมูลได้น้อย ต่อมามีการพัฒนาจึงเกิดรหัสแถบ 2 มิติขึ้น ซึ่งเป็นเทคโนโลยีที่เพิ่มเติมจากรหัสแถบ 1 มิติ มีข้อดีคือ

1. สามารถบรรจุข้อมูลได้ทั้งในแนวตั้งและแนวนอน ทำให้บรรจุข้อมูลได้มากขึ้น ประมาณ 4,000 ตัวอักษร หรือประมาณ 200 เท่าของรหัสแถบ 1 มิติในพื้นที่เท่ากันหรือเล็กกว่า

2. ข้อมูลที่บรรจุในรหัสแถบ 2 มิตินั้น สามารถใช้ภาษาอื่นๆนอกจากภาษาอังกฤษได้ เช่น ภาษาญี่ปุ่น ภาษาจีน ภาษาเกาหลี เป็นต้น

3. แม้ภาพรหัสแถบ 2 มิติบางส่วนจะมีความเสียหาย ก็สามารถถอดรหัส/อ่านค่าได้

4. เครื่องมืออ่านค่าและถอดรหัส รหัสแถบ 2 มิติมีหลากหลาย เช่น เครื่องอ่านแบบซีซีดี เครื่องอ่านแบบเลเซอร์เช่นเดียวกับการอ่านรหัสแถบ 1 มิติ หรือใช้โทรศัพท์มือถือแบบที่มีกล้องถ่ายรูปในตัวและติดตั้งโปรแกรมถอดรหัสไว้ ก็สามารถใช้อ่านและถอดรหัสได้เช่นกัน

5. รูปแบบของรหัสแถบ 2 มิติมีหลายรูปแบบ เช่น วงกลม สี่เหลี่ยมจัตุรัส หรือสี่เหลี่ยมผืนผ้าคล้ายกับรหัสแถบ 1 มิติ ตัวอย่างรหัสแถบ 2 มิติ ได้แก่ PDF417, Maxi Code, Data Matrix และ QR-Code เป็นต้น

รหัสตอบสนองอย่างรวดเร็ว (QR-Code)

เป็นรหัสแถบ 2 มิติ มีลักษณะเป็นรูปสี่เหลี่ยม ปัจจุบันนิยมนำมาใช้ในวงการค้าขายสินค้า การขนส่ง การตลาด เช่น โฆษณา นิตยสาร วารสาร หรือป้ายโฆษณา นอกจากนั้นยังสามารถให้คิวอาร์โค้ด เก็บข้อมูล URLได้ และด้วยความทันสมัยของเทคโนโลยี ยังสามารถติดตั้งซอฟต์แวร์สำหรับอ่านคิวอาร์โค้ดไว้ในโทรศัพท์เคลื่อนที่ได้อีกด้วย เช่น โทรศัพท์สมาร์ทโฟน โดยนำโทรศัพท์ไปถ่ายภาพคิวอาร์โค้ด ก็สามารถอ่านค่า หรือรับข้อมูลจากรหัสได้โดยสะดวก ง่ายดาย ซึ่งตัวคิวอาร์โค้ดนี้สามารถเก็บข้อมูลได้หลากหลายรูปแบบ ตั้งแต่ หมายเลขโทรศัพท์ wap URL web URL หรือไฟล์ข้อมูลต่าง ๆ เป็นต้น [6]

จากความต้องการเพิ่มความปลอดภัยในการใช้บัตรเครดิต รวมถึงความแปลกใหม่ของคิวอาร์โค้ด จึงได้มีแนวความคิดที่จะใช้คิวอาร์โค้ดร่วมกับวิทยาการเข้ารหัสลับ (Cryptography) เพื่อนำมาใช้เพิ่มประสิทธิภาพในการยืนยันตัวตนในการรักษาความปลอดภัยในการใช้บัตรเครดิตให้มากขึ้น

วิทยานิพนธ์ฉบับนี้จะนำคิวอาร์โค้ดมาใช้ร่วมกับขั้นตอนวิธีหนึ่งที่เรียกว่าฟังก์ชันแฮชทางเดียว (One-Way Hash Function) โดยรับข้อมูล M ที่มีขนาดความยาวแปรเปลี่ยนได้ ไปประมวลผลเพื่อให้ได้เป็นรหัสแฮช H (M) ที่มีขนาดคงที่ ฟังก์ชันแฮชดังกล่าวมีประโยชน์มากในการประยุกต์ใช้งานในทางปฏิบัติได้หลากหลาย เช่น การตรวจสอบบูรณภาพของข้อมูล (Message Integrity) หรือการลงลายเซ็นดิจิทัล (Digital Signature) [7] อีกทั้งรหัสแฮชจัดเป็นข้อมูลที่ผ่านการ

เข้ารหัส (Cipher Data) ที่ไม่สามารถถอดรหัสกลับมาเป็นข้อมูลเดิมด้วยวิธีการใด ๆ ได้ จึงเป็นวิทยาการที่มีความปลอดภัยสูง

นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) มีหลักการเบื้องต้นดังนี้

1. สัญลักษณ์รหัสตอบสนองอย่างรวดเร็ว (QR-Code) ถูกแสดงไว้ด้านหลังบัตรแทนแถบแม่เหล็ก และลายเซ็นของผู้ถือบัตรเครดิต ซึ่งเก็บรหัสแฮชจากข้อมูลเบื้องต้นของผู้ถือบัตร โดยข้อมูลดังกล่าวอาจเป็นรหัสผ่าน (Password)

2. ผู้ใช้ทราบรหัสผ่านของตนเองแต่จะไม่ทราบรหัสแฮชและฟังก์ชันแฮชที่ทำให้ได้มาซึ่งรหัสดังกล่าว

3. ธนาคารจะเป็นผู้ใช้ฟังก์ชันแฮชและสร้างรหัสแฮชแล้วบันทึกไว้บนคิวอาร์โค้ด

4. ในการใช้งานแต่ละครั้งซอฟต์แวร์การเข้ารหัสทางเดียวจะแปรเปลี่ยนรหัสผ่านของผู้ถือบัตรเป็นรหัสแฮชเพื่อเปรียบเทียบกับรหัสแฮชที่อ่านได้จากคิวอาร์โค้ด ถ้าแปลงรหัสแล้วตรงกันก็จะสามารถยืนยันความเป็นเจ้าของบัตรได้ แม้ว่าบัตรหายหรือถูกโจรกรรม ตราบใดที่ผู้ไม่หวังดีไม่ทราบรหัสผ่านก็ไม่สามารถสร้างรหัสแฮชที่ถูกต้องได้

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาและพัฒนาวิธีการนำคิวอาร์โค้ดและการเข้ารหัสแบบทางเดียวมาใช้ในการยืนยันตัวตน (Authentication) ของผู้ใช้บริการบัตรเครดิต

2. เพื่อศึกษาศักยภาพของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) เข้าสู่เชิงพาณิชย์

1.3 ขอบเขตของการวิจัย

การวิจัยครั้งนี้ เป็นการวิจัยเชิงทดลอง (Experimental Research) โดยการทดลองสร้างระบบและทดสอบระบบของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) ด้วยการพัฒนาซอฟต์แวร์คอมพิวเตอร์ แล้วนำมาทดสอบประสิทธิภาพในการยืนยันตัวตนผ่านการเข้ารหัสโดยการใช้ฟังก์ชันแฮชเพื่อสร้างรหัสแฮช จากนั้นบันทึกไว้บนรหัสตอบสนองอย่างรวดเร็ว (QR-Code)

ในการใช้งานแต่ละครั้งซอฟต์แวร์การเข้ารหัสทางเดียวจะแปรเปลี่ยนรหัสผ่านของผู้ถือบัตรเป็นรหัสแฮชเพื่อเปรียบเทียบกับรหัสแฮชที่อ่านได้จากคิวอาร์โค้ด ถ้าแปลงรหัสแล้วตรงกันก็จะสามารถยืนยันความเป็นเจ้าของบัตรได้ โดยมีรายละเอียดด้านเทคโนโลยีได้แก่

1. การอ่านค่าจากคิวอาร์โค้ด ใช้โปรแกรมสำเร็จรูปแบบเดียวกับของโทรศัพท์เคลื่อนที่
2. ขั้นตอนวิธีการเข้ารหัสทางเดียวพัฒนาบนเครื่องคอมพิวเตอร์
3. ฟังก์ชันในการเข้ารหัสตั้งอยู่บนพื้นฐานของฟังก์ชันแฮช และใช้เพียงรูปแบบเดียว
4. การทดสอบทำบนบัตรเสมือนที่มีโครงสร้างทางกายภาพใกล้เคียงกับบัตรเครดิตจริง

การวิจัยเชิงปริมาณ (Quantitative Research)โดยการวิจัยเชิงสำรวจ (Survey Research Method) รวมทั้งวิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) และใช้การเก็บข้อมูลด้วยแบบสอบถาม (Questionnaire) เพื่อวิจัยใน 2 ส่วน คือ 1. การสำรวจความต้องการในนวัตกรรมการป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต และ 2. การยอมรับระบบการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตเพื่อป้องกันการปลอมแปลงบัตรเครดิต มาหาแนวทางในการนำนวัตกรรมสู่เชิงพาณิชย์ รวมถึงความเป็นไปได้ทางธุรกิจ (ความคุ้มค่าทางด้านการลงทุน ความคาดหวังถึงกำไร แนวโน้มด้านการตลาด กลุ่มของลูกค้าที่ใช้บริการ สมมติฐานสำหรับการวิจัยและพัฒนา)

1.4 คำจำกัดความที่ใช้ในการวิจัย

นวัตกรรม หรือ **Innovation** หมายถึง แนวความคิด การปฏิบัติ หรือวิธีการปฏิบัติใหม่ๆ ที่ยังไม่เคยมีใครเคยทำมาก่อน หรืออาจเป็นการดัดแปลงสิ่งเดิม วิธีการเดิมที่มีอยู่มาพัฒนาให้ดีขึ้น เช่น การสร้างตลาดใหม่ ผลิตภัณฑ์ใหม่ กระบวนการ และการบริการใหม่ หรือการกระทำในสิ่งที่แตกต่างจากคนอื่นโดยมองการเปลี่ยนแปลงของสิ่งแวดล้อมที่เกิดขึ้นให้กลายมาเป็นโอกาส และพัฒนาไปสู่แนวความคิดใหม่ที่ทำให้เกิดประโยชน์ต่อตนเองและสังคม

บัตรเครดิต (Credit Card) คือ บัตรที่ธนาคารพาณิชย์หรือสถาบันผู้ออกบัตรต่างๆ ออกให้แก่ผู้ถือบัตรตามหลักเกณฑ์และวิธีการที่ธนาคารพาณิชย์หรือสถาบัน ผู้ออกบัตรกำหนดไว้ เพื่อใช้ชำระค่าสินค้า และบริการแทนการชำระด้วยเงินสด หรือเบิกถอนเงินสดได้ตามวงเงินที่กำหนดไว้

รหัสตอบสนองอย่างรวดเร็ว  **หรือคิวอาร์โค้ด (QR-Code)** เป็นรหัสแถบ 2 มิติชนิดหนึ่งที่มีไว้เก็บข้อมูล คล้ายกับรหัสแถบ (Bar Code) โดยมีลักษณะเป็นรูปสี่เหลี่ยม มีเอกลักษณ์เฉพาะตัว โดยมากนิยมใช้เก็บข้อมูลต่างๆของสินค้า เช่น ชื่อสินค้า ราคา เบอร์โทรศัพท์ติดต่อ หรือข้อมูล URL เพื่อเชื่อมต่อไปยังเว็บไซต์ต่างๆ

ฟังก์ชันแฮช (Hash Function) คือ ขั้นตอนวิธี (Algorithm) ที่รับข้อมูล M ที่มีขนาดความยาวแปรเปลี่ยนได้ ไปประมวลผลเพื่อให้ได้เป็นรหัสแฮช H(M) หรือ รหัสแฮช ฟังก์ชันแฮชเป็นฟังก์ชันแบบทางเดียวซึ่งไม่สามารถหาฟังก์ชันผกผันได้ ดังนั้นรหัสที่ได้จากฟังก์ชันแฮชจะไม่สามารถนำมาใช้ในการเรียกคืนรหัสดั้งเดิมกลับมาได้

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ต่อการใช้งาน

1. สามารถนำนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) ไปใช้งานได้จริง
2. ทราบแนวทางในการนำผลิตภัณฑ์นวัตกรรมนี้เข้าสู่ในเชิงพาณิชย์ได้

ประโยชน์ต่อการศึกษา

เป็นนวัตกรรมด้านการประยุกต์ระบบการยืนยันตัวตนด้วยรหัสตอบสนองอย่างรวดเร็วและวิธีการเข้ารหัสแบบทางเดียวสามารถนำไปปรับใช้กับการทำงานด้านบัตรเครดิต

1.6 ระยะเวลาในการดำเนินงาน

ตารางที่ 1-3 ระยะเวลาในการดำเนินงาน

	2553				2554				
กิจกรรม	พค.-มิย.	กค.-สค.	กย.-ตค.	พย.-ธค.	มค.-กพ.	มีค.-เมย.	พค.-มิย.	กค.-สค.	กย.-ตค.
ศึกษาหลักการทฤษฎีและทฤษฎีพื้นฐาน									
ศึกษางานวิจัยที่เกี่ยวข้อง									
รวบรวมข้อมูล									
พัฒนาระบบ									
ทดสอบคุณสมบัติทางเทคนิคของระบบ									
ทดสอบตลาด									
วิเคราะห์ผลการทดสอบ									
วางแผนกลยุทธ์ในการนำนวัตกรรมออกสู่เชิงพาณิชย์									
สรุปผลและข้อเสนอแนะ									
จัดทำรูปเล่มวิทยานิพนธ์ฉบับสมบูรณ์									

งานวิจัยฉบับนี้ประกอบด้วยหกบท โดยในบทถัดไปจะอธิบายถึงเอกสารและงานวิจัยที่เกี่ยวข้อง บทที่สามแสดงวิธีดำเนินการวิจัย บทที่สี่แสดงผลการวิเคราะห์ข้อมูล บทที่ห้าแสดงการศึกษาความเป็นไปได้ของผลิตภัณฑ์ในเชิงธุรกิจ และบทสุดท้ายคือสรุปผลการศึกษาและข้อเสนอแนะ

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

2.1.1 ทฤษฎีทัศนคติของผู้บริโภค

ทัศนคติถือได้ว่าเป็นตัวแปรหนึ่งในกระบวนการตัดสินใจของผู้บริโภค ซึ่งเกิดจากการเรียนรู้และการมีปฏิกิริยาโต้ตอบกัน (Interaction) ระหว่างผู้บริโภคกับสิ่งอื่น หรือคนอื่นๆ โดยคำจำกัดความและคำอธิบายของนักวิชาการหลายคนได้แสดงออกมาหลายอย่างและมีการขัดแย้งกันในด้านความเห็นซึ่งก็ยังหาข้อยุติไม่ได้ แต่โดยรวมแล้วกล่าวถึงแนวโน้มที่จะก่อปฏิกิริยาตอบต่อสิ่งใดสิ่งหนึ่ง ทัศนคตินั้นเมื่อเกิดขึ้นแล้วเปลี่ยนแปลงได้ยากและไม่อาจทำนายพฤติกรรมได้อย่างถูกต้องเสมอไป ดังนั้นถ้าผู้บริโภคมีทัศนคติในทางลบต่อสินค้า หรือบริการใดๆก็ตาม การจะทำการตลาดเพื่อที่จะเปลี่ยนแปลงพฤติกรรมก็จะยากไปด้วย

องค์ประกอบต่าง ๆ ของทัศนคติ (Components of Attitude)

Del I. Hawkins และคณะ[8] กล่าวว่าการศึกษาเรื่องทัศนคตินั้นจะเป็นแนวคิดที่มีประโยชน์มากทางด้านการตลาด จากการศึกษาพบว่าทัศนคติประกอบด้วยองค์ประกอบ 3 ประการ คือ

(1) ส่วนที่เกี่ยวกับความรู้ ความเข้าใจ หรือความเชื่อ (The Cognitive Component) คือ ความรู้และการรับรู้ที่แต่ละบุคคลมีโดยการผสมผสานของประสบการณ์โดยตรงกับทัศนคติที่มีต่อวัตถุที่เป็นเป้าหมาย และข่าวสารจากแหล่งต่างๆ ความรู้นี้เป็นผลทำให้เกิดการรับรู้ในรูปความเชื่อและนำไปสู่การแสดงออกถึงพฤติกรรมต่างๆ

(2) ส่วนที่เกี่ยวกับความชอบ อารมณ์ และ ความรู้สึก (Affective Component) อารมณ์หรือความรู้สึกที่มีต่อสินค้าหรือตราสินค้า โดยอารมณ์และความรู้สึกเหล่านี้ จะเป็นองค์ประกอบสำคัญเกี่ยวกับการประเมินวัตถุที่เป็นเป้าหมายของทัศนคติ คือ บุคคลจะพิจารณาหรือแสดงทัศนคติเกี่ยวกับวัตถุที่เป็นเป้าหมายว่าชอบหรือไม่ชอบ โดยมีประสบการณ์ทางด้านความรู้สึกต่อสิ่งนั้นแสดงออกมาร่วมด้วย เช่น สภาวะทางด้านอารมณ์ ความสุข ความเศร้า ความอาย ความโกรธ ความโศกเศร้า ความผิดหวัง ความประหลาดใจ ซึ่งสภาพทางอารมณ์อาจเพิ่มขึ้นหรือขยายประสบการณ์ในทางบวกหรือลบตามสิ่งแวดล้อมที่มากระทบภายหลังได้

(3) ส่วนที่เกี่ยวกับองค์ประกอบด้านพฤติกรรม (Behavioral Component) คือ การตั้งใจที่จะประพฤติในทางใดทางหนึ่งนั้นมีรากฐานมาจากความรู้สึกเฉพาะเจาะจงของบุคคล และบุคคลิกส่วนตัว ความเคยชินที่จะเป็นแนวทางในการเลือกที่จะคิดและทำสิ่งใดก็ตาม

แหล่งที่มีอิทธิพลต่อการก่อตัวของทัศนคติ

(1) ประสบการณ์ของบุคคล (Personal Experience) เกิดจากการสะสมความรู้ของบุคคล ความปรารถนาที่ตนมีอยู่ ซึ่งบุคลิกภาพที่ผู้บริโภคได้พัฒนาขึ้นมาด้วยตัวเองกระทบต่อทัศนคติที่จะเกิดขึ้น รวมทั้งความน่าเชื่อถือของข่าวสารที่ผู้บริโภคสะสมมาก็มีอิทธิพลต่อการก่อตัวของทัศนคติได้

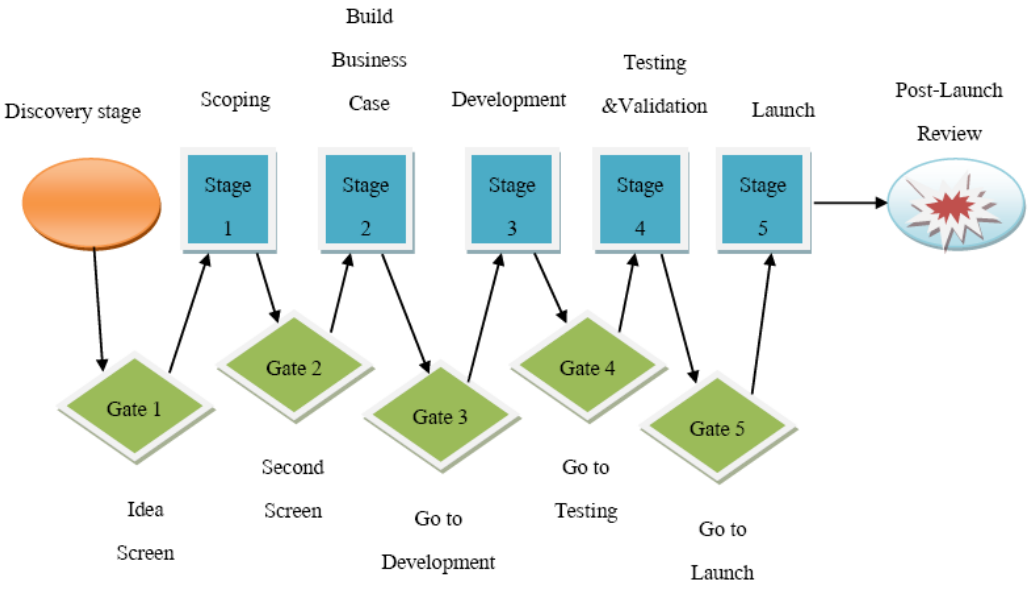
(2) อิทธิพลจากแหล่งภายนอก (External Authorities)

ทัศนคติส่วนใหญ่มักจะเกิดขึ้นโดยได้รับรับอิทธิพลจากภายนอก เช่น เพื่อน อาจารย์ บิดามารดา ญาติ เพื่อนร่วมงานและสื่อต่างๆ นอกจากนั้นผลจากวัฒนธรรมที่มีในสังคมก็สามารถก่อให้เกิดทัศนคติได้เรียกว่า สิ่งแวดล้อมทางวัฒนธรรม โดยขนบธรรมเนียมประเพณีที่เกี่ยวข้องกับสังคมจะทำให้เกิดเป็นทัศนคติที่มีต่อสถานการณ์นั้นได้

2.1.2 แนวคิดในการกำหนดขั้นตอนในกระบวนการพัฒนาผลิตภัณฑ์ใหม่ (New Product Development)

<u>แนวความคิดของคูเปอร์</u>

คูเปอร์[9] ได้เสนอแนวความคิดเกี่ยวกับกระบวนการพัฒนาผลิตภัณฑ์ใหม่ที่เรียกว่า “Stage-Gate TM Model” ซึ่งแบ่งกระบวนการพัฒนาผลิตภัณฑ์ใหม่ออกเป็นระบบที่ประกอบด้วยกระบวนการ 5 ขั้น (Stage) และ 5 ด่าน (Gate) เพื่อใช้เป็นตัวประเมิน 5 ครั้ง ดังภาพที่ 2-1



ภาพที่ 2-1 กระบวนการพัฒนาผลิตภัณฑ์ใหม่

ที่มา : Robert G. Cooper, 1990

โดยจุดเริ่มต้นเกิดจากการค้นพบแนวความคิดใหม่ (Discovery) ซึ่งแนวความคิดใหม่ นี้จะถูกนำเข้าสู่ Gate 1 (Idea Screen) เพื่อเป็นการกลั่นกรองเบื้องต้นก่อนว่าแนวความคิดดังกล่าวสมควรที่จะได้รับการสนับสนุนทางด้านการเงิน บุคลากร และอื่น ๆ จากบริษัทเพื่อเข้าสู่กระบวนการขั้นต่อไปหรือไม่ การพิจารณาครั้งแรกนี้ใช้เวลาไม่นานนัก และถ้าผ่านการพิจารณาแนวความคิดดังกล่าวก็จะได้รับการกลั่นกรองอีกเป็นครั้งที่ 2

Gate 2 (Second Screen) จะมีการวิเคราะห์ความคุ้มค่าทางธุรกิจในการนำแนวความคิดดังกล่าวไปพัฒนาต่อเป็นผลิตภัณฑ์ใหม่ ถ้าผ่านการพิจารณาในด้านที่ 2 ก็จะนำแนวคิดมาพิจารณาต่อ

Gate 3 การนำไปพัฒนา (Go to Development) ใน Gate นี้จะมีการนำแนวคิดมาพัฒนาให้เป็น“ผลิตภัณฑ์ต้นแบบ (Prototype) เพื่อที่จะสามารถทดสอบได้ว่า ผลิตภัณฑ์ดังกล่าวมีคุณสมบัติตรงตามแผนการพัฒนาผลิตภัณฑ์ที่กำหนดไว้หรือไม่

Gate 4 (Go to Testing) จะเป็นการทดสอบผลิตภัณฑ์โดยผู้วิจัย และผู้บริโภคว่าคุณสมบัติและผลการใช้งานผลิตภัณฑ์นั้นตรงตามที่ต้องการหรือไม่ นอกจากนั้นยังอาจมีการทดสอบตลาด (Test Market) ของผลิตภัณฑ์ดังกล่าวด้วยเพื่อให้ทราบถึงผลตอบรับของผู้บริโภคต่อผลิตภัณฑ์นั้นๆ

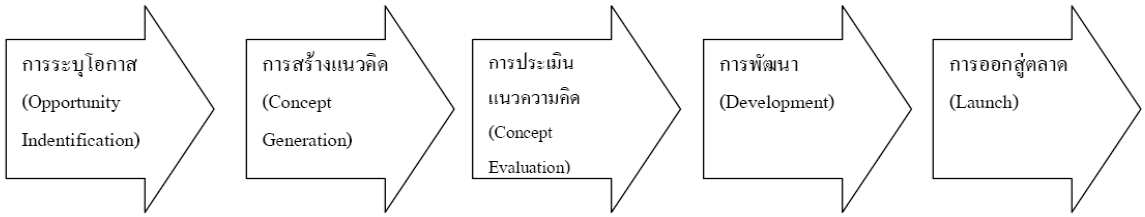
รวมทั้งมีการวิเคราะห์ทางธุรกิจและด้านการเงิน เกี่ยวกับต้นทุนและรายได้จากข้อมูลล่าสุดที่ได้จากการทดสอบตลาดด้วย

Gate 5 คือ การนำผลิตภัณฑ์ออกสู่ตลาด (Go to Launch) คือนำผลิตภัณฑ์ออกสู่ตลาดตามแผนการผลิต และการดำเนินงานที่ได้วางแผนกำหนดไว้ก่อนหน้านี้ ซึ่งจะต้องคำนึงถึงเรื่องทรัพยากรที่จะมารองรับอย่างเพียงพอด้วย

เมื่อผลิตภัณฑ์ออกสู่ตลาดแล้ว ก็จะต้องมีการทบทวนผลการดำเนินงานต่อผลิตภัณฑ์ใหม่หลังจากการนำผลิตภัณฑ์ออกสู่ตลาดเป็นระยะเวลานานพอสมควรแล้ว ซึ่งช่วงเวลานี้ผลิตภัณฑ์ได้เปลี่ยนสถานะจากผลิตภัณฑ์ใหม่มาเป็นผลิตภัณฑ์ปกติของกิจการแล้วว่าเป็นอย่างไร โดยขั้นตอนนี้ถือว่าเป็นขั้นตอนสุดท้ายของกระบวนการพัฒนาผลิตภัณฑ์

<u>แนวความคิดของ ครอว์ฟอร์ด และไค เบเนเดตโท (Merle Crawford and Anthony Di Benedetto)</u>

ครอว์ฟอร์ดและไค เบเนเดตโท [10] แบ่งกระบวนการพัฒนาผลิตภัณฑ์ใหม่ออกเป็น 5 ขั้นตอนดังภาพที่ 2-2



ภาพที่ 2-2 กระบวนการพัฒนาผลิตภัณฑ์ใหม่ตามความคิดของครอว์ฟอร์ดและไค เบเนเดตโท

ที่มา: Merle Crawford and Anthony Di Benedetto, 2008

ซึ่งมีรายละเอียดดังนี้

1. การระบุโอกาส คือ การหาข้อมูล และแนวคิดต่างๆ เพื่อดูโอกาส ความเป็นไปได้ในการพัฒนาผลิตภัณฑ์ รวมทั้งการรองรับทางการตลาด

2. การสร้างแนวคิด คือ การนำข้อมูล องค์ความรู้ต่างๆที่ศึกษา นำมาสร้างเป็นแนวความคิดใหม่ในการคิดพัฒนาผลิตภัณฑ์

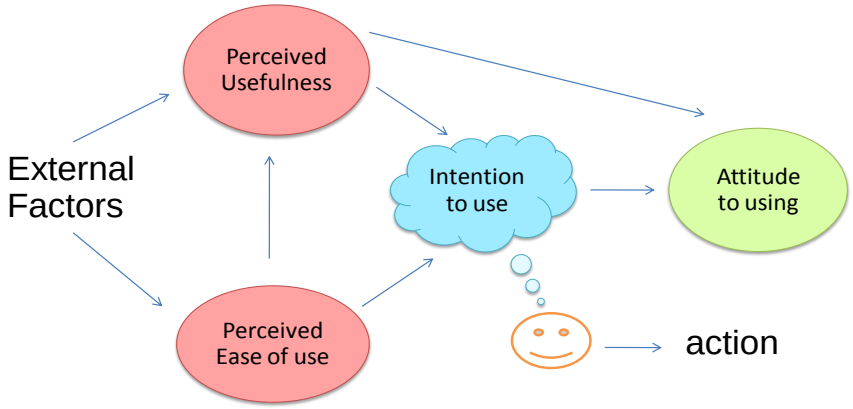
3. การประเมินแนวความคิด คือ การประเมินแนวความคิดนั้นว่ามีโอกาสพัฒนามากน้อยแค่ไหน ตรงตามกับที่คาดการณ์ไว้หรือไม่ โดยอาจจะใช้เครื่องต่างๆในการช่วยประเมินแนวความคิดนั้น เพื่อนำมาปรับปรุง หรือแก้ไขข้อบกพร่อง ก่อนที่จะพัฒนาเป็นผลิตภัณฑ์ต่อไป

4. การพัฒนา คือ การพัฒนาผลิตภัณฑ์ตามแนวความคิดที่ได้ตั้งไว้

5. การออกสู่ตลาด คือ การนำผลิตภัณฑ์ออกสู่ตลาด

2.1.3 ทฤษฎีแบบจำลองการยอมรับทางเทคโนโลยี (Technology Acceptance Model : TAM)

แบบจำลองการยอมรับเทคโนโลยีถูกสร้างขึ้นโดย เดวิส (Davis) [11] ซึ่งเป็นทฤษฎีที่แสดงรูปแบบของผู้ใช้ว่าทำอย่างไรจึงมีการยอมรับ และใช้เทคโนโลยีนั้น โดยดูจากปัจจัยที่สำคัญ 2 ส่วน คือ 1. การรับรู้ถึงประโยชน์ (Perceived Usefulness (PU)) และ 2. การรับรู้ถึงความง่ายในการใช้ (Perceived Ease-of-use (PEOU)) โดยพียู จะนำมาใช้หาระดับความเชื่อของบุคคลในเรื่องประสิทธิภาพของเทคโนโลยี และ พีอีโอยู จะนำมาใช้หาระดับความเชื่อของบุคคลในเรื่องของความง่ายในการรับรู้ ความเข้าใจในเทคโนโลยี ดังภาพที่ 2-3 โดยในงานวิจัยนี้จะใช้วิธีตามแบบจำลองการยอมรับเทคโนโลยี โดยดูความสัมพันธ์ระหว่างการรับรู้ถึงความง่ายในการใช้ระบบใหม่และการรับรู้ถึงประโยชน์และความตั้งใจที่จะใช้เทคโนโลยี



ภาพที่ 2-3 แบบจำลองการยอมรับเทคโนโลยี (TAM)

ที่มา: Davis, 1989

จากแนวคิดและทฤษฎีดังกล่าว สามารถนำมาเป็นกรอบแนวคิดการพัฒนาผลิตภัณฑ์นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิต และผสมผสานสู่การคิดหาความเป็นไปได้ในการนำนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตมาสู่เชิงพาณิชย์ได้

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 ประวัติของบัตรเครดิต

บัตรเครดิตถือกำเนิดขึ้นในประเทศสหรัฐอเมริกาปี ค.ศ. 1914 (พ.ศ. 2457) โดยบริษัท เยอเนอรัลปิโตรเลียม คอร์ปอเรชั่น ออฟแคลิฟอร์เนีย โดยทำบัตรดังกล่าวให้กับลูกค้า และพนักงานของบริษัท เพื่อนำไปชำระค่าน้ำมัน ในตอนนั้นบัตรเครดิตมีลักษณะเหมือนกับเหรียญโลหะ ในปี ค.ศ.1920 (พ.ศ. 2463) บริษัทที่จำหน่ายน้ำมันได้ออกบัตรในรูปแบบเดียวกันนี้ให้แก่ลูกค้าเพื่อเป็นการอำนวยความสะดวก และต่อมาได้รับความนิยมมาก จึงได้มีการขยายตัวของการนำบัตรเครดิตไปใช้ซื้อสินค้าและบริการอย่างอื่นมากขึ้น

ต่อมาในปี ค.ศ.1950 (พ.ศ.2493) นายแฟรงค์ แมคนามารา (Frank Mc. Namara) นักธุรกิจชาวนิวยอร์ค ได้รับประทานอาหารเย็นที่ภัตตาคารแห่งหนึ่ง แล้วลืมนำกระเป๋าเงินติดตัวไปด้วย จึงไม่มีเงินชำระค่าอาหาร ต้องโทรศัพท์ให้ภรรยานำเงินไปให้ จากเหตุการณ์นี้เองทำให้เกิดความคิดว่าน่าจะมีบัตรพิเศษที่ใช้แทนเงินสดได้ เขาจึงนำความคิดนี้ไปปรึกษากับนายราล์ฟ ชไนเดอร์ (Ralph Schncider) และในที่สุดทั้งสองจึงได้จัดตั้ง บริษัท ไดเนอร์ส คลับ (Diners Club) ออกบัตรเครดิต Diners Club เพื่อใช้ในการซื้อสินค้าและบริการแทนการชำระด้วยเงิน ซึ่งคำว่า Diners นั้นก็มาจากคำว่า Dinner ที่แปลว่า อาหารเย็นนั้นเอง (อ้างถึงใน มนัสวี มาลา [12])

ต่อมาได้มีบริษัทเอกชนอีกหลายบริษัท ได้ออกบัตรเครดิต โดยในปี พ.ศ.2501 บริษัท อเมริกันเอ็กซ์เพรส จำกัด ได้ออกบัตรเครดิต อเมริกัน เอ็กซ์เพรส และต่อมาใน พ.ศ.2502 ธนาคารแห่งอเมริกา (Bank of America) ออกบัตรเครดิต ชื่อ Bank Americard ซึ่งต่อมาเปลี่ยนชื่อเป็น Visa Card (อ้างถึงใน เมลดา วงษ์วิกิจการ [13]) จากนั้นปีพ.ศ. 2509 ธนาคารในแถบตะวันออกของสหรัฐฯ ได้ร่วมกับเวลล์ฟาร์โก ได้ออกบัตรเครดิตชื่อ Master Charge ซึ่งต่อมา เปลี่ยนเป็น Master Card ในปัจจุบัน [14]

สำหรับประเทศไทย เริ่มมีการใช้บัตรเครดิตครั้งแรก [15] เมื่อปี พ.ศ. 2512 (ค.ศ.1969) ผู้ออกบัตรคือ บริษัท บัตรไดเนอร์ส คลับ (ประเทศไทย) จำกัด แต่ไม่ได้รับความสนใจเท่าที่ควร

ปี พ.ศ. 2513 ธนาคารแห่งอเมริกา ได้นำบัตรเครดิตของต่างประเทศ ที่เรียกว่า Bank Americard หรือที่รู้จักกันในขณะนี้ว่า วีซ่า (Visa) เข้ามาใช้ในประเทศไทย

และข้อมูลจากธนาคารกสิกรไทย [16] และแหล่งอ้างอิงอื่นๆ ได้กล่าวว่า

ปี พ.ศ. 2515 ธนาคารกสิกรไทย ได้ร่วมกับธนาคารศรีนคร จำกัด ออกบัตรชื่อ “บัตรเครดิตเอนกประสงค์” ซึ่งถือว่าเป็นบัตรเครดิตบัตรแรกที่ออกโดยธนาคารของประเทศไทย

ปี พ.ศ. 2516 ธนาคารกสิกรไทย ได้ให้บริการบัตรเครดิต ซึ่งถือเป็นธนาคารแห่งแรกในประเทศไทย โดยใช้ชื่อว่า บัตรเครดิตอเนกประสงค์ ที่บริการถอนเงินสดอัตโนมัติ จากเครื่องจ่ายเงิน (ATM) 24 ชั่วโมง และนับเป็นต้นแบบของการให้บริการเอทีเอ็มที่แพร่หลายในปัจจุบัน

ปี พ.ศ. 2517 ธนาคารกสิกรไทย ได้รับสิทธิให้เป็นตัวแทน (Franchisee) ในการออกบัตรมาสเตอร์ การ์ด (Master Card) ซึ่งเป็นบัตรเครดิตต่างประเทศให้เผยแพร่ในประเทศไทย

ปี พ.ศ. 2521 ธนาคารกสิกรไทย ได้ออกบัตรเครดิตของตนเอง เรียกชื่อ บัตรเครดิตธนาคารกสิกรไทย

ปี พ.ศ. 2522 ธนาคารกสิกรไทย ได้เข้าเป็นสมาชิกของ วีซ่าอินเตอร์เนชั่นแนล (Visa International) และเป็นผู้ได้รับสิทธิในการเป็นผู้แทน (Franchisee) ออกบัตรเครดิต วีซ่า (Visa) ในประเทศไทย

ปี พ.ศ. 2533 ธนาคารศรีนครได้ร่วมกับธนาคารอื่น ๆ อีก 5 ธนาคาร คือ ธนาคารกรุงเทพพาณิชย์การ ธนาคารทหารไทย ธนาคารนครหลวงไทย ธนาคารมหานคร และสหธนาคาร ออกบัตรภายในประเทศชื่อว่า บัตรเครดิตขวัญนคร นอกจากนั้นธนาคารกรุงไทยก็ได้ออกบัตรเครดิตชื่อว่า บัตรเครดิตกรุงไทย มาเป็นส่วนแบ่งกับบัตรต่าง ๆ (อ้างถึงใน มนัสวี มาลา [12]) นอกจากนั้นก็ยังมีบัตรวีซ่าพระอาทิตย์ ที่ออกโดยธนาคารกรุงไทย และมีสิทธิประโยชน์มากกว่าโดยใช้เป็นบัตรเครดิตที่ใช้ได้ทั่วโลก

ช่วงปี พ.ศ. 2534 เป็นต้นไป ธนาคารต่างๆได้ร่วมมือกับองค์กร กลุ่มบริษัท ห้างสรรพสินค้า ออกบัตรเครดิตเพื่อใช้ชำระซื้อสินค้า และจ่ายค่าบริการอย่างแพร่หลาย และสร้างนวัตกรรมใหม่ๆให้กับบัตรเครดิตมากขึ้น เช่น

ปี พ.ศ. 2534 ธนาคารไทยพาณิชย์ออกบัตรกอล์ฟการ์ด และได้ร่วมมือกับเครือโรงแรมดุสิตธานีออกบัตรดุสิตการ์ด และร่วมมือกับกลุ่มบริษัทชินวัตรคอมพิวเตอร์ฯ ออกบัตรชินการ์ด

ปี พ.ศ. 2536 ธนาคารกรุงเทพได้ร่วมมือกับห้างสรรพสินค้าเดอะมอลล์ออกบัตร เดอะมอลล์การ์ด นอกจากนี้ธนาคารกรุงเทพยังร่วมกับห้างสรรพสินค้าโรบินสันออกบัตรเครดิต โรบินสันการ์ด

ปี พ.ศ. 2538 ธนาคารกรุงเทพมีโครงการบัตรเครดิต โดยได้เซ็นสัญญากับ Inter Bank Card Associate เพื่อออกบัตรเครดิตมาสเตอร์การ์ด และทั้งหมดนี้เป็นบัตรเครดิตที่ออกโดยสถาบัน

การเงินในประเทศไทย และเป็นที่นิยมใช้กันอย่างแพร่หลายทั้งภายในและต่างประเทศใกล้เคียง เช่น มาเลเซีย สิงคโปร์ อินโดนีเซีย รวมทั้งประเทศลาว และประเทศที่ธนาคารนั้นมีสาขาตั้งอยู่

ปี พ.ศ. 2540 ธนาคารกสิกรไทย เปิดให้บริการบัตรเครดิตสำหรับนิติบุคคล (Corporate Card) เป็นแห่งแรกของไทย

ปี พ.ศ. 2541 บริษัท วีซ่า และมาสเตอร์การ์ด ได้ระดมสมาชิกในเครือธนาคาร และ บริษัททางเทคโนโลยีต่าง ๆ ให้นำ ระบบ SET ไปใช้ ซึ่งเป็นโพรโตคอลรักษาความปลอดภัยในการใช้เครดิตการ์ดผ่านระบบอินเตอร์เน็ต

ปี พ.ศ. 2542 ธนาคารกสิกรไทย ออกบริการบัตรเครดิตวีซ่าแพลทินัม เป็นแห่งแรกของประเทศไทย

ปี พ.ศ. 2543 ธนาคารซิตี้แบงก์ จับมือบริษัท การบินไทย จำกัด (มหาชน) ออกบัตรเครดิตซิตี้แบงก์รอยัล ออร์คิด พลัส แพลตตินั่ม เงิน และทอง [17]

ปี พ.ศ. 2548 ธนาคารกสิกรไทย เริ่มให้บริการบัตรเครดิตติดชิพอัจฉริยะ ซึ่งเป็นมาตรฐานบัตรเครดิตในยุคใหม่

ปี พ.ศ. 2549 ธนาคารกสิกรไทย ออกบัตรเครดิตมาสเตอร์การ์ด แบบชิพ (Chip Card) เป็นสถาบันแรกของประเทศไทย

ปี พ.ศ. 2552 ธนาคารกสิกรไทย ให้บริการบัตรเดบิตแรกของไทยที่สามารถออกแบบรูปหน้าบัตรได้เอง ที่มีชื่อว่า “K-My Debit Card”

ในปัจจุบันนี้ ธนาคารพาณิชย์ของประเทศไทย ต่างผลักดันการให้บริการบัตรเครดิตของตนเองอย่างต่อเนื่อง ซึ่งมีผลให้มีการขยายตัวของปริมาณบัตรเครดิตเพิ่มขึ้นอย่างมาก และมีการแข่งขันกันมากขึ้นด้วย

2.2.2 การทำงานของบัตรเครดิต

เริ่มจากผู้ใช้นำบัตรเครดิตมาซื้อสินค้าและบริการ ตามจำนวนวงเงินที่ธนาคารผู้ออกบัตรอนุมัติ หลังจากผู้ให้บริการ(ร้านค้า)ได้รับบัตรเครดิตแล้ว ก็จะเช็คยอดที่ชำระกับวงเงินที่ทางธนาคารอนุมัติก่อน จากนั้นจึงได้รับรหัสอนุมัติการชำระจากธนาคาร ในสมัยก่อนการรูดบัตรเพื่อชำระเงิน ร้านค้าต้องโทรศัพท์ไปที่ธนาคาร แต่ปัจจุบันมีเครื่องรูดบัตรที่ให้รหัสอนุมัติผ่านการออนไลน์กับธนาคารได้ทันที หรือที่เรียกว่าการชำระเงินด้วยบัตรเครดิตผ่านระบบ Point of Sale (POS) [18] หลังจากที่มีการอนุมัติจากธนาคาร เครื่องจะพิมพ์สลิปออกมาให้ผู้ซื้อเซ็นชื่อเพื่อยืนยันตัวผู้ถือบัตร โดยข้อมูลการชำระเงินนั้นจะถูกส่งผ่านเครื่องรูดบัตรทางวงจรโทรศัพท์ไปตรวจสอบ

ที่ธนาคาร หรือบริษัทบัตรเครดิต ส่วนข้อมูลการสั่งซื้อของสินค้าจะถูกส่งไปเก็บที่เซิร์ฟเวอร์ผ่านทางเครือข่ายคอมพิวเตอร์ของร้านค้า

เมื่อมีการซื้อหรือขายผ่านบัตรเครดิต ผู้ใช้บัตรเครดิตจะแสดงการยอมรับว่าการซื้อขายนั้นได้เกิดขึ้นจริงด้วยการเซ็นชื่อในใบเสร็จ แต่ถ้าเป็นการซื้อขายผ่านอินเทอร์เน็ต ทางธนาคารอาจต้องให้ผู้ใช้กรอก PIN Number และหมายเลขบัตรเครดิต เพื่อเป็นการแสดงความจำนงในการซื้อขาย ปัจจุบันบัตรเครดิตนอกจากจะเป็นที่นิยมในการซื้อสินค้าตามราคาทั่วไปแล้ว ยังนิยมมาใช้ในการซื้อขายผ่านอินเทอร์เน็ตอีกด้วย โดยสามารถสรุปช่องทางการทำงานของบัตรเครดิตได้หลายวิธี [19] คือ

1. ระบบ Point of Sales (POS) เป็นวิธีที่ผู้ถือบัตร นำบัตรไปใช้ที่เคาร์เตอร์บริการ

2. ระบบ Call Center เป็นวิธีที่ผู้ถือบัตร สั่งสินค้าโดยการโทรศัพท์ไปยังศูนย์รับแจ้ง

3. ระบบ Internet Site หรือที่เรียกว่า E-Commerce เป็นวิธีที่ผู้ถือบัตรสั่งสินค้าผ่านทางระบบร้านค้าอินเทอร์เน็ต

4. ระบบ Interactive Voice Response (IVR) เป็นวิธีที่ผู้ถือบัตร สั่งสินค้าโดยการโทรศัพท์ฝากข้อความเสียงเอาไว้เพื่อให้ติดต่อกลับ

5. ระบบ Mobile Phone orders เป็นวิธีที่ผู้ถือบัตรใช้โทรศัพท์ในการสั่งสินค้า และโอนเงินค่าสินค้านั้น

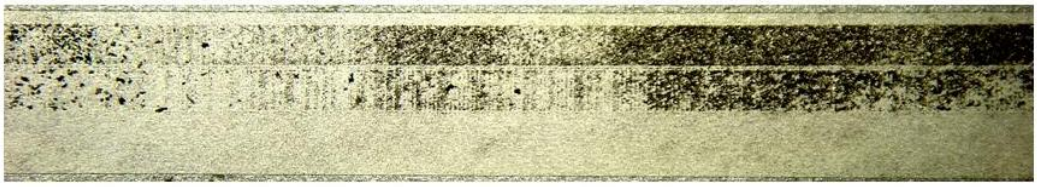
ซึ่งบัตรเครดิตที่ใช้งานในปัจจุบันมีหลายแบบ เช่น

(1) บัตรเครดิตแถบแม่เหล็ก (Magnetic stripe)

เป็นระบบที่นิยมใช้ในบัตรเครดิตรุ่นแรกๆ โดยบัตรเครดิตแบบแถบแม่เหล็ก จะใช้แถบแม่เหล็กในการบันทึกข้อมูลส่วนตัวของเจ้าของบัตรเครดิต ในลักษณะของรหัสแถบ (Bar Code) ที่ใช้ตาเปล่าไม่สามารถมองเห็นได้ แต่เราสามารถดูรหัสแถบที่ซ่อนอยู่ได้โดยใช้คุณสมบัติทางแม่เหล็กของสารแม่เหล็ก [20] วิธีการคือใช้ผงตะไบเหล็กละเอียดนำมาโรยลงบนรหัสแถบแม่เหล็กของบัตรเครดิต จากนั้นค่อยๆเคาะผงตะไบเหล็กออก ดังภาพที่ 2-4 และ 2-5 จะสามารถเห็นรหัสแถบ (Bar Code) ที่ซ่อนอยู่ได้ ซึ่งเป็นส่วนที่บันทึกข้อมูลส่วนตัวของเจ้าของบัตรเครดิต จากรูปแสดงให้เห็นว่าเส้นแรงแม่เหล็กนั้นสม่ำเสมอและมีขนาดเท่ากันหมด

ภาพที่ 2-4 วิธีการดูรหัสแถบ (Bar Code) ในแถบแม่เหล็ก

ที่มา: วิชาการดอทคอม http://www.vcharkarn.com/vcafe/115937



ภาพที่ 2-5 รหัสแถบ (Bar Code) ในแถบแม่เหล็ก

ที่มา: วิชาการดอทคอม http://www.vcharkarn.com/vcafe/115937

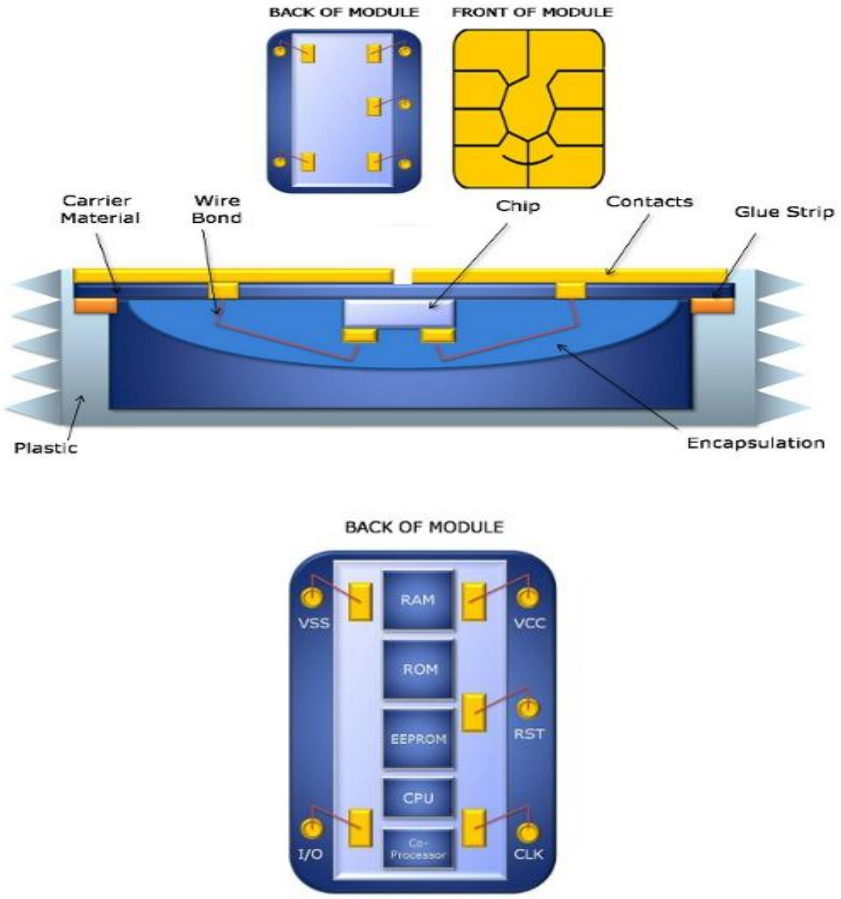
ความแรงของแม่เหล็ก (Coercivity) สังเกตได้จากแถบที่อยู่บนบัตรเครดิต มีสองชนิด คือ 1. แถบชนิดแม่เหล็กแรง 2. แถบชนิดแม่เหล็กอ่อน ซึ่งเครื่องอ่านบัตรเครดิตทั่วไปสามารถอ่านได้ทั้งสองแบบ โดยที่แถบแม่เหล็กอ่อนจะมีข้อเสียมากกว่า คือ เสียความเป็นแม่เหล็กได้ง่าย เช่น ถ้าเข้าไปใกล้แม่เหล็ก หรือเก็บรวมกับแม่เหล็กอื่นๆไม่กี่ครั้งบัตรก็จะเสีย และอ่านบัตรเครดิตนั้นไม่ได้ ส่วนแถบชนิดแม่เหล็กแรงจะสามารถทนได้มากกว่า ซึ่งการที่จะทราบว่าบัตรเครดิตนั้นเป็นแถบแม่เหล็กชนิดใดดูได้จาก แถบชนิดแม่เหล็กแรงมักเป็นสีน้ำตาลเข้มเกือบดำ ส่วนแถบชนิดแม่เหล็กอ่อนมักจะเป็นสีน้ำตาลอ่อน

การทำงานของบัตรเครดิตแบบแถบแม่เหล็กจะอาศัยคุณสมบัติทางแม่เหล็กของสารเหล็กบนแถบแม่เหล็ก การอ่านรหัสจะทำโดยการรูดบัตรผ่านเครื่องที่มีหัวอ่านข้อมูลเหมือนหัวอ่านของเทปบันทึกเสียง ซึ่งส่วนใหญ่เป็นลักษณะของขดลวดเหนี่ยวนำ เมื่อรูดบัตร รหัสแม่เหล็กบนบัตรจะเกิดการเหนี่ยวนำแม่เหล็กเกิดเป็นกระแสไฟฟ้า และถอดรหัสออกมาเป็นแบบ 1 หรือ 0 ตามลักษณะของการอ่านบาร์โค้ด โดยข้อสังเกตได้ว่า ถ้ารูดบัตรช้าๆ จะอ่านข้อมูลบนบัตรไม่ได้ เพราะความเข้มของสนามแม่เหล็กที่ถูกเปลี่ยนแปลง หรือแม่เหล็ก (Flux) ที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง ที่มีต่อหัวอ่านขดลวดมีไม่มากพอทำให้เกิดกระแสไฟฟ้าที่เป็นแปลงเป็นรหัสได้

บัตรเครดิตที่ใช้แถบแม่เหล็กในการจัดเก็บข้อมูล เป็นเทคโนโลยีที่ง่าย และมีความทนทานพอสมควร แต่ในการใช้งานจะมีข้อจำกัดอย่างมาก เพราะเก็บข้อมูลได้น้อย และมีปัญหาการทุจริตและการปลอมแปลงได้ง่าย [21]

(2) บัตรเครดิตฝังชิพคอมพิวเตอร์ (Computer Chip) หรือ Smart Card

บัตรเครดิตที่มีการฝังชิพคอมพิวเตอร์ หรือเรียกว่า สมาร์ทการ์ด คือ การฝังแผ่นไมโครชิพ (Microprocessor) และแผงวงจรอิเล็กทรอนิกส์ แบบวงจรรวม (Integrated Circuit) ลงบนตัวบัตร และมีเทคนิคในการเขียนข้อมูล และการอ่านที่ซับซ้อนมากขึ้นกว่าแบบแถบแม่เหล็ก สามารถเก็บรหัสลับและข้อมูลทางชีวภาพบางอย่างได้ เช่น ลายพิมพ์นิ้วมือ หรือรูปภาพ เป็นการเพิ่มความปลอดภัยของข้อมูลในบัตรได้สูงกว่า ทั้งยังสามารถนำมาใช้ประโยชน์ในด้านอื่นๆได้มากขึ้นกว่าเดิม (Multi-Applications in A Single Card) [22]



ภาพที่ 2-6 ส่วนประกอบของสมาร์ทการ์ด

ที่มา: http://www.ecebs.com/what-is-a-smart-card-a220

จากรูปภาพตัดขวางของบัตรสมาร์ทการ์ดแสดงให้เห็นส่วนประกอบทางกายภาพของสมาร์ทการ์ด และส่วนที่เป็นส่วนประกอบหลักๆของตัวชิพ [22] คือ

CPU ที่เรียกได้ว่าเป็นสมองสั่งการของชิพ

Memory สำหรับเก็บข้อมูล

Interface Pads ส่วนที่นำเข้าข้อมูล และควบคุมการทำงานของชิพ

สมาร์ทการ์ดสามารถแบ่งได้หลายประเภท เช่น

(2.1) ตามคุณสมบัติการใช้งาน แบ่งเป็น

- บัตรโปรแกรมการใช้งานเดียว (Single Application Card) คือบรรจุรหัส (Code) เพื่อการใช้งานเฉพาะด้านใดด้านหนึ่ง เช่น บัตรโทรศัพท์
- บัตรโปรแกรมการใช้งานหลายอย่าง (Multi-Application Card) คือ บรรจุชิพ (Chip) ระบบการทำงานที่ใช้งานได้หลายด้าน เช่น ระบบบัตรเครดิตที่สามารถสะสมแต้มการใช้จ่ายได้

(2.2) ตามชนิดของบัตร แบ่งเป็น

- สมาร์ทการ์ดแบบมีการสัมผัส (Contact Smart Cards) [23] คือ บัตรที่ผนึกชิพทองขนาดเล็กไว้ที่ด้านหน้าของบัตร แทนการใช้แถบแม่เหล็ก (Magnetic stripe) ใช้งานโดยการสอดใส่บัตรเข้าไปในเครื่องอ่านสมาร์ทการ์ด (Smart Card Reader) เมื่อผู้ใช้สอดใส่บัตรเข้าไปในเครื่องอ่านบัตรจะมีการสัมผัสกับหัวต่อ หรือคอนเน็กเตอร์ (Connector) ทางไฟฟ้า ที่จะทำการถ่ายโอนข้อมูลเข้า และออกจากชิพที่ฝังอยู่บนบัตร
- สมาร์ทการ์ดแบบไม่มีการสัมผัส (Contactless Smart Cards) คือ บัตรที่ภายในมีการผนึกชิพคอมพิวเตอร์ และขดลวดสายอากาศไว้ภายใน ใช้งานโดยการวางบัตรให้อยู่ใกล้กับสายอากาศ หรือเครื่องอ่านแบบหน้าสัมผัส ส่วนใหญ่จะใช้ติดต่อกับเครื่องรับ/เครื่องส่งที่อยู่ในระยะไกล เช่นการจัดเก็บค่าผ่านทางด่วน
- ไวร์เลส สมาร์ทการ์ด (Wireless Smart Card) [24] สมาร์ทการ์ด แบบนี้อาศัยคลื่นวิทยุในการติดต่อสื่อสาร การอ่านข้อมูลจากชิพเพื่อไปใช้งานจะผ่านด้วยเครื่องอ่านสมาร์ทการ์ด และสามารถทำงานได้ภายในระยะที่กำหนดเท่านั้น โดยมีชิพเล็กๆสีทอง ใช้เก็บข้อมูลต่างๆ ที่ต้องการ นอกจากนั้นจะมีการฝังชิพอีกตัวหนึ่งเพื่อใช้ติดต่อสื่อสารกับเครื่องอ่านสมาร์ทการ์ด ซึ่งเรียกว่า Radio-frequency Chip หรือบางทีก็เรียกว่า RF Identification หรือ RFID ซึ่งต่อมาได้มีการพัฒนาให้เหลือเพียงชิพ RFID เพียงตัวเดียวแต่สามารถทำงานได้ครบถ้วนเหมือนเดิมทุกประการ

ข้อบกพร่องสำคัญของสมาร์ทการ์ดคือ การรวมศูนย์ข้อมูลหลายอย่างมากเกินไปจึงเป็นการจูงใจ ผู้ไม่หวังดีอย่างมากที่จะเจาะระบบเอาข้อมูลเอาไปใช้อย่างไม่ถูกต้อง ดังนั้นจึงต้องวางระบบป้องกันและรักษาความปลอดภัยข้อมูลส่วนกลางเป็นอย่างดี มิฉะนั้นอาจเกิดความเสียหายกับข้อมูลสำคัญ หรือการเข้าถึงและนำข้อมูลไปใช้โดยผู้ไม่มีสิทธิ เพราะสามารถใส่ข้อมูลของลูกค้าเอาไว้ได้มาก และสามารถบันทึกข้อมูลการใช้จ่ายได้อย่างละเอียดเช่น เมื่อไปซื้อของในร้านค้าและทำการรูดบัตร เครื่องรูดจะถูกออกแบบมาให้อ่านทันทีว่าวงเงินที่สามารถรูดในบัตรได้มีเท่าไหร่แต่ไม่โชว์ให้เห็น ดังนั้นเมื่อรูดเสร็จข้อมูลจะถูกบันทึกอยู่สองทางก็คือบันทึกลงในเครื่องอ่านกับบันทึกลงไปในบัตร แม้เครื่องนั้นจะไม่ต่อกับผู้ออกบัตรอยู่แต่มันก็จะทำการบันทึกและตัดยอดอัตโนมัติ เมื่อไรที่เครื่องออนไลน์มันก็จะส่งข้อมูลนั้นไปที่ผู้ออกบัตร ดังนั้นถ้ามีผู้เจาะระบบเข้าไปได้ ก็จะสามารถรู้ข้อมูลทุกอย่างที่เป็นส่วนตัวของบุคคลนั้นทันที ซึ่งเป็นปัญหาเดียวกับที่กังวลในการใช้เทคโนโลยีนี้ในบัตรประชาชนด้วย

(3) บัตรเครดิตแบบแถบอิเล็กทรอนิกส์ (Electronic Stripe)

เทคโนโลยี Card 2.0 [25] ลักษณะจะเป็นบัตรที่มีความบางเหมือนบัตรเครดิตทั่วไป แต่ทนทานมากกว่า เพราะมีแบตเตอรี่ที่ชาร์จหนึ่งครั้งสามารถใช้งานได้นาน 3 ปี ตามตัวอย่างในภาพที่ 2-7 จะเห็นปุ่มกด 5 ปุ่ม และด้านล่างมีแถบแสดงหมายเลขบัตรแต่จะแสดงหมายเลขบัตรไม่ครบขาดไป 6 ตัว ในการใช้งาน ผู้ใช้จะต้องจำรหัส PIN ที่ใช้กดรหัสจากปุ่มกดทั้ง 5 เพื่อปลดล็อคให้ตัวเลขที่หายไปปรากฏขึ้นมา จึงจะรูดใช้งานได้ หลังจากใช้งานเสร็จแล้ว เมื่อทิ้งไว้สักครู่ตัวเลขจะหายไป และข้อมูลในแถบอิเล็กทรอนิกส์ก็จะถูกลบออกไปด้วย ดังนั้นเมื่อมีการโจรกรรมไปก็ไม่สามารถใช้งานได้

ภาพที่ 2-7 ตัวอย่างบัตรเครดิตด้วยแถบอิเล็กทรอนิกส์
ที่มา: http://www.trueinnovationaward.com

2.2.3 การทุจริตข้อมูลบัตรเครดิต

การทุจริตข้อมูลของมิจฉาชีพมีหลายวิธีเช่น

วิธีที่1 เจาะข้อมูลผ่านระบบอินเทอร์เน็ต และปลอมแปลงหน้าเว็บธนาคาร [26] ด้วยการเจาะไปที่ฐานข้อมูลเว็บไซต์ที่ขายของบนอินเทอร์เน็ต ซึ่งเก็บรวบรวมรหัสบัตรเครดิตของลูกค้า และ ข้อมูลบัตรเครดิตของลูกค้าธนาคารไว้ โดยการส่งอีเมล์ (Email) ปลอมไปยังลูกค้าของธนาคารให้เข้าใจผิดคิดว่าเป็นอีเมล์จากธนาคาร และมีการดัดแปลงชื่อผู้ส่ง(Sender)ให้เป็นอีเมล์แอดเดด (Email Address)ที่มาจากธนาคาร ซึ่งความจริงธนาคารไม่ได้ส่งอีเมล์ดังกล่าว จากนั้นจะทำทีเป็นแจ้งปัญหาในการใช้งานอินเทอร์เน็ตแบงค์กิ้ง(Internet Banking) หรือขอข้อมูลลูกค้าโดยมีจุดมุ่งหมายเพื่อให้เข้าถึงข้อมูลในหน้าเวบเพจ (Web Page) ที่สร้างขึ้นมาให้มีลักษณะเหมือน/ใกล้เคียงกับเวบไซต์ (Website)จริงๆของธนาคาร เมื่อผู้ใช้กรอกรหัสเข้าไปในหน้านั้นแล้ว อาชญากรทางคอมพิวเตอร์ (Hacker)ก็จะได้ชื่อผู้ใช้ และรหัสผ่านในการเข้าระบบของธนาคารเพื่อทำธุรกรรมแทนในนามของผู้ใช้ตัวจริงได้อย่างสะดวก

วิธีที่ 2 การทุจริตโดยการดูดข้อมูลบัตรเครดิตผ่านทางสายโทรศัพท์ [27] ซึ่งในแต่ละครั้งจะสามารถดูดข้อมูลเป็นจำนวนมาก และนำข้อมูลที่ได้มาดัดแปลงเป็นข้อมูลที่ใช้สำหรับปลอมบัตรเครดิตที่แหล่งผลิตบัตรเครดิตปลอม

วิธีที่ 3 การทุจริตทางกายภาพอันเนื่องมาจากการโจรกรรม และการปลอมแปลงลายเซ็น [28] โดยที่ผู้ถือบัตรไม่ได้อนุญาต อาจเกิดได้เมื่อผู้ถือบัตรเครดิตถูกคนร้ายโจรกรรม ทำหล่นหาย ลืมบัตรไว้ที่ร้านค้าที่ไปซื้อสินค้า หรือใช้บริการโดยไม่รู้ตัว และไม่ได้แจ้งอายัดบัตรโดยทันที ทำให้ผู้ไม่หวังดีนำไปใช้ในการทำธุรกรรมในทางทุจริต ได้ทรัพย์สิน เช่น ปลอมแปลงลายเซ็นในสลิปใบเสร็จ

วิธีที่ 4 คือ ทำสำเนาแถบแม่เหล็กบัตรเครดิต [29] โดยเมื่อผู้ใช้บัตรรูดซื้อสินค้าผ่านเครื่องบันทึกข้อมูลหรือ สกิมเมอร์ (Skimmer) ที่ผู้ไม่หวังดีติดตั้งไว้ การสำเนาข้อมูลในแถบแม่เหล็กจากบัตรจริงด้วยเครื่องสกิมมิ่ง(Skimming)นั้น จะทำการคัดลอกและสำเนาข้อมูลในบัตรเครดิตจริงแล้วเก็บข้อมูลดังกล่าวไว้ เพื่อนำไปถ่ายลงหรือทำสำเนาลงในแถบแม่เหล็กในบัตรเครดิตปลอมที่จัดทำขึ้นใหม่ ซึ่งเป็นการกระทำในลักษณะเดียวกันกับการติดตั้งเครื่องสกิมมิ่งที่ตู้ ATM ความเสียหายในลักษณะทำปลอมบัตรเครดิตในลักษณะนี้ ปัจจุบันมีมูลค่าสูงมาก

วิธีที่ 5 การทุจริตจากร้านค้า เช่น ร้านค้าแก้ไขตัวเลขจำนวนเงินในสลิปใบเสร็จ ร้านค้าเจตนารูดบัตรทำรายการหลายครั้ง ทำให้เกิดเป็นยอดการใช้จ่ายเกินจริง และลูกค้าไม่ได้ตรวจสอบเป็นต้น

วิธีที่ 6 กลุ่มมิจฉาชีพทางโทรศัพท์มือถือ [30] เช่น โทรมาแจ้งว่ามีหนี้ค้างชำระในบัตรเครดิตกับทางธนาคาร เมื่อผู้เสียหายปฏิเสธก็จะอ้างถึงการลักลอบขโมยข้อมูล และกลุ่มมิจฉาชีพจะแกล้งช่วยเหลือโดยอ้างว่าจะแจ้งหน่วยงาน กรมสอบสวนคดีพิเศษ (Department Of Special Investigation) หรือ DSI ให้ หลังจากนั้นก็จะมีเจ้าหน้าที่ DSI (กลุ่มมิจฉาชีพ) ติดต่อเข้ามาอ้างตัวและทำทีเป็นสอบสวนเรื่องการทำธุรกรรมทางการเงิน หรือให้บอกข้อมูลทางบัญชี และถ่ายโอนบัญชี จากนั้นจะใช้ข้อมูลทางบัญชีที่ผู้เสียหายบอกไปทำการโจรกรรมเงิน

2.2.4 การรักษาความปลอดภัยของบัตรเครดิต

(1) มาตรการรักษาความปลอดภัยด้านเทคโนโลยี

ใช้กลไกของการพิสูจน์ตัวตน [31](Authentication Mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

สิ่งที่คุณมี (Something You Have) เช่น กุญแจ หรือเครดิตการ์ด เป็นต้น

สิ่งที่คุณรู้ (Something You Know) เช่น รหัสผ่าน (Passwords) หรือการใช้พิน (PIN) เป็นต้น

สิ่งที่คุณเป็น (Something You Are) เช่น ลายนิ้วมือ รูปแบบจอตา (Retinal Patterns) หรือใช้รูปแบบเสียง (Voice Patterns) เป็นต้น

(2) มาตรการรักษาความปลอดภัยด้านพฤติกรรม

สิริพร จิตต์เจริญธรรม เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล [30] ได้เสนอวิธีป้องกันไว้ว่า เมื่อใช้บัตรเครดิตซึ่งบัตรมีรูปแบบคล้ายคลึงกับบัตรเอทีเอ็ม ดังนั้นการป้องกันไม่ให้ตกเป็นเหยื่อของการปลอมแปลงบัตรจึงมีวิธีคล้ายกัน สามารถทำได้ดังนี้

- ผู้ใช้ไม่ควรให้ผู้อื่นนำบัตรเอทีเอ็ม/บัตรเครดิตไปใช้แทน
- สังเกตบริเวณช่องใส่บัตร หากมีความผิดปกติ ไม่ควรใช้
- ขณะป้อนรหัสบัตรเครดิตควรกระทำด้วยความระมัดระวังเพื่อไม่ให้บุคคลที่อยู่ด้านหลังสามารถนำรหัสดังกล่าวไปใช้ หรือปลอมแปลงต่อไปได้

(3) มาตรการรักษาความปลอดภัยทางกฎ/ระเบียบ

มาตรฐาน PCI DSS

มาตรฐาน PCI DSS หรือ Payment Card Industry Data Security Standard [32] เป็นมาตรฐานความปลอดภัยสารสนเทศ จัดตั้งโดยคณะกรรมการ Payment Card Industry Security Standards Council (PCI SSC) ที่เกิดขึ้นจากบริษัท American Express (AMEX), MasterCard, VISA, JCB และ Discover Financial Services เพื่อสร้างมาตรฐานในการให้บริการแก่ผู้ถือบัตรเครดิตให้เกิดความปลอดภัยมากขึ้น ซึ่งมาตรฐานนี้ถูกกำหนดขึ้นเพื่อช่วยองค์กร หรือสถาบันต่างๆ ที่มีการรับชำระเงินด้วยบัตรเครดิต สามารถป้องกันการฉ้อโกงบัตรเครดิตได้ โดยการป้องกันข้อมูลและปิดช่องโหว่ต่างๆ ให้เข้มงวดมากยิ่งขึ้น PCI เริ่มประกาศใช้ตั้งแต่ต้นปี ค.ศ. 2005 (พ.ศ. 2548) ปัจจุบันมาตรฐาน PCI DSS เป็นเวอร์ชั่น 1.2 โดยเน้นไปที่การป้องกันข้อมูลลูกค้า การประมวลผล และการรับส่งข้อมูลของผู้ถือบัตรเครดิตเป็นหลัก

โครงสร้างของมาตรฐาน PCI DSS ประกอบด้วยวัตถุประสงค์การควบคุมในระดับสูง (High Level Control Objectives) ทั้งหมด 6 วัตถุประสงค์ โดยมีข้อกำหนด (Requirement) ให้ผู้ให้บริการบัตรเครดิตปฏิบัติตาม ดังนี้

1. สร้างและป้องกันเครือข่ายให้ปลอดภัย (Build and Secure Network) ผู้ให้บริการบัตรเครดิต ต้องมีการติดตั้งไฟร์วอลล์ในการป้องกันข้อมูลของผู้ถือบัตร และต้องไม่ใช้ชื่อผู้ใช้และรหัสผ่านที่เป็นค่าโดยกำหนด (Default) ที่ถูกกำหนดมาตั้งแต่ตอนเริ่มติดตั้งระบบอย่างเด็ดขาด เพราะอาจถูกโจมตีจากแฮกเกอร์ได้

2. ปกป้องข้อมูลผู้ถือบัตร (Protect Card Holder Data) ผู้ให้บริการบัตรเครดิตต้องมีการป้องกันข้อมูลบัตรที่เก็บอยู่ในวัสดุจัดเก็บข้อมูล เช่น Hard disk หรือ SAN และต้องมีการเข้ารหัสข้อมูลเมื่อมีการส่งผ่านข้อมูลบัตรเครดิตทางระบบเครือข่าย ไม่ว่าจะเป็น การส่งข้อมูลภายในระบบของผู้ให้บริการเอง หรือ การส่งผ่านเครือข่ายสาธารณะ (Public Network) เช่น ระบบอินเทอร์เน็ต เป็นต้น เพื่อป้องกันการขโมยข้อมูล (Eavesdropping, Tapping และ Sniffing)

3. บำรุงรักษาโปรแกรมที่ใช้จัดการกับสิ่งรบกวนข้อมูล (Maintain a Vulnerability Management Program) ผู้ให้บริการบัตรเครดิต ต้องมีการติดตั้งโปรแกรมในการป้องกัน Malware และ Virus ต่าง ๆ และควร Update Virus Signature อย่างสม่ำเสมอ นอกจากนั้นต้องติดตั้งระบบ VM (Vulnerability Management) ในการตรวจสอบช่องโหว่ของระบบอย่างต่อเนื่อง

4. ควบคุมการเข้าถึงข้อมูลโดยใช้มาตรการที่รัดกุม (Implement Strong Access Control Measures) ผู้ให้บริการบัตรเครดิต ต้องจำกัดการเข้าถึงข้อมูลของบัตรเครดิต เฉพาะผู้ที่ได้รับ

อนุญาตเท่านั้น และต้องมีการกำหนด User ID ให้กับพนักงานที่มีสิทธิในการเข้าถึงข้อมูลของลูกค้าให้ไม่ซ้ำกัน (Unique User ID) และมีการเก็บประวัติในการเข้าถึงข้อมูลทุกครั้ง รวมถึงการเข้มงวดในเรื่องการเข้าถึงทางกายภาพด้วย (Physical Security)

5. ตรวจตราและทดสอบเครือข่ายต่างๆอย่างสม่ำเสมอ (Regularly Monitor and Test Networks) ผู้ให้บริการบัตรเครดิต ต้องมีการตรวจสอบและคอยเฝ้าระวังการเข้าถึงข้อมูลในระบบเครือข่ายอยู่ตลอดเวลา และต้องมีการทดสอบระดับความปลอดภัยของระบบอย่างสม่ำเสมอโดยทำการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) และทดสอบความเข็งแกร่งของระบบโดยการจำลองเจาะเข้าระบบในลักษณะคล้ายกับการโจมตีของแฮกเกอร์ (Penetration Testing)

6. รักษานโยบายความปลอดภัยสารสนเทศไว้ (Maintain an Information Security Policy) ผู้ให้บริการบัตรเครดิต ต้องมีการกำหนดนโยบายด้านปลอดภัยข้อมูล และมีการกำหนดมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) ขั้นตอนในการปฏิบัติ (Procedure) ตลอดจนมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(4) มาตรการรักษาความปลอดภัยทางกฎหมาย

ประเทศไทยได้ออกกฎหมายกำหนดโทษผู้กระทำผิดเรื่องการปลอมแปลงบัตรเครดิตตามประมวลกฎหมายอาญา [33] ดังนี้

หมวด 3 ความผิดเกี่ยวกับเอกสาร

มาตรา 264 ผู้ใดทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง หรือประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง ผู้นั้นกระทำความผิดฐานปลอมเอกสารต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน หกพันบาท หรือทั้งจำทั้งปรับ

ผู้ใดกรอกข้อความลงในแผ่นกระดาษหรือวัตถุอื่นใด ซึ่งมีลายมือชื่อของผู้อื่นโดยไม่ได้รับความยินยอม หรือโดยฝ่าฝืนคำสั่งของผู้อื่นนั้น ถ้าได้กระทำเพื่อนำเอาเอกสารนั้นไปใช้ในกิจการที่อาจเกิดเสียหายแก่ผู้หนึ่งผู้ใดหรือประชาชน ให้ถือว่าผู้นั้นปลอมเอกสาร ต้องระวางโทษเช่นเดียวกัน

หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

มาตรา269/1-269/7 ผู้ใดทำบัตรอิเล็คทรอนิกส์ปลอมขึ้นทั้งฉบับหรือส่วนใดส่วนหนึ่ง เติม หรือตัดทอนข้อความ หรือแก้ไข ในบัตรที่แท้จริงอันน่าจะเกิดความเสียหายต่อผู้อื่น เพื่อให้คนอื่นหลงเชื่อว่าเป็นบัตรอิเล็คทรอนิกส์ที่แท้จริง ผิดฐานปลอมบัตรอิเล็คทรอนิกส์ ต้องจำคุกตั้งแต่ 1 ปี ถึง 5 ปี และปรับตั้งแต่ 20, 000 บาท - 100,000 บาท

ผู้ใดใช้หรือมีไว้เพื่อใช้บัตรอิเล็คทรอนิกส์โดยรู้ว่าเป็นของที่ปลอมขึ้นมา ต้องจำคุกตั้งแต่ 1 ปีถึง 7 ปี หรือปรับ 20,000 บาท -140,000 บาท

ผู้ใดใช้บัตรอิเล็คทรอนิกส์ของผู้อื่นโดยมิชอบและน่าจะก่อให้เกิดความเสียหายแก่ผู้อื่น จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท

ผู้ใดทำหรือมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมแปลง ต้องจำคุกตั้งแต่ 1 ปีถึง 5 ปี และปรับตั้งแต่ 20,000 บาท - 100,000 บาท

นอกจากนั้นยังมีกฎหมายธุรกรรมทางอิเล็กทรอนิกส์อื่นๆอีก เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 เป็นต้น

จะเห็นได้ว่ามีมาตรการทางกฎหมายออกมาควบคุมดูแลการทุจริต/ปลอมแปลงบัตรเครดิตมากขึ้นหลายฉบับ แต่จากข้อมูลสถิติการรับแจ้งและจับกุมกลุ่มคดีอาญาทั่วราชอาณาจักร ช่วงปี พ.ศ. 2544-2553 และ ข้อมูลเกี่ยวกับการประทุษร้ายต่อทรัพย์ ทั่วราชอาณาจักร พ.ศ.2544-2553 ตามที่ได้กล่าวไว้แล้วในบทที่ 1 ก็ยังมีจำนวนที่สูงมาก และการจับกุมเป็นไปได้ยาก ดังนั้นการหาทางป้องกันจึงน่าจะเป็นวิธีการที่ดีที่สุด

(5) มาตรการรักษาความปลอดภัยทางคอมพิวเตอร์

เนื่องจากข้อมูลในบัตรเครดิตถูกเก็บไว้ในฐานข้อมูลคอมพิวเตอร์ของธนาคาร และในปัจจุบันระบบคอมพิวเตอร์ได้ถูกคุกคามมากขึ้นทั้งจากไวรัสคอมพิวเตอร์ และผู้ไม่ประสงค์ดี ดังนั้นการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security) [31] จะช่วยปกป้องเครื่องคอมพิวเตอร์รวมไปถึงอุปกรณ์ต่างๆที่เกี่ยวข้อง และยังสามารถช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบ หรือที่เรียกว่า ความปลอดภัยทางข้อมูลสารสนเทศ (Information Security) ได้ด้วย วัตถุประสงค์หลักของการรักษาความปลอดภัยทางข้อมูลสารสนเทศ คือ ความลับ (Confidentiality) ความคงสภาพ (Integrity) การพิสูจน์ทราบตัวตน (Authentication) ความพร้อมใช้งาน

(Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่างๆ โดยมีรายละเอียดดังนี้

1. ความลับ (Confidentiality) คือการรับรองว่าข้อมูลที่เก็บไว้จะเป็นความลับ โดยสามารถเข้าถึงข้อมูลหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาติเท่านั้น

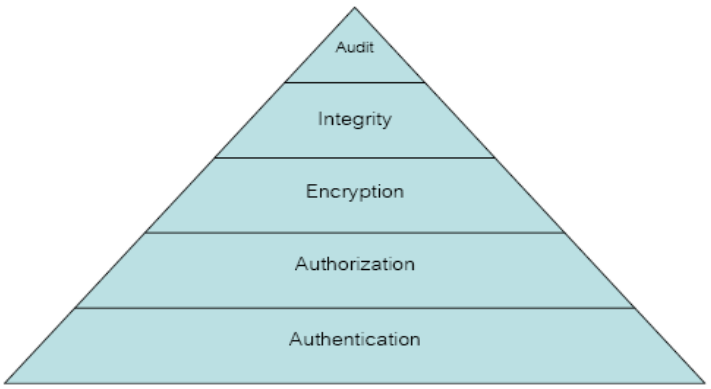
2. ความคงสภาพ (Integrity) คือการรักษาความถูกต้อง และสมบูรณ์ของข้อมูลที่เก็บไว้จะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา

3. การพิสูจน์ทราบตัวตน (Authentication) คือการพิสูจน์ว่าบุคคลที่ส่งข้อความ หรือใช้งานผ่านระบบคอมพิวเตอร์นั้น เป็นบุคคลที่ได้รับอนุญาตจริงๆไม่ใช่ผู้อื่นปลอมแปลงมา

4. ความพร้อมใช้งาน (Availability) คือการรับรองว่าข้อมูลและระบบบริการสื่อสารต่าง ๆ สามารถเข้าถึงและใช้งานได้เมื่อต้องการ

5. การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือการสื่อสารที่มีหลักฐานว่าผู้ส่งสารได้มีการส่งข้อมูลออกไป และผู้รับสารก็ได้รับการยืนยันว่าได้รับแล้ว โดยทราบว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งสารและผู้รับสารจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

ซึ่งสามารถกำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้เป็น 5 ระดับตามภาพที่ 2-8 โดยเป็นองค์ประกอบสำคัญของความมั่นคงปลอดภัยคอมพิวเตอร์ด้วย เพราะเป็นการกำหนดสิทธิและควบคุมการกระทำการของบุคคลที่สามารถเข้าสู่ระบบ หรือเข้าสู่ข้อมูลภายในระบบได้ โดยอนุญาติตามระดับชั้นของความสำคัญของข้อมูล รวมไปถึงการจัดเก็บลักษณะการใช้งานระบบของบุคคลที่เข้าสู่ข้อมูลบนระบบทั้งหมดด้วย



ภาพที่ 2-8 ระดับชั้นของการควบคุมความปลอดภัย
ที่มา : ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน, 2547

การพิสูจน์ตัวตนถือว่าเป็นการตรวจสอบหลักฐานที่สำคัญอย่างหนึ่งในระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

2.2.5 ระบบรหัสลับ

วัตถุประสงค์หลักของระบบรหัสลับคือ การทำให้บุคคล 2 ฝ่าย สามารถติดต่อสื่อสารระหว่างกันผ่านช่องสัญญาณได้ แม้ว่าช่องทางนั้นอาจจะมีความไม่ปลอดภัยจากการปลอมแปลงหรือการเจาะข้อมูล โดยมีองค์ประกอบ คือ

- ข้อความต้นฉบับ (Plaintext) หมายถึงข้อความหรือข้อมูลต้นฉบับที่จะนำไปผ่านการเข้ารหัสลับ

- ขั้นตอนวิธีการเข้ารหัส (Encryption Algorithm) หมายถึงกระบวนการหรือขั้นตอนที่ใช้ในการเปลี่ยนแปลงข้อความต้นฉบับให้อยู่ในรูปแบบที่เปลี่ยนไปจากเดิม และผู้อื่นไม่สามารถเข้าใจได้

- กุญแจลับ (Key) คือ องค์ประกอบหนึ่งที่ป้อนให้กับขั้นตอนวิธีเข้ารหัส

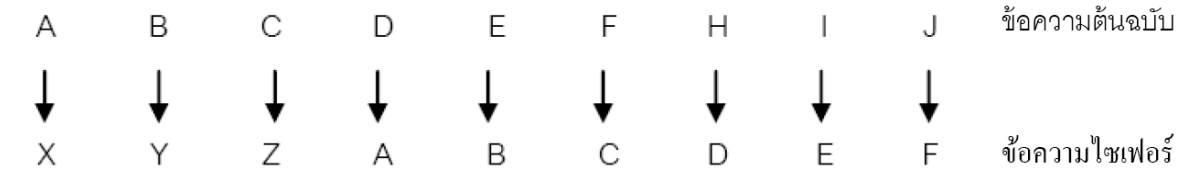
- ข้อความไซเฟอร์ (Ciphertext) เป็นผลลัพธ์ที่ได้จากการนำข้อความต้นฉบับไปผ่านกระบวนการเข้ารหัสลับ โดยใช้กุญแจลับตามที่ผู้ใช้กำหนด

- ขั้นตอนวิธีการถอดรหัส (Decryption Algorithm) คือ กระบวนการ หรือขั้นตอนในการแปลงจากข้อความไซเฟอร์ให้กลับเป็นข้อความต้นฉบับตามเดิมโดยอาศัยกุญแจลับดอกเดียวกับที่ใช้ในขั้นตอนการเข้ารหัสลับ

การเข้ารหัสลับ หรือการเปลี่ยนแปลงจากข้อความต้นฉบับเป็นข้อความไซเฟอร์ สามารถกระทำได้ 2 รูปแบบ คือ การแทนที่ (Substitution) และการสลับเปลี่ยนตำแหน่ง (Permutation) [7]

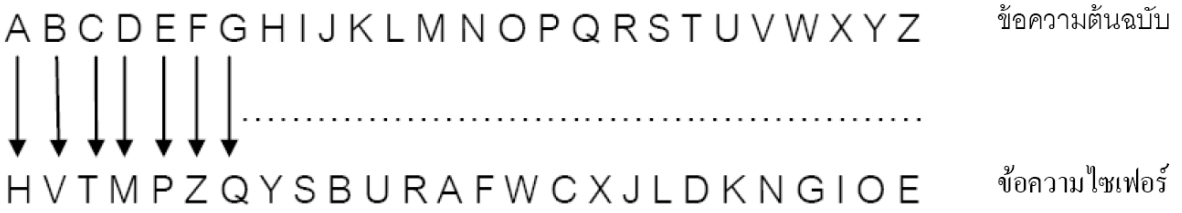
(1) การเข้ารหัสลับแบบแทนที่ (Substitution)

- ไซเฟอร์แบบเลื่อน (Shift Cipher) มีการทำงานโดยให้แทนอักษรของข้อความต้นฉบับแต่ละตัวด้วยอักษรที่อยู่เลื่อนออกไป N ตำแหน่ง ดังภาพที่ 2-9



ภาพที่ 2-9 ตัวอย่างไซเฟอร์แบบเลื่อน
ที่มา : วิทยาการรหัสลับเบื้องต้น, 2548

- ไซเฟอร์แบบแทนที่อักษรเดี่ยว (Monoalphabetic Substitution Cipher) เป็นระบบรหัสลับที่มีหลักการของการแทนที่อักษรข้อความต้นฉบับด้วยอักษรอื่น ซึ่งคล้ายกับ กรณีของไซเฟอร์แบบเลื่อน เพียงแต่ว่าของไซเฟอร์แบบแทนที่อักษรเดี่ยวจะเป็นการเลือกรูปแบบการแทนที่ของอักษรแต่ละตัวจะเป็นอิสระจากกัน คือจะเลือกอักษรตัวใดมาแทนที่ก็ได้ตราบเท่าที่อักษรนั้นไม่เคยถูกเลือกมาก่อน

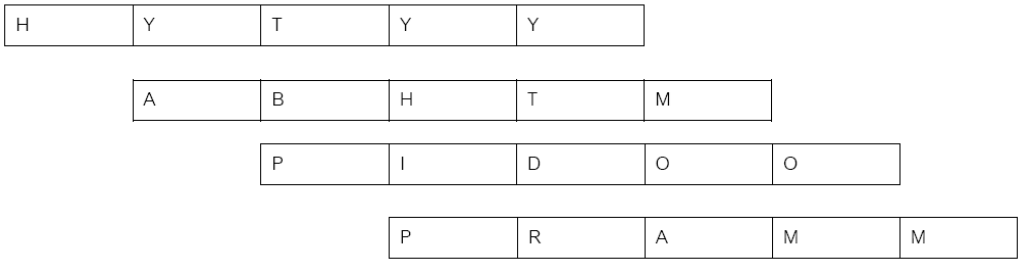


ภาพที่ 2-10 ตัวอย่างไซเฟอร์แบบแทนที่อักษรเดี่ยว
ที่มา : วิทยาการรหัสลับเบื้องต้น, 2548

(2) การเข้ารหัสลับแบบสลับเปลี่ยนตำแหน่ง (Permutation)

ระบบนี้อาศัยการสลับหรือเปลี่ยนตำแหน่งของอักษรที่อยู่ในข้อความต้นฉบับใหม่ ไซเฟอร์ชนิดนี้ไม่ทำให้อักษรแต่ละตัวที่บรรจุอยู่ในข้อความต้นฉบับเปลี่ยนแปลงไปจากเดิม มีเพียงแต่ตำแหน่งการเรียงตัวเท่านั้นที่เปลี่ยนไป

- ไซเฟอร์แบบแนวรั้ว (Rail Fence Cipher) อาศัยหลักการที่ให้เขียนข้อความต้นฉบับทีละอักษรลงในแนวทแยงตามจำนวนแถวที่ระบุไว้ล่วงหน้า เมื่อครบทุกแถวแล้วให้ขยับไปทางขวามือแล้วเริ่มต้นเขียนอักษรทีละแถวใหม่ การกำหนดกุญแจขึ้นอยู่กับจำนวนแถวที่ใช้



ภาพที่ 2-11 ตัวอย่างไซเฟอร์แบบแนวรั้ว
ที่มา : วิทยาการรหัสลับเบื้องต้น, 2548

- ไซเฟอร์แบบสลับคอลัมน์ (Columnar Transposition Cipher) เริ่มด้วยการกำหนดขนาดของคอลัมน์ที่ใช้ในการเข้ารหัสลับ แล้วเขียนข้อความต้นฉบับทีละแถวลงในเมทริกซ์ที่มีจำนวนคอลัมน์ตามที่กำหนด และอ่านข้อความออกจากเมทริกซ์ในแนวคอลัมน์ทีละคอลัมน์ โดยลำดับของคอลัมน์ที่อ่านให้เรียงตามกุญแจที่กำหนดไว้ เช่น ตามภาพที่ 2-12 ใช้กุญแจลับคือ 52314 ทำให้ได้ข้อความไซเฟอร์ขึ้นมา

5	2	3	1	4
m	y	h	o	m
e	t	o	w	n
i	s	p	h	i
t	c	h	i	t

ภาพที่ 2-12 ตัวอย่างไซเฟอร์แบบสลับคอลัมน์
ที่มา : วิทยาการรหัสลับเบื้องต้น, 2548

- ไซเฟอร์แบบสลับเปลี่ยนตำแหน่ง คือ การกำหนดตารางการสับเปลี่ยนตำแหน่งของอักษรได้อย่างอิสระ ไม่มีข้อจำกัดในเรื่องของรูปแบบการสลับเปลี่ยนตำแหน่ง โดยอาศัยตารางการสลับเปลี่ยนตำแหน่งสำหรับอักษรในแต่ละตำแหน่งครบทุกตัว ยิ่งต้องการสลับอักษรในช่วงกว้างมากเท่าไหร่ ตารางที่ใช้ก็ต้องมีขนาดเพิ่มขึ้นตามไปด้วย

การปกป้องฐานข้อมูลรหัสผ่านโดยทั่วไปทำได้โดยการนำข้อมูลเหล่านั้นไปผ่านการเข้ารหัสลับ และบรรจุข้อความไซเฟอร์ลงในฐานข้อมูลแทนข้อความรหัสผ่าน ดังนั้น ถึงแม้ว่าจะได้ข้อมูลบรรจุรหัสผ่านไป ก็ไม่สามารถทราบค่ารหัสผ่านที่แท้จริงได้ มีเพียงผู้ดูแลระบบเท่านั้นที่จะ

ทราบกุญแจลับสำหรับการถอดรหัสกลับคืนมา การใช้วิธีนี้แม้ว่าจะทำให้การปลอมรหัสผ่านเกิดขึ้นได้ยาก แต่ถ้าคำนึงถึงเรื่องความเป็นส่วนตัวของผู้ใช้บริการ ถือว่ายังไม่สมบูรณ์ เพราะยังมีบุคคลกลุ่มหนึ่งที่รู้รหัสผ่านของผู้ใช้แต่ละราย คือ ผู้ดูแลระบบ ฉะนั้นหากระบบต้องการให้ข้อมูลลับของผู้ใช้บริการมีความสมบูรณ์เต็มรูปแบบ พบว่าสามารถทำได้โดยอาศัยฟังก์ชันแฮช [7] คือ ขั้นแรกให้นำรหัสผ่านของผู้ใช้บริการแต่ละรายมาผ่านฟังก์ชันแฮช จากนั้นบรรจุค่าแฮชที่คำนวนได้ลงในฐานข้อมูลแทนการจัดเก็บค่ารหัสผ่านจริง เมื่อใดที่ผู้ใช้บริการเข้าสู่ระบบให้นำรหัสผ่านที่ผู้ใช้พิมพ์เข้าไปผ่านฟังก์ชันแฮชก่อน แล้วจึงนำไปเปรียบเทียบกับค่าแฮชของผู้ใช้ดังกล่าวที่บรรจุอยู่ในฐานข้อมูล ถ้าตรงกันก็จะอนุญาตให้ผู้ใช้รายนั้นเข้าสู่ระบบได้ หรือหากไม่ตรงกันก็จะปฏิเสธการเข้าใช้งาน

2.2.6 ฟังก์ชันแฮช (Hash Function)

ฟังก์ชันแฮช (Hash Function) [7] คือ ขั้นตอนวิธีที่รับข้อมูล M ที่มีขนาดความยาวแปรเปลี่ยนได้ ไปประมวลผลเพื่อให้ได้เป็นรหัสแฮช H (M) หรือ รหัสแฮช ที่มีขนาดคงที่ ดังนั้นไม่ว่าข้อความที่นำมาประมวลผลนั้นจะมีความยาวแตกต่างกันเพียงใดก็ตาม รหัสแฮช ที่ได้ก็จะมีขนาดที่เท่ากันทั้งหมด โดยรหัสนี้จะแสดงถึงเอกลักษณ์ของข้อความแต่ละข้อความที่ไม่เหมือนกัน หรือการย่อยข้อความให้เล็กลง (Message Digest)

ฟังก์ชันแฮชมีประโยชน์มากในการประยุกต์ใช้งานในทางปฏิบัติได้หลากหลาย เช่น การตรวจสอบความคงสภาพของข้อมูล (Message Integrity) การลงลายเซ็นดิจิทัล (Digital Signature) ระบบจัดการรหัสผ่าน (Password) ของผู้ใช้บริการอินเทอร์เน็ตบนเว็บไซต์ รหัสแฮชจัดเป็นข้อมูลที่ผ่านการเข้ารหัส (Cipher Data) ที่ไม่สามารถถอดรหัสกลับมาเป็นข้อมูลเดิมด้วยวิธีการใด ๆ ได้ จึงเป็นวิทยาการที่มีความปลอดภัยสูง คุณสมบัติของฟังก์ชันแฮชที่สำคัญ คือ กระบวนการที่จะใช้หาข้อความต้นฉบับจากรหัสแฮช นั้นจะเป็นกระบวนการที่ยากมาก เนื่องจากฟังก์ชันแฮช ถูกออกแบบมาเป็นฟังก์ชันทางเดียว นอกจากนั้นข้อความ 2 ข้อความที่จะให้ค่ารหัสแฮช ที่เป็นค่าเดียวกันหลังจากผ่านฟังก์ชันนี้ เป็นเรื่องที่ยากมาก โดยเรียกคุณสมบัตินี้ว่า คุณสมบัติปลอดการชน (Collision Free)

ขั้นตอนวิธี (Algorithm) ที่ให้ผลตรงตามคุณลักษณะของฟังก์ชันแฮชมีหลายวิธี เช่น MD4, MD5, SHA-1, RIPEMD-160 เป็นต้น

ขั้นตอนวิธี MD5

MD5 เป็นอัลกอริธึมแฮชแบบทางเดียว (One-Way Hash Algorithm) อย่างหนึ่ง ที่มีขนาดคงที่ 128 บิต ให้ค่าเป็นตัวเลขฐาน 16 (0123456789ABCDEF) โดยมีลักษณะแปลงข้อความต้นฉบับให้เล็กลง (Message Digest) และแสดงออกมาเป็นค่าแฮชที่มีความยาว 32 ตัวอักษร แทนข้อความเดิม ซึ่งค่าแฮชที่ออกมานั้นเป็นประโยชน์ในการทำลายมือชื่อดิจิทัล (Digital Signature) และงานด้านความปลอดภัย

กระบวนการทำงานของขั้นตอนวิธี MD5 คือ

1. เพิ่มบิตเติมเต็ม (Append Padding Bits) คือ การนำข้อความต้นฉบับมาเพิ่มเติมเต็มบิต (Padding Bits) เพื่อให้ได้ข้อความที่มีจำนวนบิตเท่ากับ 448 mod 512 ดังนั้นข้อความจะได้รับการปรับให้มีขนาดเป็นค่าสั้นกว่า 64 บิตของค่าที่เป็นจำนวนเท่าของ 512 บิต และเป็นขั้นตอนที่จะต้องทำเสมอ แม้ว่าข้อความต้นฉบับมีจำนวนบิตเท่ากับ 448 mod 512 อยู่แล้ว

2. เพิ่มค่าความยาว (Append Length) คือ การนำข้อความต้นฉบับที่ผ่านการเพิ่มบิตเติมเต็มในขั้นตอนที่ 1 มาเพิ่มอีก 64 บิต โดยบิตเหล่านี้ระบุขนาดความยาวของข้อความต้นฉบับ ไม่นับรวมบิตเติมเต็ม แต่ถ้าข้อความต้นฉบับมีขนาดความยาวเกิน 2^{64} บิต จะนำเฉพาะ 64 บิตล่างสุดของความยาวมาต่อท้าย โดยผลลัพธ์ที่ได้จะเป็นข้อความที่มีขนาดเป็นจำนวนเท่าของ 512 บิตพอดี

3. กำหนดค่าตั้งต้นให้กับบัฟเฟอร์ MD (Initialize MD Buffer) กำหนดบัฟเฟอร์ขนาด 128 บิต เพื่อใช้สำหรับการคำนวน Message Digest โดยแบ่งเป็น 4 ส่วนย่อย เรียกว่า เรจิสเตอร์ (A,B,C,D) ที่แต่ละส่วนมีขนาดเท่ากับ 32 บิต

4. ประมวลผลบล็อกข้อความขนาด 16 เวิร์ด (Process Message in 16-word Blocks) คือ การนำข้อความต้นฉบับที่ผ่านการเพิ่มเติมเต็มมาพิจารณา และประมวลผลครั้งละ 1 บล็อกขนาด 512 บิต หรือเท่ากับ 16 เวิร์ด

5. ผลลัพธ์ที่ด้านออก (Output) จากกระบวนการทั้งหมด ผลลัพธ์ที่ได้คือค่าที่บรรจุอยู่ในเรจิสเตอร์ A,B,C,D โดย เริ่มจาก A ไปยัง B C ไปสิ้นสุดที่ D

ขั้นตอนวิธี SHA-1

ได้รับการพัฒนาขึ้นเพื่อใช้เป็นองค์ประกอบส่วนหนึ่งของขั้นตอนวิธีการสร้างลายมือชื่อดิจิทัล ขั้นตอนวิธี SHA-1 สามารถรองรับข้อความที่มีขนาดไม่เกิน 2^{64} บิต โดยให้ผลลัพธ์เป็น Message Digest ที่มีขนาดคงที่เท่ากับ 160 บิต โดยที่ค่า Message Digest ที่คำนวณได้จะนำไปใช้เป็นส่วนหนึ่งของกระบวนการสร้างลายมือชื่อดิจิทัลให้แก่ข้อความ และนำไปใช้อีกครั้งในขั้นตอน

การตรวจสอบความถูกต้องของลายมือชื่อที่ได้รับ ซึ่งในขั้นตอนของการตรวจสอบความถูกต้องของลายมือชื่อ หากมีการเปลี่ยนแปลงบิตในข้อความเพียงเล็กน้อยระหว่างทาง โอกาสที่ค่า Message Digest จะแตกต่างไปจากเดิมมีค่าสูงมาก ซึ่ง ขั้นตอนวิธี SHA-1 มีคุณสมบัติคือ หากกำหนด Message Digest มาให้หนึ่งค่า จะต้องเป็นไปไม่ได้ที่จะหาข้อความต้นฉบับ และการหาข้อความต้นฉบับสองชุดที่ให้ผลเป็น Message Digest เดียวกันต้องเป็นเรื่องที่ยากมาก

จากคุณสมบัติของฟังก์ชันแฮชดังกล่าว ได้พิจารณาหาขั้นตอนวิธีที่เหมาะสมมาประยุกต์ใช้กับนวัตกรรมยืนยันตัวของผู้ใช้บริการบัตรเครดิต โดยจะใช้วิธี MD5 เพราะ MD5 จะประมวลผลลัพธ์ออกมาเร็วกว่า SHA-1 ที่มีจำนวนบิตมากกว่า ซึ่งเหมาะสมกับการนำมาใช้งานจริง โดยที่ทั้ง 2 แบบให้คุณสมบัติที่เหมือนกัน

2.2.7 ประเภทของรหัสแถบ

(1) รหัสแถบ 1 มิติ (1 Dimension Barcode)

รหัสแถบ1 มิติ (Bar code) หรือ บาร์โค้ด 1 มิติ [34] มีลักษณะเป็นเส้นแถบ ประกอบด้วยเส้นสีดำสลับกับเส้นสีขาวบางหนาแตกต่างกันไป ใช้แสดงแทนรหัสตัวเลขหรือตัวอักษร และสามารถบรรจุข้อมูลได้ประมาณ 20 ตัวอักษร โดยการใช้งานรหัสแถบมักใช้ร่วมกับฐานข้อมูลคือจะต้องอ่านรหัสแถบและถอดรหัสแล้ว ถึงนำรหัสที่ได้มาใช้เรียกดูข้อมูลจากฐานข้อมูลได้ รหัสแถบ 1 มิติมีหลายชนิด เช่น UPC EAN-13 หรือ ISBN ซึ่งรหัสแถบ 1 มิติเหล่านี้สามารถพบได้ตามสินค้าทั่วไปในซูเปอร์มาร์เก็ต หรือห้างสรรพสินค้า

ภาพที่ 2-13 รหัสแถบ 1 มิติแต่ละชนิด

ที่มา : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย: แนะนำเทคโนโลยี 2 มิติ, 2549

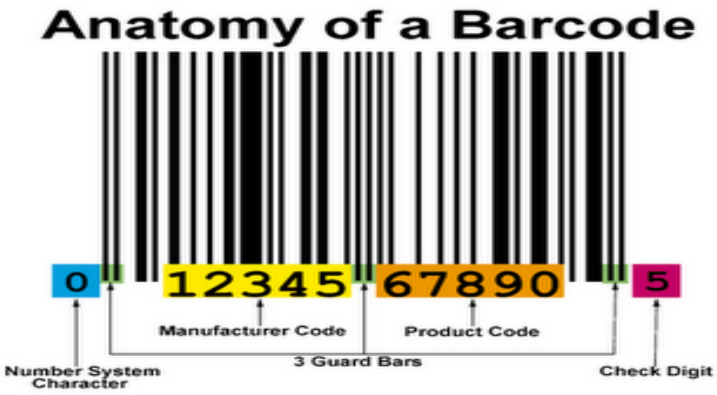
รหัสแถบที่ใช้สื่อแทนข้อมูลตัวเลขจะมีลักษณะเป็นเส้นแถบที่มีความหนาบางแตกต่างกันขึ้นอยู่กับตัวเลขที่ใส่อยู่ข้างล่าง โดยการอ่านข้อมูลจะอาศัยหลักการสะท้อนแสงอ่อน/เข้ม เพื่ออ่านข้อมูลและจัดเก็บเข้าสู่คอมพิวเตอร์ได้โดยตรงไม่จำเป็นต้องผ่านการกดปุ่มที่แป้นพิมพ์ ระบบนี้เป็นที่นิยมใช้กันทั่วโลก เพราะการนำเข้าข้อมูลจากรหัสแถบของสินค้าเป็นวิธีที่สะดวกและข้อมูลมีความน่าเชื่อถือได้สูง อีกทั้งยังให้ความสะดวกแก่ผู้ใช้งานได้ดีอีกด้วย [35]

ส่วนประกอบของรหัสแถบ คือ

1. ส่วนลายเส้น เป็นลายเส้นสีขาว (โปร่งใส) และลายเส้นสีดำ มีขนาดความกว้างของเส้นตามมาตรฐานของรหัสแถบแต่ละชนิด

2. ส่วนข้อมูลตัวอักษร/ตัวเลข เป็นส่วนที่สื่อถึงความหมายของข้อมูลลายเส้นสำหรับให้อ่านเข้าใจได้

3. ส่วนแถบว่าง (Quiet Zone) เป็นส่วนที่เครื่องอ่านรหัสแถบใช้กำหนดขอบเขตของรหัสแถบและกำหนดค่าให้กับแถบสีขาว โดยอาศัยความเข้มของการสะท้อนแสงกับสีของพื้นผิวรหัสแถบ ซึ่งแถบแต่ละเส้นจะมีความยาวเท่ากันเรียงตามลำดับในแนวนอนจากซ้ายไปขวา เพื่อให้เครื่องอ่านรหัสแถบ (Barcode Scanner) ใช้อ่านข้อมูลที่บันทึกไว้



ภาพที่ 2-14 โครงสร้างของรหัสแถบ 1 มิติ

ที่มา : http://www.justinlessard.wordpress.com/2008...ode-666/

ปัจจุบัน มีการประยุกต์ใช้รหัสแถบในเรื่องต่างๆมากขึ้น โดยมีจุดประสงค์เพื่อบ่งบอกวัตถุอย่างอัตโนมัติ (Automatic Identification) เนื่องจากเทคนิคและอุปกรณ์สำหรับการอ่านรหัสแถบนี้พร้อมใช้งานได้อย่างดี

ในการอ่านรหัสแถบ [36] จะใช้หลักการที่ว่า พื้นที่สว่างจะสะท้อนกลับได้มากกว่าพื้นที่มืด ดังนั้นเมื่อเครื่องอ่านสแกนไปที่รหัสแถบ ลำแสงจากหัวอ่านจะสะท้อนกลับมามากหรือน้อยก็ขึ้นอยู่กับว่า แสงนั้นได้ตกกระทบแถบขาวหรือแถบดำ ซึ่งแสงสะท้อนกลับจะถูกดัดแปลงให้เป็นสัญญาณไฟฟ้า โดยมีอุปกรณ์อิเล็กทรอนิกส์ชนิดสองขั้ว (Photo Diode) ติดอยู่ที่หัวอ่าน ซึ่งขนาดของลำแสงที่ส่งออกมานั้น จะต้องสัมพันธ์กับความละเอียด (Resolution) ของแถบ คือขนาดจะต้องไม่ใหญ่กว่าความกว้างของแถบดำหรือแถบขาวที่แคบที่สุด ซึ่งส่วนใหญ่จะเป็นจุดลำแสงที่มีขนาดเส้นผ่าศูนย์กลางประมาณ 0.2 มม. ในส่วนของความยาวคลื่นของแสงที่ใช้ จะขึ้นอยู่กับว่าใช้อ่านรหัสแถบสีอะไร โดยทั่วไปใช้แสงอินฟราเรด (Infrared) ที่มีความยาวคลื่นประมาณ 0.95 ไมครอน (Micron) สำหรับอ่านแถบขาวดำ และใช้แสงสีแดงที่มีความยาวคลื่น 0.65 ถึง 0.7 ไมครอน สำหรับอ่านรหัสแถบสีเขียวหรือสีน้ำเงินที่พิมพ์บนพื้นสีเหลืองหรือส้ม

รหัสแถบมีหลากหลายชนิด เช่น รหัสแทนตัวเลข รหัสแทนทั้งตัวเลขและตัวอักษร เป็นต้น ดังนั้นการเลือกใช้จึงดูที่ลักษณะของงานเป็นหลัก โดยพิจารณาจากชุดตัวอักษรที่รหัสสามารถแทนได้ ความยาก/ง่ายในการใส่รหัส ความแม่นยำของรหัส ความยืดหยุ่นของความเร็วที่ใช้ในการอ่าน และความต้านทานต่อความไม่สมบูรณ์ในการพิมพ์ เป็นต้น ซึ่งรหัสที่ใช้กันแพร่หลายในปัจจุบัน ได้แก่ UPC (Universal Product Code), EAN (European Artic number), Codebar, 2 ใน 5 และรหัส 39 [36]

รหัส EAN/UPC

เป็นรหัสที่แทนด้วยตัวเลขเท่านั้น แถบรหัสหนึ่งจะประกอบด้วยเลข 8 ตัว หรือ 13 ตัว ก็ได้ แต่ที่แพร่หลายที่สุดคือ ขนาด 13 ตัว โดยแถบรหัสจะขึ้นต้นและลงท้ายด้วยรหัส 101 เสมอ และตัวเลข 13 หลักนี้จะถูกแบ่งเป็นสามส่วน ส่วนแรกประกอบด้วยเลข 2 ตัว หมายถึงประเทศ ส่วนที่สองประกอบด้วยเลข 4 ตัว หมายถึงผู้ผลิต และส่วนสุดท้ายมีรหัส 01010 เป็นตัวคั่นจากส่วนที่สอง หมายถึงรหัสตัวสินค้า ซึ่งรหัสแต่ละตัวจะมีแถบ 7 แถบ แต่ละแถบมีความกว้างเท่ากัน โดยแถบดำแทนด้วย 1 และแถบขาวแทนด้วย 0 รหัส EAN/UPC นี้นิยมใช้กันแพร่หลายทั่วโลกกับสินค้าอุปโภคบริโภค

Codabar

เป็นรหัสที่แทนด้วยตัวเลข โดยมีความยาวของแถบรหัสจาก 1 ถึง 32 ตัว เป็นรหัสที่ใช้ในธนาคารโลหิตของสหรัฐอเมริกา อุตสาหกรรมยา และทางการแพทย์ ซึ่งตัวรหัส 1 ตัว จะประกอบด้วย 7 บิต ซึ่งแบ่งเป็น แถบดำ 4 แถบ และแถบขาว 3 แถบ การแทนค่าดูที่ความกว้าง/แคบเป็นหลัก คือ แถบดำหรือขาวที่แคบแทน 0 และแถบดำหรือขาวกว้างแทน 1

รหัส 2 ใน 5

เป็นรหัสชนิดแรกที่ถูกใช้อย่างเป็นทางการ รหัส 1 ตัวจะประกอบด้วยแถบห้าแถบ ซึ่งสองในจำนวนนี้จะมีลักษณะแตกต่างจากที่เหลือ รหัสในตระกูลนี้ได้แก่ 2 ใน 5 อุตสาหกรรม, 2 ใน 5 เมทริกซ์ และ 2 ใน 5 สอดแทรก ทั้งหมดเป็นรหัสแทนตัวเลข

ตารางที่ 2-1 ตัวอย่างของรหัสตระกูล 2 ใน 5

1	10001
2	01001
3	11000
4	00101
5	10100
6	01100
7	00011
8	10010
9	01010
10	00110
CODE START	110
CODE STOP	101

ที่มา : วารสารคอมพิวเตอร์ สมาคมคอมพิวเตอร์แห่งประเทศไทย, 2531

1. รหัส 2 ใน 5 อุตสาหกรรม เป็นแถบรหัสที่มีความยาวระหว่าง 1 ถึง 32 ตัว รหัสชนิดนี้แถบดำเท่านั้นที่ถือเป็นองค์ประกอบของแถบรหัส โดยแถบดำแคบถือเป็น 0 และแถบดำกว้างถือเป็น 1 รหัสนี้เป็นรหัสที่ง่ายต่อการพิมพ์ แต่ขาดความแม่นยำในการอ่าน ดังนั้นจึงต้องเติมอักษรควบคุมเพิ่มที่ท้ายแถบรหัส รหัส 2 ใน 5 อุตสาหกรรม มักนิยมใช้ในโรงงานอุตสาหกรรม ตั๋วเครื่องบิน และเครื่องคัดแยกจดหมาย

2. รหัส 2 ใน 5 เมทริกซ์ ทั้งแถบดำและแถบขาวถือเป็นองค์ประกอบของรหัส หนึ่งตัวรหัสประกอบด้วยแถบดำ 3 แถบ และแถบขาว 2 แถบ โดยระหว่างรหัสแต่ละตัวจะมีช่องว่างกั้น แถบรหัสจะขึ้นต้นและลงท้ายด้วยรหัส 10000 เสมอ การใช้แถบขาวเป็นองค์ประกอบหนึ่งของรหัสแถบทำให้รหัสชนิดนี้กินเนื้อที่น้อยกว่ารหัสชนิดแรก จาก 28 ถึง 33 เปอร์เซ็น แต่มีข้อเสียคือมีความต้านทานต่อความผิดพลาดต่ำ

3. รหัส 2 ใน 5 สอดแทรก รหัสชนิดนี้ทั้งแถบดำและแถบขาวเป็นองค์ประกอบของรหัสเช่นเดียวกับ 2 ใน 5 เมทริกซ์ แต่จะไม่มีช่องว่างกั้นระหว่างรหัส การใส่รหัสจะทำในลักษณะของ

การสอดแทรก คือ อักษรตัวแรก ใส่รหัสด้วยรหัส 2 ใน 5 อุตสาหกรรม โดยใช้แถบดำเป็นตัวประกอบ อักษรตัวต่อมาใส่รหัสด้วย 2 ใน 5 อุตสาหกรรม ใช้แถบขาวเป็นตัวประกอบ แถบขาวที่ใช้มีห้าแถบด้วยกัน คือแบ่งเป็นแถบกว้าง 2 แถบ และแถบแคบ 3 แถบ นำไปแทรกเข้าสลับกับแถบดำ 5 แถบที่ได้จากการใส่รหัสตัวอักษรแรก แถบรหัสของ 2 ใน 5 สอดแทรก นี้จะขึ้นต้นด้วยรหัส 0000 และลงท้ายด้วยรหัส 100 เมื่อเทียบกับรหัส 2 ใน 5 อุตสาหกรรม รหัสชนิดนี้ให้ความหนาแน่นมากกว่าจาก 36 ถึง 42 เปอร์เซ็น และจาก 10 ถึง 12 เปอร์เซ็น เมื่อเทียบกับรหัส 2 ใน 5 เมทริกซ์ วงการอุตสาหกรรมนิยมใช้เป็นอย่างมาก

รหัส 39

รหัส 39 เป็นรหัสที่ใช้แทนตัวอักษรชนิดแรก ประกอบด้วยสัญลักษณ์ 43 ตัว (เดิม 39 ตัว) แบ่งเป็นพยัญชนะ 26 ตัว ตัวเลข 10 ตัว และอักษรพิเศษที่เหลือ 7 ตัว โดยตัวรหัสหนึ่งตัวประกอบด้วย 9 ตัวประกอบ แบ่งเป็น แถบกว้าง 3 ตัว และแถบแคบ 2 ตัว ในแถบรหัส 1 แถบจะมี1-3 ตัวอักษร และตามด้วย Check digit ดังนั้นรหัส 39 จึงมีความแน่นอนในการอ่านสูง แต่เปลืองเนื้อที่ รหัสชนิดนี้นิยมใช้กันมากในอุตสาหกรรมอิเล็กทรอนิกส์ โดยใช้ในการแยกชนิดแผงวงจร

รหัสชนิดอื่น ที่เราสามารถพบเห็นได้ นอกเหนือจากรหัสที่กล่าวข้างต้น เพียงแต่ว่าไม่เป็นที่แพร่หลายเท่า รหัสเหล่านี้ได้แก่ รหัส 128, รหัส 2 ใน 7 และรหัส 11

(2) รหัสแถบ 2 มิติ (2 Dimension Barcode)

เป็นเทคโนโลยีที่พัฒนามาจากรหัสแถบ 1 มิติ ออกแบบให้บรรจุข้อมูลได้ทั้งแนวตั้งและแนวนอน สามารถบรรจุข้อมูลมากได้ประมาณ 4,000 ตัวอักษร หรือประมาณ 200 เท่าของรหัสแถบ 1 มิติในพื้นที่เท่ากันหรือเล็กกว่า สามารถบรรจุข้อมูลด้วยภาษาอื่นๆได้นอกเหนือจากภาษาอังกฤษ เช่น ภาษาญี่ปุ่น จีน เกาหลี เป็นต้น ข้อดีของรหัสแถบ 2 มิติ คือ แม้ภาพรหัสแถบบางส่วนมีความเสียหาย แต่รหัสแถบ 2 มิติก็สามารถถอดรหัสได้ นอกจากนั้นอุปกรณ์ที่ใช้อ่านและถอดรหัสรหัสแถบ 2 มิติมีหลายอย่าง เช่น เครื่องอ่านแบบซีซีดีหรือเครื่องอ่านแบบเลเซอร์เหมือนกับของรหัสแถบ 1 มิติ โทรศัพท์มือถือแบบมีกล้องถ่ายรูปในตัวซึ่งติดตั้งโปรแกรมถอดรหัสไว้ รหัสแถบ 2 มิติมีอยู่มากมายตามชนิดของรหัสแถบ [37] เช่น วงกลม สี่เหลี่ยมจัตุรัส หรือสี่เหลี่ยมผืนผ้าคล้ายกับรหัสแถบ 1 มิติ ตัวอย่างรหัสแถบ 2 มิติ ได้แก่ PDF417, MaxiCode, Data Matrix และ QR-Code ดังตัวอย่างตามภาพที่ 2-15

ภาพที่ 2-15 ตัวอย่างของรหัสแถบ 2 มิติชนิดต่างๆ

ที่มา : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2549

ซึ่งรหัสแถบ 2 มิติแต่ละแบบต่างก็มีคุณสมบัติที่แตกต่างกันตามตารางที่ 2-2

ตารางที่ 2-2 เปรียบเทียบรหัสแถบ 2 มิติชนิดต่างๆ

บาร์โค้ด 2 มิติ		PDF417	MAXICODE	DATA MATRIX	QR CODE
ผู้พัฒนา(ประเทศ)		(อเมริกา)	(อเมริกา)	(อเมริกา)	(ญี่ปุ่น)
ประเภทบาร์โค้ด		แบบสแต็ก	แบบเมตริกซ์	แบบเมตริกซ์	แบบเมตริกซ์
ขนาดความจุข้อมูล	ตัวเลข	2,710	138	3,116	7,089
	ตัวอักษร	1,850	93	2,355	4,296
	เลขฐานสอง	1,018	-	1,556	2,953
	ตัวอักษรญี่ปุ่น	554	-	778	1,817
ลักษณะที่สำคัญ		-บรรจุข้อมูลได้มาก	-มีความเร็วในการอ่านสูง	-บาร์โค้ดมีขนาดเล็ก	-บาร์โค้ดมีขนาดเล็ก -มีความเร็วในการอ่านสูง -บรรจุข้อมูลได้มาก
มาตรฐานที่ได้รับ		-ISO/IEC 15438 -AIM USS-PDF417	-ISO/IEC 16023 -ANSI/AIM BC-10-ISS-MAXICODE	-ISO/IEC 16022 -ANSI/AIM BC-11-ISS-MATRIX	-ISO/IEC 18004 -JIS X 0510 -JEIDA-55 -AIM ITS/97/001 ISS-QR CODE

ที่มา : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2549

จากตาราง 2-2 แสดงให้เห็นว่าเมื่อเปรียบเทียบลักษณะและคุณสมบัติของรหัสแถบ 2 มิติชนิดต่างๆแล้ว QR-Code ได้รวมคุณสมบัติที่ดีของรหัสแถบ 2 มิติชนิดอื่นๆเอาไว้ได้ครบ เช่น บรรจุข้อมูลได้มาก มีความเร็วในการอ่านสูง และบาร์โค้ดมีขนาดเล็ก ซึ่งเหมาะในการนำมาใช้กับนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตที่ต้องการคุณสมบัติดังกล่าว

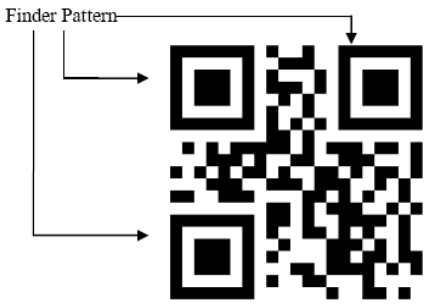
รหัสตอบสนองอย่างรวดเร็ว (QR-Code)

เป็นรหัสแถบ 2 มิติแบบเมตริกซ์ มีชื่อเต็มๆว่า Quick Response Code คือรหัสชนิดหนึ่งที่มีไว้เก็บข้อมูล โดยคิวอาร์โค้ดนี้ได้มีการพัฒนามาจากรหัสแถบ ซึ่งถูกพัฒนาขึ้น โดยบริษัท Nippon Denso ประเทศญี่ปุ่น มีลักษณะเป็นสี่เหลี่ยมจัตุรัสสีขาวดำ และมีสัญลักษณ์เฉพาะตัว มีโมดูลข้อมูล 21x21 ถึง 177x177 โมดูล สามารถบรรจุข้อมูล ตัวเลขอารบิกมากที่สุด 7,089 ตัวเลข หรือ บันทึกตัวอักษรภาษาอังกฤษผสมตัวเลขอารบิกได้สูงสุด 4,296 ตัวอักษร ข้อมูลเลขฐานสองขนาด 8 บิตได้สูงสุด 2,953 ไบต์ และตัวอักษรญี่ปุ่น (อักษรคันจิหรือคะตาคะนะ) ได้สูงสุด 1,817 ตัวอักษร [6]

<u>คุณสมบัติของรหัสตอบสนองอย่างรวดเร็ว</u>

คิวอาร์โค้ด ส่วนใหญ่ใช้ในงานที่ต้องการบรรจุข้อมูลจำนวนมากลงในรหัสแถบ และต้องการอ่านข้อมูลจาก รหัสแถบอย่างรวดเร็ว ผ่านการติดตั้งซอฟต์แวร์สำหรับอ่านคิวอาร์โค้ด

1. ความสามารถในการอ่านข้อมูลได้ 360 องศาด้วยความเร็วสูง โดยความสามารถดังกล่าวเป็นลักษณะเด่นของรหัสแถบแบบเมตริกซ์ คือ มีตัวรูปแบบค้นหา (Finder Pattern) [34] ทำหน้าที่เป็นตัวอ้างอิงตำแหน่งในการอ่าน และถอดรหัสข้อมูล ช่วยให้อ่านข้อมูลได้รวดเร็ว และสามารถอ่านรหัสแถบได้แม้รหัสแถบเอียง หมุน หรือกลับหัว โดยที่รูปแบบค้นหาของคิวอาร์โค้ด อยู่ที่มุมทั้งสามของรหัสแถบ คือ มุมซ้ายบน มุมซ้ายล่าง และมุมขวาบน ดังภาพที่ 2-16 อีกทั้งยังทำให้เครื่องอ่านมีความเสถียรในเรื่องของความเร็วในการอ่าน และเป็นตัวป้องกันการรบกวนของพื้นหลังอีกด้วย



ภาพที่ 2-16 ลักษณะตัวค้นหาของ QR-Code

ที่มา : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2549

2. มีคุณสมบัติในการควบรวม [19] คิวอาร์โค้ดสามารถแบ่งข้อมูลหนึ่งสัญลักษณ์เป็นหลายๆสัญลักษณ์ได้ และในขณะเดียวกันก็สามารถจะนำสัญลักษณ์ดังกล่าวนั้นมาวางติดกันแล้วอ่านข้อมูลออกมาเป็นชิ้นเดียวกันได้ โดย 1 สัญลักษณ์สามารถแบ่งได้ สูงสุดถึง 16 สัญลักษณ์ จึงเป็นประโยชน์อย่างมากต่อการใช้งานในพื้นที่จำกัด

3. ความคงทนต่อความเสียหาย [38] แม้รหัสจะมีความเสียหายบางส่วนก็สามารถอ่านค่าได้ โดยแบ่งเป็นระดับ (Level) ตามลักษณะความเสียหายของคิวอาร์โค้ด เช่น

Level L, ประมาณ 7% สามารถเรียกข้อมูลคืนได้

Level M, ประมาณ 15% สามารถเรียกข้อมูลคืนได้

Level Q, ประมาณ 25% สามารถเรียกข้อมูลคืนได้

Level H, ประมาณ 30% สามารถเรียกข้อมูลคืนได้

4. มีโปรแกรมสำหรับอ่านข้อมูลหลากหลาย สามารถติดตั้งซอฟต์แวร์สำหรับอ่านคิวอาร์โค้ดไว้ในโทรศัพท์มือถือได้นอกเหนือจากอุปกรณ์ปกติ เมื่อพบคิวอาร์โค้ดในนิตยสาร หรือป้ายโฆษณา Bill Board เมื่อเอามือถือไปสแกนคิวอาร์โค้ด โปรแกรมก็จะแสดงข้อมูลขึ้นมาตามที่ได้บรรจุข้อมูลนั้นไว้

5. สามารถประยุกต์ใช้ได้หลากหลายรูปแบบ ส่วนใหญ่นิยมใช้เก็บข้อมูลสินค้า เช่น ชื่อสินค้า ราคาสินค้า เก็บข้อมูล URL ของเว็บไซต์, ข้อความ, เบอร์โทรศัพท์ และข้อมูลที่เป็นตัวอักษรได้มากมาย ประโยชน์ที่เห็นได้ชัดที่สุดของคิวอาร์โค้ดก็คือการเก็บ URL ของเว็บไซต์ เพราะ URL โดยปกติแล้วจะยาว และจดจำได้ยาก บางอันใช้ภาษาเฉพาะมีความซับซ้อนมาก ขนาดบันทึกบนกระดาษไม่ได้ แต่ด้วยคิวอาร์โค้ดเราเพียงแค่ยกโทรศัพท์มาถ่ายคิวอาร์โค้ดตามผลิตภัณฑ์ต่างๆ นิตยสาร ฯลฯ จากนั้นโทรศัพท์ที่มีการติดตั้งเครื่องอ่านคิวอาร์โค้ด จะเข้าถึงหน้าเว็บที่คิวอาร์โค้ดนั้นๆ บันทึกข้อมูลอยู่โดยอัตโนมัติ นอกจากนั้นยังมีการนำเทคโนโลยีรหัสแถบ 2 มิติมาใช้งานด้านอื่นๆอีก เช่น

<u>ด้านอุตสาหกรรมยานยนต์</u> มีการติดคิวอาร์โค้ดบนชิ้นส่วนอะไหล่ยนต์ต่างๆ เพื่อเก็บข้อมูลของอะไหล่ชิ้นนั้น

<u>ด้านกระบวนการผลิตสินค้า</u> มีการติดคิวอาร์โค้ดบนแผงวงจรอิเล็กทรอนิกส์ เพื่อเก็บข้อมูลรายละเอียดต่างๆของแผงวงจรนั้น

<u>ด้านการขนส่งสินค้า</u> มีการพิมพ์คิวอาร์โค้ดบนใบส่งสินค้า เพื่อใช้ในการจัดเก็บข้อมูลต่างๆ เช่น ข้อมูลลูกค้า ข้อมูลการขนส่ง เป็นต้น

ด้านการจัดการสต็อกสินค้า เพื่อตรวจสอบชื่อรุ่นของสินค้า รหัสสินค้า และจำนวนของสินค้าคงเหลือ

ด้านการตลาด คิวอาร์โค้ดสามารถพัฒนาเป็นเครื่องมือทางการตลาดได้ [6] เช่น

- เครื่องมือในการเข้าถึงลิงค์เว็บไซต์เพื่อเข้าถึงข้อมูลเพิ่มเติม
- E-coupon โปรโมชั่นส่วนลด
- บอกตำแหน่งที่ตั้งร้านค้าแทนแผนที่
- E-commerce ช่องทางการซื้อและชำระเงิน
- เครื่องมือ Information ในรูปแบบข้อความ
- Human interest เรียกร้องความสนใจได้ เพราะไม่สามารถอ่านด้วยตาเปล่าได้

2.2.8 งานวิจัยที่เกี่ยวข้อง

จากการทบทวนวรรณกรรม ความไม่ปลอดภัยในการใช้บัตรเครดิต และการทำธุรกรรมทางการเงิน โดย Pieter de Bruyne [39] ได้กล่าวว่าการใช้บัตรเครดิตในปัจจุบัน ที่มีวิธีการตรวจสอบลายเซ็นที่สลิปกับตัวอย่างลายเซ็นที่บัตรด้วยสายตา ผู้ขายจะไม่ได้ตรวจสอบอย่างเคร่งครัด จนเป็นเหตุให้เกิดการฉ้อโกงได้ และแม้จะมีการใช้แถบแม่เหล็ก แต่แถบแม่เหล็กก็เป็นเครื่องมือในการตรวจบัตรที่ถูกขโมยหรือใช้ไม่ได้โดยอัตโนมัติ อีกทั้งยังมีข้อเสียที่ไม่รู้ว่าแถบแม่เหล็กเป็นของแท้หรือลอกเลียนแบบ นอกจากนั้น แทบแม่เหล็กยังไม่สามารถใช้ในการระบุตัวผู้ใช้ได้ นอกจากนั้น Young Sil Lee [40] ได้กล่าวถึงความไม่ปลอดภัยในการทำธุรกรรมทางการเงินผ่านระบบอินเทอร์เนต หรือ e-banking system ที่มีการขโมยข้อมูลด้วยวิธีระดับสูงที่เรียกว่า Phishing หรือ Pharming ซึ่งอันตรายกว่าการขโมย ID และ รหัสของผู้ใช้ เสียอีก

Sida Lin และ Qi Xie [41] กล่าวถึงการเพิ่มความปลอดภัยของการส่งผ่านข้อมูลระหว่างเครื่องคอมพิวเตอร์อย่างประสิทธิภาพโดยใช้การเข้ารหัสแบบทางเดียวที่เรียกว่า “ฟังก์ชันแฮช” ซึ่งจะอยู่ในขั้นตอนของการเปลี่ยนรหัสผ่านเป็นค่าแฮชที่มีความยาวคงที่และไม่มีความหมาย จากนั้นค่าแฮชดังกล่าวจะถูกเก็บไว้ในเครื่องแม่ข่ายเพื่อใช้ในการเปรียบเทียบและยืนยันตัวตนซึ่งจะให้ความปลอดภัยในการใช้งานมากกว่าการรวบรวมฐานข้อมูลของรหัสผ่านโดยตรง นอกจากนั้น Essam Abdel-azeem และคณะ [42] ได้กล่าวว่าฟังก์ชันแฮชในวิทยาการเข้ารหัสลับถูกนำมาใช้ประโยชน์ในเรื่องของการลงลายเซ็นดิจิทัล และการพิจารณาการพิสูจน์ตัวตนได้ โดยที่ฟังก์ชันแฮชเป็นฟังก์ชันแบบทางเดียวซึ่งไม่สามารถหาฟังก์ชันผกผันได้ ดังนั้นรหัสที่ได้จากฟังก์ชันแฮชจะไม่สามารถนำมาใช้ในการเรียกคืนรหัสดั้งเดิมกลับมาได้ อีกทั้งฟังก์ชันแฮชยังมีคุณสมบัติปลอดการ

ชนซึ่งให้ความปลอดภัยสูงเพราะความเป็นไปได้ที่รหัสผ่านสองชุดจะให้ค่าแฮชมีน้อยมาก ซึ่งสอดคล้องกับ Chuanhua Zhou และ Baohua Zhao [43] ที่ได้กล่าวว่า ฟังก์ชันแฮชได้นำมาใช้อย่างกว้างขวาง โดยเฉพาะอย่างยิ่งในการรักษาความปลอดภัยของการลงลายเซ็นดิจิทัลของธุรกิจผ่านทางเครือข่ายอินเทอร์เน็ต (E-Business) ที่ทำให้มั่นใจได้ว่ามีความปลอดภัยในการส่งผ่านข้อมูลและยืนยันตัวตนของทั้งสองฝ่ายที่ส่งข้อมูลหากันได้ถูกต้อง

Kuan-Chieh Liao และคณะ [44] ได้เสนอรูปแบบการส่งผ่านข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่มีความปลอดภัยด้วยการใช้ รหัสผ่านที่ใช้ครั้งเดียว (One-Time Password) ร่วมกับ QR-Code บนโทรศัพท์เคลื่อนที่ เพื่อป้องกันการแทรกแซงข้อมูลระหว่างการสื่อสารระยะไกลผ่านทางฮาร์ดแวร์ นอกจากนั้น Young Sil Lee [40] ก็ได้เสนอการยืนยันตัวตนของผู้ใช้บริการการทำธุรกรรมผ่านระบบอินเทอร์เน็ตด้วยวิธีการใช้ Mobile OTP ร่วมกับ QR-Code ซึ่งแตกต่างจากบาร์โค้ด 2 มิติโดยทั่วไป มีวิธีคือให้ธนาคารเป็นผู้ออก QR-Code โดยใช้ข้อมูลโอนเงินที่ผู้ใช้เป็นคนคีย์เข้าเครื่อง ซึ่งธนาคารเอารหัส OTP ไปเปลี่ยนเป็น QR-code แล้วส่งให้ผู้ใช้ เมื่อมีการใช้งานผู้ใช้ต้องอ่านรหัส QR-code ที่ธนาคารออกให้ ได้เป็นรหัส OTP แล้วจึงนำไปใช้ทำธุรกรรมได้

ซึ่งสอดคล้องกับเทคโนโลยี QR-TAN ของ Guenther Starnberger, Lorenz Froihofer and Karl M.Goeschka [45] ที่เสนอการทำธุรกรรมอิเล็กทรอนิกส์ หรือ Internet Banking โดยการใช้ QR-Code มายืนยันความถูกต้องเช่นเดียวกัน โดยเป็นการทำธุรกรรมแบบปิด (Offline) ที่ไม่จำเป็นต้องใช้ Server ทางสายที่เสี่ยงต่อการโจรกรรมข้อมูล เพราะตรวจสอบการยืนยันตัวตนที่โทรศัพท์มือถือด้วยการติดตั้ง Software เอาไว้ได้เลย ไม่ต้องส่งไปที่ เครื่องปลายทาง (Terminal) ตรวจสอบ

นอกจากนั้นแล้วยังมีงานวิจัยทางด้านเทคโนโลยีการยืนยันตัวตนของผู้ใช้บัตรเครดิตด้วยเทคโนโลยีบัตรเพลน (Plain card) ของ Pieter de Bruyne [39] ซึ่งกล่าวถึงบัตรที่มีลักษณะเรียบ ไม่มีการระบุชื่อ หมายเลข หรือลายเซ็นของผู้ใช้ โดยเปลี่ยนข้อมูลดังกล่าวเป็นรหัสหรือภาษาคอมพิวเตอร์และเก็บไว้ในรหัสแถบ (barcode) แถบแม่เหล็ก หรือหน่วยความจำอิเล็กทรอนิกส์แทนและมีการเพิ่มในส่วนของระบบการตรวจสอบลายเซ็นอัตโนมัติเพื่อยืนยันตัวตนด้วย ซึ่งคล้ายกับระบบรักษาความปลอดภัยในการใช้บัตรเครดิตของ Jung Eun Kim [46] ที่เสนอวิธีที่เรียกว่า NNCC (No Number Credit Card) คือเป็นบัตรเครดิตที่ไม่ระบุหมายเลขที่บัตร โดยเน้นการเพิ่มความปลอดภัยในการทำธุรกรรมบัตรเครดิตผ่านอินเทอร์เน็ต (On-line) โดยใช้ระบบการยืนยันตัวตนผ่านระบบที่เรียกว่า โปรโตคอล เคอร์บิรอส (Kerberos Protocol) เป็น

มาตรฐานอินเตอร์เน็ตที่ใช้สำหรับพิสูจน์สิทธิผู้ใช้ โดยเป็นการเข้ารหัส และเก็บข่าวสารที่จะระบุตัวผู้ใช้ รวมถึงพิสูจน์สิทธิผู้ใช้ของบุคคลนั้น ๆ เมื่อมีการสมัครเข้าใช้งาน

จากการทบทวนงานวิจัยที่เกี่ยวข้องกล่าวได้ว่าได้มีความพยายามนำเทคโนโลยีด้านต่างๆ เข้ามาใช้ในการป้องกันภัยในการทำธุรกรรมทางการเงิน ซึ่งสิ่งที่น่าสนใจคือมีการนำ QR-Code และฟังก์ชันแฮชมาใช้ในการยืนยันตัวตนเพื่อเพิ่มความปลอดภัยของผู้ใช้บริการบัตรเครดิตด้วย แต่เป็นการนำมาใช้ร่วมกับเทคโนโลยีที่แตกต่างกัน ยังไม่มีการนำมาใช้ร่วมกัน ซึ่งเป็นสิ่งที่น่าสนใจที่จะนำคุณสมบัติที่ดีของทั้งสองส่วนมาใช้ร่วมกันเพื่อพัฒนานวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตได้

บทที่ 3

วิธีดำเนินการวิจัย

วิธีดำเนินการวิจัยนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองที่รวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) ซึ่งเป็นซอฟต์แวร์เพื่อใช้ในการเพิ่มความปลอดภัยในการใช้บัตรเครดิต จะต้องอาศัยกระบวนการพัฒนาผลิตภัณฑ์ใหม่ (New Product development) ที่เกิดจากการศึกษาและการทบทวนทฤษฎีและงานวิจัยต่างๆตามรายละเอียดที่ได้กล่าวไว้ในบทที่ 2 โดยแบ่งงานวิจัยทั้งหมดเป็น 3 ส่วนคือ

1. ศึกษาความต้องการของกลุ่มตัวอย่าง และวิธีการที่มีความเหมาะสมต่อการพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิต ด้วยการหาข้อมูลจากแหล่งปฐมภูมิ และทุติยภูมิ

2. ดำเนินการทดลองเชิงวิทยาศาสตร์ของระบบการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสการตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption)

3. ดำเนินการด้านสังคมศาสตร์ โดยศึกษาความเป็นไปได้ในเชิงพาณิชย์ โดยการสำรวจการยอมรับในผลิตภัณฑ์นวัตกรรม

ซึ่งมีขั้นตอนการทำวิจัยดังนี้

1. ศึกษาความต้องการของกลุ่มตัวอย่าง และวิธีการที่มีความเหมาะสมต่อการพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิต ด้วยการหาข้อมูลจากแหล่งปฐมภูมิ และทุติยภูมิ

2. การดำเนินการทดลองเชิงวิทยาศาสตร์

- ทดลองพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่
- ทดสอบประสิทธิภาพของนวัตกรรมต้นแบบด้วยซอฟต์แวร์บนบัตรเสมือนที่มีโครงสร้างทางกายภาพใกล้เคียงกับบัตรเครดิตจริง
- สรุปผลการทดลอง

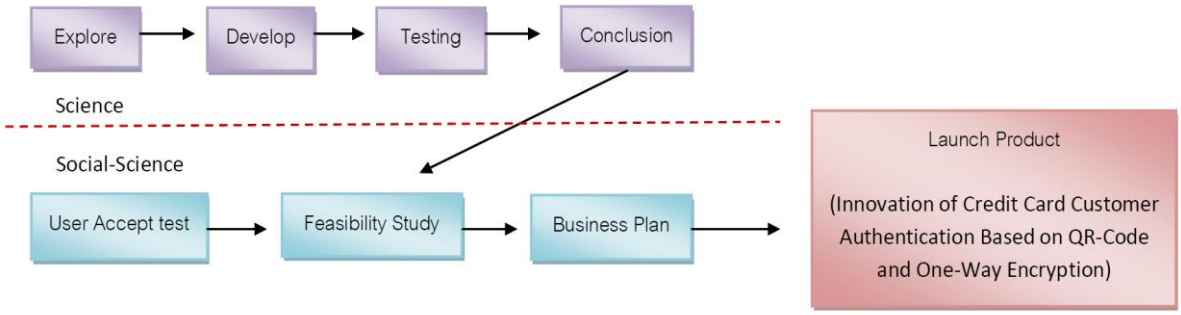
3. การนำผลการพัฒนาออกสู่เชิงพาณิชย์

- สำรวจการยอมรับของผู้บริโภค หลังการพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิต

- ศึกษาความเป็นไปได้ในการดำเนินธุรกิจระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่

- วางแผนกลยุทธ์การออกสู่เชิงพาณิชย์

ขั้นตอนวิธีวิจัย



ภาพที่ 3-1 ขั้นตอนวิธีวิจัย

3.1 ศึกษาความต้องการของกลุ่มตัวอย่าง และวิธีการที่มีความเหมาะสมต่อการพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิต ด้วยการหาข้อมูลจากแหล่งปฐมภูมิและทุติยภูมิ

การศึกษาแนวทางการและวิธีการที่มีความเหมาะสมต่อการพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิต ด้วยการหาข้อมูลจากแหล่งปฐมภูมิ และทุติยภูมิ ซึ่งในการศึกษางานวิจัยฉบับนี้ ผู้ทำการวิจัยทำการศึกษาข้อมูลจาก สื่อสารสนเทศ บทความทางวิชาการ วารสารทางด้านเทคโนโลยี สื่อของสถาบันการเงิน นวัตกรรมที่เกี่ยวข้องกับวิธีการปลอมแปลง และโจรกรรมข้อมูลบัตรเครดิต รวมถึง การป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตในรูปแบบต่างๆรวมทั้งและการหานวัตกรรมรูปแบบใหม่ๆ

- ข้อมูลทุติยภูมิ เป็นการเก็บข้อมูลที่ได้จากงานวิจัยที่เกี่ยวข้องกับปัจจัยที่มีผลต่อการใช้บัตรเครดิต พฤติกรรมการใช้บัตรเครดิต เครื่องมือที่นำมาใช้ในการพัฒนานวัตกรรม การรวบรวมข้อมูลจากเอกสารทางวิชาการ หนังสือ วารสาร สิ่งพิมพ์ และข้อมูลที่เผยแพร่ทางอินเตอร์เน็ตที่สามารถอ้างอิงถึงที่มาได้ ซึ่งมีประเด็นที่เกี่ยวข้องกับบัตรเครดิต

- ข้อมูลปฐมภูมิ เป็นการเก็บข้อมูลของผู้วิจัย โดยการสัมภาษณ์ และแจกแบบสอบถาม เพื่อสำรวจทัศนคติ และความต้องการต่อระบบการป้องกันการปลอมแปลงของบัตรเครดิต โดยใช้กลุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น (Non-Probability Sampling) วิธีการคัดเลือกตัวอย่างแบบสะดวก (Convenience Sampling) จำนวน 107 คน

<u>ประชากรและกลุ่มตัวอย่าง</u>

1. ประชากร

ใช้กลุ่มประชากรผู้เกี่ยวข้องกับบัตรเครดิต และอาศัยอยู่ในเขตกรุงเทพมหานคร โดยจำแนกกลุ่มประชากรออกเป็น 2 กลุ่ม ตามความเกี่ยวข้องกับบัตรเครดิตดังนี้

กลุ่มที่ 1 ผู้บริโภคทั่วไปที่ใช้บัตรเครดิต และผู้ประกอบการ/หน่วยงานที่เกี่ยวข้อง

กลุ่มที่ 2 ผู้บริโภคทั่วไปที่ไม่ใช้บัตรเครดิต

2. กลุ่มตัวอย่าง

ใช้กลุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น (Non-Probability Sampling) วิธีการคัดเลือกตัวอย่างแบบสะดวก (Convenience Sampling) จากกลุ่มประชากร 2 กลุ่มที่กล่าวข้างต้น

<u>การเก็บรวบรวมข้อมูล</u>

สำรวจความคิดเห็นและความต้องการ โดยให้กลุ่มตัวอย่างทำแบบสอบถามเพื่อศึกษาความคิดเห็นของผู้บริโภคในความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต เพื่อดูทัศนคติ และความต้องการต่อระบบต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต จากนั้นจึงให้กลุ่มตัวอย่างทดลองใช้ระบบนวัตกรรม และให้ทำแบบสอบถามอีกครั้งเพื่อศึกษาความพึงพอใจของผู้บริโภคต่อนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว **(QR-Code)** และการเข้ารหัสแบบทางเดียว **(One-way Encryption)** และทำการวิเคราะห์ข้อมูลจากแบบสอบถาม

<u>เครื่องมือที่ใช้ในการวิจัย</u>

ใช้แบบสอบถาม (Questionnaire) โดยได้จากการรวบรวมข้อมูลทั้งทฤษฎีและงานวิจัยที่เกี่ยวข้อง แบ่งออกเป็น 2 ฉบับ คือ แบบประเมินความต้องการในนวัตกรรม และแบบประเมินการยอมรับในนวัตกรรม โดยตั้งข้อคำถาม ออกเป็น 3 ส่วน คือ

ส่วนที่ 1 เป็นคำถามเกี่ยวกับตัวแปรที่ใช้ในการศึกษา 5 ด้าน คือ ความมีประโยชน์ ความง่ายในการใช้งาน ความน่าเชื่อถือ ทัศนคติต่อเทคโนโลยี และความตั้งใจในการใช้บริการ ลักษณะแบบสอบถามเป็นแบบมาตราส่วนประมาณค่า (Rating Scale) 5 ระดับ ได้แก่ มากที่สุด มาก ปานกลาง น้อย และน้อยที่สุด ซึ่งลักษณะคำถามจะกำหนดการให้คะแนนคำตอบของแบบสอบถาม โดยมีข้อที่ให้คะแนนรวมแบบ Rating Scale ดังนี้

5 หมายถึง มากที่สุด

4 หมายถึง มาก

3 หมายถึง ปานกลาง

2 หมายถึง น้อย

1 หมายถึง น้อยที่สุด

ส่วนที่ 2 เป็นคำถามเกี่ยวกับพฤติกรรมการใช้บัตรเครดิต เป็นการวัดโดยใช้คำถามแบบปลายปิด (Closed Ended) ซึ่งลักษณะคำถามจะเป็นแบบคำตอบหลายตัวเลือก (Multiple Choices) และคำถามปลายเปิด (Open-Ended Question) สำหรับให้ผู้ตอบแบบสอบถามแสดงความคิดเห็นหรือข้อเสนอแนะ

ส่วนที่ 3 เป็นคำถามเกี่ยวกับข้อมูลส่วนบุคคล ได้แก่ เพศ อายุ สถานภาพ ระดับการศึกษา อาชีพ รายได้ต่อเดือน วัดโดยการใช้คำถามแบบปลายปิด (Closed Ended) ซึ่งลักษณะ คำถามจะเป็นแบบคำตอบหลายตัวเลือก (Multiple Choices)

<u>คำถามในการวิจัย</u> <u>(แบบสอบถามที่ 1 ศึกษาความคิดเห็นของผู้บริโภคในความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต)</u>

1. ปัจจัยการรับรู้ในเรื่องต่างๆของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต โดยสอบถามจากตัวแปรที่ใช้ในการศึกษา 5 ด้าน คือ ความมีประโยชน์ ความง่ายในการใช้งาน ความน่าเชื่อถือ ทัศนคติต่อเทคโนโลยี และความตั้งใจในการใช้บริการ

2. พฤติกรรมการใช้บัตรเครดิต โดยให้ตอบคำถามเกี่ยวกับลักษณะการใช้บัตรเครดิต ทั้งกลุ่มที่มีการใช้บัตรเครดิต และไม่มีการใช้ จากนั้นให้แสดงความคิดเห็นหรือข้อเสนอแนะเกี่ยวกับระบบการป้องกันการปลอมแปลงบัตรเครดิต

3. ข้อมูลทั่วไป

<u>การศึกษาความคิดเห็นผู้บริโภคจากการทดสอบสมมติฐาน</u>

เป็นการศึกษาจากแบบสอบถามดังที่กล่าวไว้แล้วข้างต้น โดยแบ่งแบบสอบถามออกเป็น 2 แบบ คือ การสอบถามประเมินความต้องการในนวัตกรรม และการประเมินการยอมรับในนวัตกรรมภายหลังจากการพัฒนานวัตกรรมแล้ว โดยใช้แนวคิดทฤษฎีของตัวแบบการยอมรับเทคโนโลยี (Technology Acceptance Model) มาเป็นตัวแบบในการตั้งหัวข้อคำถาม คือ คุณลักษณะของผู้บริโภค การรับรู้ว่านวัตกรรมมีประโยชน์ การรับรู้ว่านวัตกรรมใช้งานง่าย ทัศนคติต่อผลิตภัณฑ์นวัตกรรม และความตั้งใจในการใช้นวัตกรรม โดยมีตัวแปรที่ใช้ในการศึกษา คือ

<u>ตัวแปรต้น</u>

1. **คุณลักษณะและการใช้งานของผู้บริโภค** ได้แก่ เพศ อายุ ระดับการศึกษา อาชีพ รายได้ และสถานภาพ
2. **ปัจจัยการรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตมีประโยชน์**ได้แก่ ความปลอดภัย
3. **ปัจจัยการรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตง่ายต่อการเรียนรู้การใช้งาน** เช่น ฟังค์ชันการให้บริการ และวิธีการเข้าถึงนวัตกรรม
4. **ปัจจัยการรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตมีความน่าเชื่อถือ** เช่น มั่นใจเรื่องการจัดเก็บข้อมูล และประสิทธิภาพของเทคโนโลยีเครือข่ายการให้บริการ
5. **ทัศนคติต่อเทคโนโลยีของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิต** เช่น ความชอบ ความคุ้มค่า ความแปลกใหม่ และความทันสมัยของเทคโนโลยี

<u>ตัวแปรตาม</u>

ความต้องการใช้บริการนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิต (ความสนใจที่จะใช้บริการ , ความตั้งใจที่จะมาใช้บริการ)

จากตัวแปรต้น และตัวแปรตามที่ได้กำหนดขึ้น นำมาตั้งเป็นข้อคำถามได้ดังนี้

<u>ตัวแปรต้น</u>

1. คุณลักษณะและการใช้งานของผู้บริโภค ได้แก่ เพศ อายุ สถานภาพ ระดับการศึกษา อาชีพ รายได้

   <u>ข้อคำถาม</u>

เป็นคำถามเกี่ยวกับข้อมูลส่วนบุคคล ได้แก่ เพศ อายุ สถานภาพ ระดับการศึกษา อาชีพ รายได้ต่อเดือน วัดโดยการใช้คำถามแบบปลายปิด (Closed Ended) ซึ่งลักษณะ คำถามจะเป็นแบบคำตอบหลายตัวเลือก (Multiple Choices)

2. ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต มีประโยชน์

ข้อคำถาม

- คุณคิดว่าการป้องกันการปลอมแปลงลายเซ็นมีความจำเป็น
- คุณคิดว่าบัตรเครดิตจะต้องมีระบบป้องกันการปลอมแปลงให้มากกว่าที่มีอยู่
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความคุ้มค่าในการสมัครใช้บริการบัตรเครดิต
- คุณคิดว่าระบบการป้องกันการปลอมแปลงลายเซ็นจะเป็นทางเลือกใหม่ในการป้องกันความปลอดภัยในการใช้บัตรเครดิต

3. ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต ง่ายต่อการเรียนรู้การใช้งาน

ข้อคำถาม

- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นไม่เป็นอุปสรรคกับการใช้งานบัตรเครดิตที่มีอยู่
- คุณคิดว่าต้องสามารถเข้าถึงระบบป้องกันการปลอมแปลงลายเซ็นได้ทุกที่ ทุกเวลา
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นต้องมีขั้นตอนสะดวก และกระชับ ง่ายต่อการใช้งาน

4. ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต มีความน่าเชื่อถือ

ข้อคำถาม

- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็น สามารถนำไปใช้ได้จริง
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นจะสามารถลดความเสี่ยงต่อการถูกโจรกรรมได้

5. ทัศนคติต่อเทคโนโลยี ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

ข้อคำถาม

- คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นมีความน่าสนใจ
- คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความมั่นใจในการทำธุรกรรมทางการเงิน

ตัวแปรตาม

ความต้องการในการใช้บริการระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต คือ ความสนใจที่จะใช้บริการ ความตั้งใจที่จะมาใช้บริการ

ข้อคำถาม

- คุณตั้งใจว่าจะใช้เทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นในอนาคต
- คุณคิดว่าจะแนะนำให้เพื่อน หรือคนรู้จักใช้ระบบการป้องกันการปลอมแปลงลายเซ็น

โดยการวิเคราะห์ตัวแปรเหล่านี้ จะใช้ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (SD) เพื่อคำนวณหาค่าระดับความคิดเห็นของกลุ่มตัวอย่าง เพื่อแปลความหมาย โดยใช้เกณฑ์ในการวิเคราะห์และแปลผลข้อมูล ดังนี้

คะแนนเฉลี่ย	4.50-5.00	กำหนดให้อยู่ในเกณฑ์	มากที่สุด
คะแนนเฉลี่ย	3.50-4.49	กำหนดให้อยู่ในเกณฑ์	มาก
คะแนนเฉลี่ย	2.50-3.49	กำหนดให้อยู่ในเกณฑ์	ปานกลาง
คะแนนเฉลี่ย	1.50-2.49	กำหนดให้อยู่ในเกณฑ์	น้อย
คะแนนเฉลี่ย	1.00-1.49	กำหนดให้อยู่ในเกณฑ์	น้อยที่สุด

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลที่ได้จากแบบสอบถาม โดยใช้โปรแกรมสำเร็จรูป SPSS for Windows ซึ่งการวิเคราะห์ข้อมูลเพื่อนำเสนอ และสรุปข้อมูลในการวิจัยครั้งนี้ ได้ใช้การคำนวณค่าสถิติ โดยสถิติที่ใช้กันอยู่ในทางวิจัย แบ่งออกได้เป็น 2 ประเภทใหญ่ ๆ คือ

1. สถิติเชิงบรรยายหรือสถิติเชิงพรรณนา (Descriptive Statistics) เป็นสถิติที่บรรยายคุณลักษณะของสิ่งที่ต้องการศึกษา จากกลุ่มใดกลุ่มหนึ่งโดยเฉพาะ ซึ่งอาจจะเป็นกลุ่มเล็กหรือกลุ่มใหญ่ก็ได้ ผลที่ได้จากการศึกษาไม่สามารถนำไปอ้างอิงถึงกลุ่มประชากร (Population) ได้ สถิติที่ใช้ในการบรรยายคุณลักษณะของข้อมูล ได้แก่ ความถี่ (Frequency) ร้อยละ (Percentage) ค่าเฉลี่ย (Mean) มัธยฐาน (Median) พิสัย (Range) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

- **ค่าร้อยละ (Percentage)** เป็นค่าสถิติที่นิยมใช้กันมาก โดยเป็นการเปรียบเทียบความถี่ หรือจำนวนที่ต้องการกับความถี่หรือจำนวนทั้งหมดที่เทียบเป็น 100 เป็นสถิติที่นิยมใช้กันมากในการวิจัยเพราะเป็นตัวเลขที่เข้าใจ ง่าย ดังนั้นในการคำนวณหาค่าร้อยละจึงใช้ตัวเลขของข้อมูลที่เราต้องการเปรียบเทียบคูณด้วย 100 แล้วหารด้วยจำนวนเต็มของข้อมูลนั้น

- **ค่าเฉลี่ย ($\bar{x}$)** เป็นสถิติที่ใช้เป็นตัวแทนของข้อมูล คือค่าเฉลี่ยของข้อมูลที่ต้องการศึกษา ซึ่งคำนวณได้จากการนำเอาค่าทั้งหมดที่รวบรวมได้มารวมกันเข้าแล้วหารด้วยจำนวนของค่าเหล่านั้น

- ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation: SD) เป็นการวัดการกระจายของข้อมูล เขียนแทนด้วย S.D. หรือ S

2. สถิติเชิงอ้างอิงหรือสถิติอนุมาน (Inferential Statistics) เป็นสถิติที่ศึกษาข้อมูลจากกลุ่มตัวอย่าง (Sample) แล้วนำผลสรุปที่ได้จากกลุ่มตัวอย่าง สรุปอ้างอิงไปยังลักษณะประชากร โดยสถิติที่อ้างอิงจะเกี่ยวกับการประมาณค่า (Estimation) และการทดสอบสมมติฐาน (Hypothesis Testing) โดยการทดสอบงานวิจัยนี้อยู่บนพื้นฐานของการทดสอบสมมติฐานด้วยวิธีไคสแควร์และค่าสัมประสิทธิสหสัมพันธ์จากกลุ่มตัวอย่างผู้ใช้ 107 คน

3.2 การดำเนินการทดลองเชิงวิทยาศาสตร์

3.2.1 ทดลองพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่

โดยที่ตัวแบบในการวิจัย (Model) จะใช้แนวคิดของการพิสูจน์ทราบตัวตนมาประยุกต์ใช้เข้ากับคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว

1. การสร้างโปรแกรม และปรับเปลี่ยนรูปแบบวิธีเพื่อให้เข้ากับการใช้งานจริง
2. ทดลองสร้างนวัตกรรมต้นแบบ

3.2.2 การทดสอบประสิทธิภาพของนวัตกรรมต้นแบบ

1. การวัดความปลอดภัยในการใช้ระบบ
   - ใช้วิธีการคำนวณจากการนับ (Counting)
   - อ้างอิงจากผลงานวิจัยที่เกี่ยวข้อง
2. การทดลองใช้งานอุปกรณ์จำลอง
   - ทำการทดสอบบนบัตรเสมือนที่มีโครงสร้างทางกายภาพใกล้เคียงกับบัตรเครดิตจริง
   - อุปกรณ์การอ่านรหัสตอบสนองอย่างรวดเร็ว (QR-Code) ใช้โปรแกรมสำเร็จรูปแบบเดียวกับโปรแกรมของโทรศัพท์เคลื่อนที่
   - ขั้นตอนวิธีการเข้ารหัสทางเดียว พัฒนาโปรแกรมบนเครื่องคอมพิวเตอร์ และใช้ฟังก์ชันในการเข้ารหัส โดยตั้งอยู่บนพื้นฐานของฟังก์ชันแฮช ซึ่งใช้เพียงรูปแบบเดียวเท่านั้น

- การป้อนรหัส (Password) เพื่อแปลงเป็นค่า Hash นั้น ใช้คีย์บอร์ดขนาดเล็ก เชื่อมต่อด้วยสัญญาณบลูทูธ เพื่อความสะดวกในการป้อนรหัส และปกปิดบุคคลภายนอก

3.2.3 สรุปผลการทดลอง

สรุปข้อดีและข้อด้อยของการทดสอบประสิทธิภาพนำมาปรับปรุง และศึกษาเพื่อนำนวัตกรรมออกสู่เชิงพาณิชย์

3.3 การนำผลการพัฒนาออกสู่เชิงพาณิชย์

3.3.1 สำรวจการยอมรับของผู้บริโภค หลังการพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิต

ทางด้านการยอมรับในผลิตภัณฑ์ของผู้บริโภค ได้สร้างตัวแปรขึ้นมาเป็นกรอบในการศึกษา โดยได้พื้นฐานมาจากตัวแบบการยอมรับเทคโนโลยี (TAM Model) ซึ่งเป็นตัวแปรที่นำมาใช้ศึกษาทั้งทางด้านความต้องการ และการยอมรับในตัวผลิตภัณฑ์

ภาพที่ 3-2 การแสดงกรอบแนวคิดในการวิจัย

โดยในส่วนของการยอมรับนั้น แบ่งเป็น 2 ส่วน คือ ส่วนแรกเป็นวิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) ของผู้ที่มีส่วนเกี่ยวข้องในการลงทุนธุรกิจบัตรเครดิต ซึ่งใช้กลุ่มตัวอย่างในการสัมภาษณ์ธนาคารผู้มีส่วนเกี่ยวข้องกับบัตรเครดิต 1 แห่ง คือ ธนาคารกสิกรไทย ส่วนที่สองให้กลุ่มตัวอย่างดูวิธีการทดลองใช้ระบบจากวิดีโอสาธิต และทำการเก็บข้อมูลด้วยแบบสอบถาม โดยในการเก็บข้อมูลนี้ ผู้วิจัยได้ออกแบบสอบถาม (Questionnaire) ซึ่งเป็นเครื่องมือที่ใช้ในการประเมินการวิจัย เพื่อทดสอบเรื่องความสะดวกในการใช้งาน จากกลุ่มตัวอย่างจำนวน 50 คน และร้านค้า

คำถามในการวิจัย (แบบสอบถามที่ 2 ศึกษาการยอมรับของผู้บริโภคต่อนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption)

1. ปัจจัยการรับรู้ในเรื่องต่างๆของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต โดยสอบถามจากตัวแปรที่ใช้ในการศึกษา 5 ด้าน คือ ความมีประโยชน์ ความง่ายในการใช้งาน ความน่าเชื่อถือ ทัศนคติต่อเทคโนโลยี และความตั้งใจในการใช้บริการ

2. ข้อมูลทั่วไป

จากนั้นดำเนินการวิเคราะห์ข้อมูลด้วยวิธีทางสถิติ โดยประมวลผลด้วยโปรแกรม SPSS และสรุปความคิดเห็น ต่อไปก็วางแผนเพื่อที่จะนำระบบนวัตกรรมยืนยันตัวตนด้วยคิวอาร์โค้ดและการเข้ารหัสแบบทางเดียวออกสู่เชิงพาณิชย์

3.3.2 ศึกษาความเป็นไปได้ในการดำเนินธุรกิจระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่

ศึกษาความเป็นไปได้ในการดำเนินธุรกิจระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่ ด้วยการหาข้อมูลจากแหล่งปฐมภูมิ และทุติยภูมิ แบ่งเป็น 2 ด้าน คือ

1. จากผลการวิเคราะห์การศึกษาความต้องการ และการยอมรับในนวัตกรรมการยืนยันตัวตนของบัตรเครดิต

2. จากการวิเคราะห์ตลาดด้วยเครื่องมือต่างๆ เช่น

(1) SWOT Analysis วิเคราะห์ข้อมูลที่พิจารณาความเป็นไปได้ทางการตลาด

(2) Market Trend วิเคราะห์แนวโน้มของตลาด

(3) Target Market วิเคราะห์ตลาดกลุ่มเป้าหมาย

3.3.3 วางแผนกลยุทธ์การออกสู่เชิงพาณิชย์

การเตรียมนำผลิตภัณฑ์ออกสู่ตลาดเป็นส่วนหนึ่งของกลยุทธ์ในแผนธุรกิจ (Business Plan) เรื่องการวางแผนทางการตลาด ซึ่งเมื่อทำการวิเคราะห์ตลาดด้วยเครื่องมือข้างต้นแล้ว ขั้นต่อไปคือ

1. วางกลยุทธ์ในการนำผลิตภัณฑ์ออกสู่เชิงพาณิชย์

การวางกลยุทธ์จะใช้หลักของ 4Ps คือ

(1) Product การกำหนดตัวผลิตภัณฑ์ให้เหมาะสมกับเป้าหมาย

(2) Price ตั้งราคาให้เหมาะสมกับผลิตภัณฑ์ และกลุ่มเป้าหมาย

(3) Place โดยคำนึงถึง 2 เรื่อง คือ

- ช่องทางการจัดจำหน่าย (Chanel of Distribution)
- การกระจายตัวสินค้า (Product of Distribution)

(4) Promotion มีการส่งเสริมตลาด เพื่อแจ้งข่าวสารหรือชักจูงให้เกิดทัศนคติและพฤติกรรมการซื้อ

2. การวางแผนการลงทุน โดยวิเคราะห์ในเรื่องต้นทุนโครงการ และ การคาดการณ์รายได้

บทที่ 4
ผลการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลในการวิจัยเรื่องนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) จะแบ่งออกเป็น 4 ส่วน คือ 1.ศึกษาความคิดเห็นของผู้บริโภคในความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต 2. การพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่ 3. การทดสอบประสิทธิภาพของระบบ 4. ศึกษาการยอมรับของผู้บริโภคต่อนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) โดยส่วนที่ 1 และ 4 จะวิเคราะห์จากข้อมูลพื้นฐานของกลุ่มตัวอย่าง และการทดสอบสมมติฐานที่ได้ตั้งไว้ ส่วนที่ 2 และ 3 จะแสดงถึงการพัฒนาระบบและการทดสอบ

4.1 การศึกษาความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

ผู้วิจัยนำข้อมูลจากแบบสอบถามที่ได้แจกให้กลุ่มตัวอย่างจำนวน 107 คนและได้รับกลับคืนมา 107 คน คิดเป็นร้อยละ 100 ในการวิเคราะห์ข้อมูลโดยได้ผลดังนี้

4.1.1 การวิเคราะห์ข้อมูลพื้นฐานของกลุ่มตัวอย่าง

- ลักษณะทางประชากร (เพศ)

ตารางที่ 4-1 ลักษณะทางประชากร (เพศ)

เพศ	ความถี่	ร้อยละ
ชาย	32	29.9
หญิง	75	70.1
รวม	107	100.0

จากตารางที่ 4-1 พบว่า จากกลุ่มตัวอย่างทั้งหมด 107 คน เป็นเพศชายจำนวน 32 คน คิดเป็นร้อยละ 29.9 กลุ่มตัวอย่างเป็นเพศหญิงจำนวน 75 คน คิดเป็นร้อยละ 70.1

- ลักษณะทางประชากร (อายุ)

ตารางที่ 4-2 ลักษณะทางประชากร (อายุ)

อายุ (ปี)	ความถี่	ร้อยละ
20-29	49	45.8
30-39	34	31.8
40-49	17	15.9
50-59	7	6.5
รวม	107	100.0

พบว่า กลุ่มตัวอย่างส่วนใหญ่มีอายุระหว่าง 20-29 ปี (ร้อยละ 45.8) รองลงมาจะมีอายุระหว่าง 30-39 ปี (ร้อยละ 31.8) และอายุ 40-49 ปี มีร้อยละ 15.9 ตามลำดับ

- ลักษณะทางประชากร (สถานภาพ)

ตารางที่ 4-3 ลักษณะทางประชากร (สถานภาพ)

สถานภาพ	ความถี่	ร้อยละ
โสด	85	79.4
สมรส	19	17.8
หม้าย/หย่า	3	2.8
รวม	107	100.0

พบว่า กลุ่มตัวอย่างส่วนใหญ่มีสถานภาพโสดร้อยละ 79.4 และสมรสรองลงมาร้อยละ 17.8 ส่วนหม้าย/หย่ามีร้อยละ 2.8

- ลักษณะทางประชากร (ระดับการศึกษา)

ตารางที่ 4-4 ลักษณะทางประชากร (ระดับการศึกษา)

ระดับการศึกษา	ความถี่	ร้อยละ
ต่ำกว่าปริญญาตรี	10	9.3
ปริญญาตรี	80	74.8
ปริญญาโท	16	15.0
สูงกว่าปริญญาโท	1	0.9
รวม	107	100.0

พบว่า กลุ่มตัวอย่างส่วนใหญ่มีระดับการศึกษาที่ระดับปริญญาตรี จำนวน 80 คน (ร้อยละ 74.8) รองลงมามีการศึกษาระดับปริญญาโทจำนวน 16 คน (ร้อยละ 15.0)

- ลักษณะทางประชากร (อาชีพ)

ตารางที่ 4-5 ลักษณะทางประชากร (อาชีพ)

อาชีพ	ความถี่	ร้อยละ
เอกชน	45	42.1
ข้าราชการ	44	41.1
รัฐวิสาหกิจ	10	9.3
ธุรกิจส่วนตัว	8	7.5
รวม	107	100.0

พบว่า กลุ่มตัวอย่างส่วนใหญ่มีอาชีพพนักงานบริษัทเอกชน 45 คน คิดเป็นร้อยละ 42.1 รองลงมามีอาชีพข้าราชการ มีจำนวน 44 คน คิดเป็นร้อยละ 41.1 โดยที่กลุ่มอาชีพธุรกิจส่วนตัวมีจำนวนน้อยที่สุด 8 คน คิดเป็นร้อยละ 7.5

- ลักษณะทางประชากร (รายได้ต่อเดือน)

ตารางที่ 4-6 ลักษณะทางประชากร (รายได้ต่อเดือน)

รายได้ต่อเดือน (บาท)	ความถี่	ร้อยละ
15,000-25,000	89	83.2
25,001-35,000	7	6.5
35,001-45,000	6	5.6
45,001-55,000	1	0.9
55,001 ขึ้นไป	4	3.7
รวม	107	100.0

พบว่า กลุ่มตัวอย่างส่วนใหญ่มีรายได้ 15,000 - 25,000 บาท มีจำนวน 89 คน (ร้อยละ 83.2) รองลงมามีรายได้อยู่ระหว่าง 25,001-35,000 มีจำนวน 7 คน (ร้อยละ 6.5)

4.1.2 การวิเคราะห์ข้อมูลจากพฤติกรรมการใช้บัตรเครดิตของกลุ่มตัวอย่าง ได้ผลตามข้อคำถาม ดังนี้

- ท่านมีบัตรเครดิตหรือไม่

ตารางที่ 4-7 จำนวนผู้ถือบัตรเครดิต

	ความถี่	ร้อยละ
มีบัตรเครดิต	62	57.9
ไม่มีบัตรเครดิต	45	42.1
รวม	107	100.0

พบว่า กลุ่มตัวอย่างส่วนใหญ่มีบัตรเครดิต 62 คน (ร้อยละ 57.9) และไม่มีบัตรเครดิต 45 คน (ร้อยละ 42.1)

- ความถี่ในการใช้บัตรเครดิตต่อเดือน (สำรวจเฉพาะผู้ที่มีบัตรเครดิต)

ตารางที่ 4-8 ความถี่ในการใช้บัตรเครดิตต่อเดือน

	ความถี่	ร้อยละ
ไม่มีการใช้	2	3.2
1-5 ครั้ง	53	85.5
6-10 ครั้ง	7	11.3
รวม	62	100.0

พบว่า ในกลุ่มที่ใช้บัตรเครดิตมีความถี่ในการใช้บัตรอยู่ที่ 1-5 ครั้งต่อเดือน คิดเป็นร้อยละ 85.5 รองลงมาคือ 6-10 ครั้ง คิดเป็นร้อยละ 11.3 และผู้ที่มีบัตรเครดิตแต่ไม่มีการใช้งาน เป็นจำนวนร้อยละ 3.2 ตามลำดับ

- ท่านใช้บัตรเครดิตในเรื่องใดบ่อยครั้งที่สุด (สำรวจเฉพาะผู้ที่ใช้บัตรเครดิต)

ตารางที่ 4-9 วัตถุประสงค์ในการใช้บัตรเครดิต

	ความถี่	ร้อยละ
ใช้ซื้อสินค้าอุปโภค-บริโภค	45	75
ใช้ชำระค่าสาธารณูปโภค	6	10
ใช้เบิกเงินสดล่วงหน้า	6	10
อื่นๆ (ผ่อนสินค้า, สะสมแต้ม)	3	5
รวม	60	100.0

จากตารางที่ 4-9 พบว่า ในกลุ่มที่ใช้บัตรเครดิตมีวัตถุประสงค์ในการใช้บัตรเครดิตในเรื่องอุปโภค-บริโภคมากที่สุดคือ ร้อยละ 75 ใช้ชำระค่าสาธารณูปโภค กับใช้เบิกเงินสดล่วงหน้า มีจำนวนเท่ากัน คือ ร้อยละ 10 และมีวัตถุประสงค์ในด้านอื่นๆ เช่น ผ่อนสินค้า หรือสะสมแต้มแลกรางวัล มีร้อยละ 5

- สาเหตุที่ท่านไม่ใช้บัตรเครดิต (สำรวจเฉพาะผู้ที่ไม่ใช้บัตรเครดิต)

ตารางที่ 4-10 เหตุผลที่ไม่ใช้บัตรเครดิต

	ความถี่	ร้อยละ
ไม่มั่นใจในเรื่องความปลอดภัย	10	21.3
ไม่อยากมีหนี้สิน	28	59.5
ไม่สะดวกในการใช้งาน	6	12.8
อื่นๆ (ไม่ชอบบริการของธนาคาร/ ความยุ่งยากในการทำบัตร)	3	6.4
รวม	47	100.0

พบว่า ในกลุ่มคนที่ไม่ใช้บัตรเครดิต โดยรวมกลุ่มคนที่ไม่มีบัตรเครดิต กับกลุ่มคนที่มีบัตรเครดิตแต่ไม่มีการใช้ คิดเป็นร้อยละ 43.9 โดยสาเหตุที่ไม่ใช้บัตรเครดิตมากที่สุดคือไม่อยากมีหนี้สินคิดเป็นร้อยละ 59.5 รองลงมาคือ ไม่มั่นใจในเรื่องความปลอดภัย คิดเป็นร้อยละ 21.3

ผลที่ได้จากการสำรวจข้อมูลทั่วไปของกลุ่มตัวอย่าง และพฤติกรรมการใช้บัตรเครดิต

จากผลการวิเคราะห์พบว่า ลักษณะของกลุ่มตัวอย่าง โดยส่วนมากเป็นเพศหญิง โดยอยู่ในช่วงอายุ 20-29 ปี ซึ่งมีระดับการศึกษาปริญญาตรี ซึ่งสอดคล้องกับงานวิจัยของ วุฒิชัย เชื้อวงศ์พรหม [47] ที่ว่าผู้ใช้บัตรเครดิตส่วนใหญ่ มีการศึกษาระดับปริญญาตรี เพราะมีระดับวิจารณญาณระดับหนึ่งในการตัดสินใจทำบัตรเครดิตได้ ส่วนมากมีอาชีพเป็นพนักงานบริษัทเอกชน และมีรายได้เฉลี่ยต่อเดือนคือ 15,000-25,000 บาท ซึ่งมีพฤติกรรมการใช้บัตรเครดิตคือ ส่วนใหญ่จะมีบัตรเครดิต และมีการใช้จ่ายผ่านบัตร ประมาณ 1-5 ครั้งต่อเดือน โดยใช้บัตรเครดิตในเรื่องการซื้อสินค้าอุปโภค-บริโภค มากที่สุด รองลงมาคือใช้ชำระค่าสาธารณูปโภค และการเบิกเงินสดล่วงหน้า

ส่วนในกลุ่มที่ไม่ได้ใช้บัตรเครดิต โดยรวมทั้งกลุ่มที่มีบัตรเครดิตแต่ไม่ได้ใช้ กับกลุ่มที่ไม่มีบัตรเครดิต คิดเป็นร้อยละ 43.9 พบว่าที่ไม่ใช้บัตรเครดิตมีสาเหตุเกิดจากไม่อยากมีหนี้สินมากที่สุด คือ 28 คน คิดเป็นร้อยละ 59.5 รองลงมาคือ กังวลในเรื่องความปลอดภัย (การปลอมแปลงการโจรกรรม) คิดเป็นร้อยละ 21.3 โดยมีความคิดเห็นเพิ่มเติมว่า อยากให้มีระบบป้องกันที่ซับซ้อนมากขึ้นกว่าเดิม และนอกจากการป้องกันการปลอมแปลงแล้ว อยากให้มีความปลอดภัยเกี่ยวกับ

ข้อมูลของผู้ถือบัตรด้วย ต้องการให้ปกปิดข้อมูลเพื่อป้องกันการซื้อขายข้อมูลไม่ให้ตกอยู่ในมือของมิจฉาชีพได้

4.1.3 การวิเคราะห์ข้อมูลจากปัจจัยที่มีอิทธิพลต่อความต้องการใช้บริการ

สำรวจจากกลุ่มตัวอย่างทั้งหมด 107 คน รวมทั้งกลุ่มที่มีบัตรเครดิต และไม่มีบัตรเครดิต โดยแต่ละข้อคำถามมีคะแนนเต็ม 5 คะแนน โดยใช้เกณฑ์ในการวิเคราะห์และแปลผลข้อมูลดังนี้

คะแนนเฉลี่ย	4.50-5.00	กำหนดให้อยู่ในเกณฑ์	มากที่สุด
คะแนนเฉลี่ย	3.50-4.49	กำหนดให้อยู่ในเกณฑ์	มาก
คะแนนเฉลี่ย	2.50-3.49	กำหนดให้อยู่ในเกณฑ์	ปานกลาง
คะแนนเฉลี่ย	1.50-2.49	กำหนดให้อยู่ในเกณฑ์	น้อย
คะแนนเฉลี่ย	1.00-1.49	กำหนดให้อยู่ในเกณฑ์	น้อยที่สุด

- ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต มีประโยชน์

ตารางที่ 4-11 ค่าเฉลี่ยของข้อคำถาม “ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต มีประโยชน์”

ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต มีประโยชน์	Mean	Std. Deviation	ระดับ
- คุณคิดว่าการป้องกันการปลอมแปลงลายเซ็นมีความจำเป็น	4.7757	.48191	มากที่สุด
- คุณคิดว่าบัตรเครดิตจะต้องมีระบบป้องกันการปลอมแปลงให้มากกว่าที่มีอยู่	4.7196	.52834	มากที่สุด
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความคุ้มค่าในการสมัครใช้บริการบัตรเครดิต	4.5234	.70505	มากที่สุด
- คุณคิดว่าระบบการป้องกันการปลอมแปลงลายเซ็นจะเป็นทางเลือกใหม่ในการป้องกันความปลอดภัยในการใช้บัตรเครดิต	4.4486	.69000	มาก
ค่าเฉลี่ย ($\bar{x}$)	4.6168		มากที่สุด

แสดงให้เห็นว่า ระดับความคิดเห็นเกี่ยวกับการรับรู้ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีประโยชน์ เฉลี่ยอยู่ในระดับมากที่สุด ($\bar{x}$ = 4.6168) เมื่อพิจารณาเป็นรายข้อพบว่าข้อที่มีความเห็นอยู่ในเกณฑ์ที่สูงสุดคือ คุณคิดว่าการป้องกันการปลอมแปลงลายเซ็นมีความจำเป็น

- ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการเรียนรู้ใช้งาน

ตารางที่ 4-12 ค่าเฉลี่ยของข้อคำถาม “ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการเรียนรู้ใช้งาน”

ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการเรียนรู้ใช้งาน	Mean	Std. Deviation	ระดับ
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นจะไม่เป็นอุปสรรคกับการใช้งานบัตรเครดิตที่มีอยู่	4.0654	.90357	มาก
- คุณคิดว่าต้องสามารถเข้าถึงระบบป้องกันการปลอมแปลงลายเซ็น ได้ทุกที่ ทุกเวลา	4.3178	.78426	มาก
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นต้องมีขั้นตอนสะดวก และกระชับ ง่ายต่อการใช้งาน	4.4393	.75458	มาก
ค่าเฉลี่ย ($\bar{x}$)	4.2742		มาก

แสดงให้เห็นว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการเรียนรู้ใช้งาน เฉลี่ยอยู่ในระดับมาก ($\bar{x}$ = 4.2742) เมื่อพิจารณาเป็นรายข้อพบว่า ข้อที่มีความเห็นอยู่ในเกณฑ์ที่สูงสุดคือ คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นต้องมีขั้นตอนสะดวก และกระชับ ง่ายต่อการใช้งาน

- ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความน่าเชื่อถือ

ตารางที่ 4-13 ค่าเฉลี่ยของข้อคำถาม “ปัจจัยการรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความน่าเชื่อถือ”

ปัจจัยการรับรู้ว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความน่าเชื่อถือ	Mean	Std. Deviation	ระดับ
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็น สามารถนำไปใช้ได้จริง	4.0374	.80006	มาก
- คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นจะสามารถลดความเสี่ยงต่อการถูกโจรกรรมได้	4.0467	.76950	มาก
ค่าเฉลี่ย ($\bar{x}$)	4.0421		มาก

แสดงให้เห็นว่า ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความน่าเชื่อถือเฉลี่ยอยู่ในระดับมาก ($\bar{x}$ = 4.0421) เมื่อพิจารณาเป็นรายข้อพบว่า ข้อที่มีความเห็นอยู่ในเกณฑ์ที่สูงสุดคือ คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นจะสามารถลดความเสี่ยงต่อการถูกโจรกรรมได้

- ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

ตารางที่ 4-14 ค่าเฉลี่ยของข้อคำถาม “ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต”

ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	Mean	Std. Deviation	ระดับ
- คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นมีความน่าสนใจ	4.3084	.67867	มาก
- คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความมั่นใจในการทำธุรกรรมทางการเงิน	4.3271	.69738	มาก
ค่าเฉลี่ย ($\bar{x}$)	4.3178		มาก

แสดงให้เห็นว่า ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต เฉลี่ยอยู่ในระดับมาก ($\bar{x}$ = 4.3178) เมื่อพิจารณาเป็นรายข้อพบว่า ข้อที่มีความเห็นอยู่ในเกณฑ์ที่สูงสุดคือ คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความมั่นใจในการทำธุรกรรมทางการเงิน

- ความต้องการในการใช้บริการระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

ตารางที่ 4-15 ค่าเฉลี่ยของข้อคำถาม “ความต้องการในการใช้บริการระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต”

ความต้องการในการใช้บริการระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	Mean	Std. Deviation	ระดับ
- คุณต้องการว่าจะใช้เทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นในอนาคต	4.3738	.68022	มาก
- คุณคิดว่าจะแนะนำให้เพื่อน หรือคนรู้จักใช้ระบบการป้องกันการปลอมแปลงลายเซ็น	4.2336	.72136	มาก
ค่าเฉลี่ย ($\bar{x}$)	4.3037		มาก

แสดงให้เห็นว่า ความต้องการในการใช้ระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต เฉลี่ยอยู่ในระดับมาก ($\bar{x}$ = 4.3037) เมื่อพิจารณาเป็นรายข้อพบว่า ข้อที่มีความเห็นอยู่ในเกณฑ์ที่สูงสุดคือ คุณต้องการว่าจะใช้เทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นในอนาคต

ผล : จากตารางแสดงค่าตัวแปรที่เกี่ยวข้องกับความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตข้างต้น พบว่าคำตอบจากข้อคำถามในแบบสอบถามมีค่าเฉลี่ยอยู่ในระดับมาก คือ 4.3551 ซึ่งแสดงให้เห็นว่ากลุ่มตัวอย่างมีความสนใจในระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตในระดับมาก

4.1.4 การวิเคราะห์การทดสอบสมมติฐาน

จากตัวแปรต้น และตัวแปรตาม ดังที่ได้กล่าวไว้ในบทที่ 3 สามารถตั้งสมมติฐานการวิจัยได้ดังนี้

สมมติฐานที่ 1: การรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตมีประโยชน์ มีความสัมพันธ์กับทัศนคติต่อเทคโนโลยีของระบบการยืนยันตัวตนของผู้ใช้บัตรเครดิต

สมมติฐานที่ 2: การรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตง่ายต่อการใช้งาน มีความสัมพันธ์กับทัศนคติต่อเทคโนโลยีของระบบการยืนยันตัวตนของผู้ใช้บัตรเครดิต

สมมติฐานที่ 3: ทัศนคติต่อเทคโนโลยีของระบบการยืนยันตัวตนของผู้ใช้บัตรเครดิต มีความสัมพันธ์กับความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

สมมติฐานที่ 4: ความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต มีความสัมพันธ์กับความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

<u>ผลการทดสอบในแต่ละสมมติฐาน</u>

สมมติฐานที่ 1: การรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตมีประโยชน์ มีความสัมพันธ์กับทัศนคติต่อเทคโนโลยีของระบบการยืนยันตัวตนของผู้ใช้บัตรเครดิต

H_0= การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีประโยชน์ไม่มีความสัมพันธ์ต่อทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

H_1 = การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีประโยชน์มีความสัมพันธ์ต่อทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

ตารางที่ 4-16 ผลการทดสอบสมมติฐานที่ 1

		การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีประโยชน์	ทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต
การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีประโยชน์	Pearson Correlation	1	.214*
	Sig. (2-tailed)		.027
	N	107	107
ทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	Pearson Correlation	.214*	1
	Sig. (2-tailed)	.027	
	N	107	107

*. Correlation is significant at the 0.05 level (2-tailed).

ผล : ยอมรับ H_1 ความคิดที่ว่าการป้องกันการปลอมแปลงลายเซ็นมีความจำเป็นมีความสัมพันธ์ต่อทัศนคติต่อความสนใจในเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นที่ระดับนัยสำคัญ 0.027

สมมติฐานที่ 2: การรับรู้ว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตง่ายต่อการใช้งานมีความสัมพันธ์กับทัศนคติต่อเทคโนโลยีของระบบการยืนยันตัวตนของผู้ใช้บัตรเครดิต

H_0 = การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการใช้งานไม่มีความสัมพันธ์ต่อทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

H_1 = การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการใช้งานมีความสัมพันธ์ต่อทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

ตารางที่ 4-17 ผลการทดสอบสมมติฐานที่ 2

		การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการใช้งาน	ทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต
การรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการใช้งาน	Pearson Correlation	1	.230*
	Sig. (2-tailed)		.017
	N	107	107
ทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	Pearson Correlation	.230*	1
	Sig. (2-tailed)	.017	
	N	107	107

*. Correlation is significant at the 0.05 level (2-tailed).

ผล : ยอมรับ H_1 ที่ว่าระบบการรับรู้ว่าระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตง่ายต่อการใช้งานมีความสัมพันธ์ต่อทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตที่ระดับนัยสำคัญ 0.017

สมมติฐานที่ 3: ทัศนคติต่อเทคโนโลยีของระบบการยืนยันตัวตนของผู้ใช้บัตรเครดิต มีความสัมพันธ์กับความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

H_0= ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตไม่มีความสัมพันธ์ต่อความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

H_1 = ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความสัมพันธ์ต่อความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

ตารางที่ 4-18 ผลการทดสอบสมมติฐานที่ 3

		ทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต
ทัศนคติที่มีต่อเทคโนโลยีป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	Pearson Correlation	1	.279**
	Sig. (2-tailed)		.004
	N	107	107
ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต	Pearson Correlation	.279**	1
	Sig. (2-tailed)	.004	
	N	107	107

**. Correlation is significant at the 0.01 level (2-tailed).

ผล : ยอมรับ H_1 ทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความสัมพันธ์ต่อความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตที่ระดับนัยสำคัญ 0.004

จากสมมติฐานข้อที่ 3 วิเคราะห์ได้ว่าทัศนคติต่อเทคโนโลยีระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตในทางที่ดี หรือไม่ดี ก็ตาม ย่อมมีผลกระทบต่อความต้องการระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต เพราะถ้ามีทัศนคติที่ดี มีความเชื่อมั่นในเทคโนโลยีแล้ว จะทำให้เกิดความรู้สึกอยากที่จะใช้เทคโนโลยีนั้นมากขึ้น ซึ่งสอดคล้องกับแนวคิดของ Del I. Hawkins และคณะ [48] ที่ได้ศึกษาเรื่ององค์ประกอบของทัศนคติที่นำมาสู่แนวโน้มทางพฤติกรรม และความต้องการที่จะซื้อว่ามีความเกี่ยวข้องกัน

สมมติฐานที่ 4: ความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต มีความสัมพันธ์กับความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

H_0= ความน่าเชื่อถือของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตไม่มีความสัมพันธ์ต่อความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

H_1 = ความน่าเชื่อถือของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความสัมพันธ์ต่อความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

ตารางที่ 4-19 ผลการทดสอบสมมติฐานที่ 4

		ความน่าเชื่อถือของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต
ความน่าเชื่อถือของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต	Pearson Correlation	1	.373**
	Sig. (2-tailed)		.000
	N	107	107
ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต	Pearson Correlation	.373**	1
	Sig. (2-tailed)	.000	
	N	107	107

**. Correlation is significant at the 0.01 level (2-tailed).

ผล : ยอมรับ H_1 ความน่าเชื่อถือของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตมีความสัมพันธ์ต่อความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตที่ระดับนัยสำคัญ 0.000

4.1.5 การวิเคราะห์องค์ประกอบด้านคุณลักษณะของผู้บริโภคด้านต่างๆต่อความต้องการระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

องค์ประกอบด้านคุณลักษณะของผู้บริโภคด้านต่างๆ

- เพศ

ตารางที่ 4-20 ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามเพศ

เพศ	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อยที่สุด	ปานกลาง	มาก	มากที่สุด	
ชาย	1	1	18	12	32
ร้อยละ	3.125	3.125	56.25	37.5	100
หญิง	0	11	36	28	75
ร้อยละ	0	14.7	48.0	37.3	100
รวม	1	12	54	40	107
ร้อยละรวม	0.9	11.2	50.5	37.4	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ทั้งเพศชาย และเพศหญิง มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมาก คิดเป็นร้อยละ 50.5 และมากที่สุดร้อยละ 37.4 จากกลุ่มตัวอย่างทั้งหมด

- อายุ

ตารางที่ 4-21 ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามอายุ

อายุ (ปี)	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
20-29	0	1	22	26	49
ร้อยละ	0	2.0	44.9	53.1	100
30-39	1	6	14	13	34
ร้อยละ	2.9	17.6	41.3	38.2	100
40-49	0	1	8	8	17
ร้อยละ	0	5.8	47.1	47.1	100
50-59	0	1	2	4	7
ร้อยละ	0	14.3	28.6	57.1	100
รวม	1	9	46	51	107
ร้อยละรวม	0.9	8.4	43	47.7	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ช่วงอายุระหว่าง 20-29 ปี จะมีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมากที่สุด คือมีจำนวน 26 คน ช่วงอายุระหว่าง 30-39 ปี มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมาก มีจำนวน 14 คน ช่วงอายุระหว่าง 40-49 ปี มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมาก และมากที่สุดเท่ากัน คือ 8 คน และ ช่วงอายุระหว่าง 50-59 ปี มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมากที่สุด คือ 4 คน จากจำนวนรวมของแต่ละกลุ่มช่วงอายุ โดยความต้องการในการใช้นวัตกรรมการยืนยันตัวตนเฉลี่ยในทุกช่วงอายุ อยู่ในระดับมากที่สุด คิดเป็นร้อยละ 47.7

- สถานภาพ

ตารางที่ 4-22 ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามสถานภาพ

สถานภาพ	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อยที่สุด	ปานกลาง	มาก	มากที่สุด	
โสด	1	7	45	32	85
ร้อยละ	1.2	8.2	53	37.6	100
สมรส	0	4	7	8	19
ร้อยละ	0	21.1	36.8	42.1	100
หม้าย/หย่า	0	1	2	0	3
ร้อยละ	0	33.3	66.6	0	100
รวม	1	12	54	40	107
ร้อยละรวม	0.9	11.2	50.5	37.4	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ในสถานภาพโสดมีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมาก เป็นจำนวน 45 คน สถานภาพสมรสอยู่ในระดับมากที่สุด เป็นจำนวน 8 คน และสถานภาพหม้าย/หย่า อยู่ในระดับมาก มีจำนวน 2 คน โดยเฉลี่ยทุกสถานภาพมีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมาก คิดเป็นร้อยละ 50.5

- ระดับการศึกษา

ตารางที่ 4-23 ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามระดับการศึกษา

ระดับการศึกษา	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
ต่ำกว่าปริญญาตรี	0	1	4	5	10
ร้อยละ	0	10	40	50	100
ปริญญาตรี	1	5	36	38	80
ร้อยละ	1.25	6.25	45	47.5	100
ปริญญาโท	0	2	6	8	16
ร้อยละ	0	12.5	37.5	50	100
สูงกว่าปริญญาโท	0	1	0	0	1
ร้อยละ	0	100	0	0	100
รวม	1	9	46	51	107
ร้อยละรวม	0.9	8.4	43	47.7	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ที่ระดับการศึกษาต่ำกว่าปริญญาตรี ระดับปริญญาตรี และระดับสูงกว่าปริญญาตรี มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมากที่สุดเหมือนกัน คิดเป็นร้อยละ 47.7

- อาชีพ

ตารางที่ 4-24 ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามอาชีพ

อาชีพ	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
พนักงานบริษัทเอกชน	0	1	23	21	45
ร้อยละ	0	2.2	51.1	46.7	100
ข้าราชการ	1	7	14	22	44
ร้อยละ	2.3	15.9	31.8	50	100
พนักงานรัฐวิสาหกิจ	0	1	3	6	10
ร้อยละ	0	10	30	60	100
ธุรกิจส่วนตัว	0	0	6	2	8
ร้อยละ	0	0	75	25	100
รวม	1	9	46	51	107
ร้อยละรวม	0.9	8.4	43	47.7	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ในอาชีพ พนักงานบริษัทเอกชน และธุรกิจส่วนตัว มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตอยู่ในระดับมาก เป็นจำนวน 23 และ 6 คน ตามลำดับ ส่วนอาชีพข้าราชการ และพนักงานรัฐวิสาหกิจ มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตอยู่ในระดับมากที่สุด เป็นจำนวน 22 และ 6 คน ตามลำดับ โดยเฉลี่ยความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามอาชีพอยู่ในระดับมากที่สุด คิดเป็นร้อยละ 47.7

- รายได้ต่อเดือน

ตารางที่ 4-25 ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนจำแนกตามรายได้ต่อเดือน

รายได้ต่อเดือน (บาท)	ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อยที่สุด	ปานกลาง	มาก	มากที่สุด	
15,000 -25,000	1	8	48	32	89
ร้อยละ	1.1	9	53.9	36	100
25,001-35,000	0	2	3	2	7
ร้อยละ	0	28.5	43	28.5	100
35,001-45,000	0	0	2	4	6
ร้อยละ	0	0	33.3	66.7	100
45,001-55,000	0	0	0	1	1
ร้อยละ	0	0	0	100	100
55,001 ขึ้นไป	0	2	1	1	4
ร้อยละ	0	50	25	25	100
รวม	1	12	54	40	107
ร้อยละ	0.9	11.2	50.5	37.4	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ที่มีรายได้ต่อเดือนในช่วง 15,000 -25,000 บาท และช่วง 25,001-35,000 บาท จะมีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตอยู่ในระดับมาก เป็นจำนวน 48 และ 3 คน ตามลำดับ รายได้ต่อเดือนในช่วง 35,001-45,000 และ ช่วง 45,001-55,000 บาท มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตอยู่ในระดับมากที่สุด เป็นจำนวน 4 และ 1 คน ตามลำดับ และรายได้ต่อเดือนในช่วง 55,001 ขึ้นไป มีความต้องการในการใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตอยู่ในระดับปานกลางเป็นจำนวน 2 คน โดยเฉลี่ยของทุกกลุ่มรายได้ความต้องการในการใช้นวัตกรรมการยืนยันตัวตนอยู่ในระดับมาก คิดเป็นร้อยละ 50.5

4.1.6 การวิเคราะห์องค์ประกอบด้านคุณลักษณะของผู้บริโภคด้านต่างๆต่อความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

<u>องค์ประกอบด้านคุณลักษณะของผู้บริโภคด้านต่างๆ</u>

- เพศ

ตารางที่ 4-26 การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามเพศ

เพศ	การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
ชาย	1	4	16	11	32
ร้อยละ	3.1	12.5	50	34.4	100
หญิง	1	19	34	21	75
ร้อยละ	1.4	25.3	45.3	28	100
รวม	2	23	50	32	107
ร้อยละรวม	1.9	21.5	46.7	29.9	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ทั้งเพศชาย และหญิง มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมาก เป็นจำนวน 16 และ 34 คน ตามลำดับ คิดเป็นร้อยละ 46.7 ของกลุ่มตัวอย่างทั้งหมด

- อายุ

ตารางที่ 4-27 การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามอายุ

อายุ (ปี)	การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
20-29	0	7	25	17	49
ร้อยละ	0	14.3	51	34.7	100
30-39	3	11	10	10	34
ร้อยละ	8.8	32.4	29.4	29.4	100
40-49	0	3	10	4	17
ร้อยละ	0	17.6	58.9	23.5	100
50-59	0	2	3	2	7
ร้อยละ	0	28.6	42.9	28.6	100
รวม	3	23	48	33	107
ร้อยละรวม	2.8	21.5	44.9	30.8	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ในช่วงอายุ 20-29, 40-49 และ 50-59 มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมาก เป็นจำนวน 25, 10, 3 คน ตามลำดับ ส่วนช่วงอายุ 30-39 มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับปานกลาง เป็นจำนวน 11 คน โดยเฉลี่ยการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามอายุอยู่ในระดับมาก คิดเป็นร้อยละ 44.9

- สถานภาพ

ตารางที่ 4-28 การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามสถานภาพ

สถานภาพ	การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
โสด	3	18	40	24	85
ร้อยละ	3.5	21.1	47.1	28.3	100
สมรส	0	3	7	9	19
ร้อยละ	0	15.8	36.8	47.4	100
หม้าย/หย่า	0	2	1	0	3
ร้อยละ	0	66.7	33.3	0	100
รวม	3	23	48	33	107
ร้อยละรวม	2.8	21.5	44.9	30.8	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ในสถานภาพโสดมีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมาก เป็นจำนวน 40 คน ส่วนในสถานภาพสมรส มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมากที่สุด เป็นจำนวน 9 คน ในสถานภาพหม้าย/หย่า มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับปานกลางเป็นจำนวน 2 คน โดยเฉลี่ยการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามอายุอยู่ในระดับมาก คิดเป็นร้อยละ 44.9

- ระดับการศึกษา

ตารางที่ 4-29 การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามระดับการศึกษา

ระดับการศึกษา	การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
ต่ำกว่าปริญญาตรี	0	3	6	1	10
ร้อยละ	0	30	60	10	100
ปริญญาตรี	1	16	38	25	80
ร้อยละ	1.25	20	47.5	31.25	100
ปริญญาโท	1	3	6	6	16
ร้อยละ	6.25	18.75	37.5	37.5	100
สูงกว่าปริญญาโท	0	1	0	0	1
ร้อยละ	0	100	0	0	100
รวม	2	23	50	32	107
ร้อยละรวม	1.9	21.5	46.7	29.9	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ของการศึกษาระดับต่ำกว่าปริญญาตรี และปริญญาตรีมีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมาก เป็นจำนวน 6 และ 38 คน ตามลำดับ ส่วนการศึกษาระดับปริญญาโทมีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมากถึงมากที่สุดเป็นจำนวน 6 คน ส่วนระดับสูงกว่าปริญญาโท มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต ในระดับปานกลาง

- อาชีพ

ตารางที่ 4-30 การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามอาชีพ

อาชีพ	การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
พนักงานบริษัทเอกชน	0	6	22	17	45
ร้อยละ	0	13.3	18.9	37.8	100
ข้าราชการ	1	12	17	14	44
ร้อยละ	2.3	27.3	38.6	31.8	100
พนักงานรัฐวิสาหกิจ	0	2	7	1	10
ร้อยละ	0	20	70	10	100
ธุรกิจส่วนตัว	1	3	4	0	8
ร้อยละ	12.5	37.5	50	0	100
รวม	2	23	50	32	107
ร้อยละรวม	1.9	21.5	46.7	29.9	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ของทุกอาชีพ คือ พนักงานบริษัทเอกชน ข้าราชการ พนักงานรัฐวิสาหกิจ และธุรกิจส่วนตัว มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมาก เป็นจำนวน 22, 17, 7, 4 คน ตามลำดับ

- รายได้ต่อเดือน

ตารางที่ 4-31 การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนจำแนกตามรายได้ต่อเดือน

รายได้ต่อเดือน (บาท)	การรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต				รวม (คน)
	น้อย	ปานกลาง	มาก	มากที่สุด	
15,000 -25,000	2	19	42	26	89
ร้อยละ	2.3	21.3	47.2	29.2	100
25,001-35,000	0	2	5	0	7
ร้อยละ	0	28.6	71.4	0	100
35,001-45,000	0	2	2	2	6
ร้อยละ	0	33.3	33.3	33.3	100
45,001-55,000	0	0	0	1	1
ร้อยละ	0	0	0	100	100
55,001 ขึ้นไป	0	0	1	3	4
ร้อยละ	0	0	25	75	100
รวม	2	23	50	32	107
ร้อยละคน	1.9	21.5	46.7	29.9	100.0

ผล : สัดส่วนของกลุ่มตัวอย่างเป็นส่วนใหญ่ ที่รายได้ต่อเดือน 15,000 -25,000 และ 25,001-35,000 บาท มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมาก เป็นจำนวน 42 และ 5 คน ตามลำดับ รายได้ 35,001-45,000 บาท มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับปานกลาง มาก และมากที่สุด เป็นจำนวนเท่าๆกัน คือ 2 คน ส่วนรายได้ 45,001-55,000 และ 55,001 ขึ้นไป มีการรับรู้เกี่ยวกับความน่าเชื่อถือของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในระดับมากที่สุด

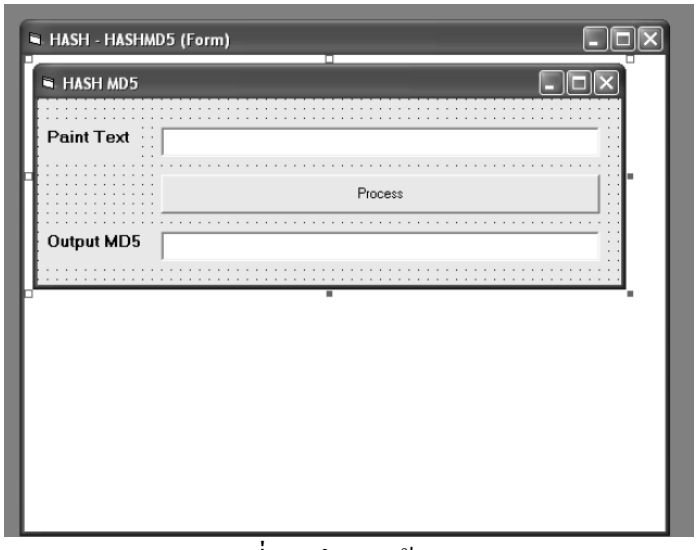
4.2 การพัฒนาระบบการป้องกันการปลอมแปลงของบัตรเครดิตรูปแบบใหม่

4.2.1 การสร้างโปรแกรม และปรับเปลี่ยนรูปแบบวิธีเพื่อให้เข้ากับการใช้งานจริง

ในการป้อนรหัสผ่านโปรแกรมเพื่อให้ได้ค่าแฮชออกมานั้น ค่าแฮชที่ได้มาจากโปรแกรมเข้ารหัส MD5 ที่ถูกพัฒนาด้วย Visual Basic ร่วมกับ Library ชื่อ bas MD5 และมีการสร้าง Form ดังภาพที่ 4-1 เพื่อรับค่าอินพุตหรือรหัสผ่านเพื่อนำไปเข้ารหัส MD5 จากนั้นก็ทำการเข้ารหัสจาก function MD5_string () หลังจากนั้นค่าที่ถูกเข้ารหัสแล้วก็จะมาแสดงใน txtOutput.text ที่จะได้เห็นเมื่อลูกค้าได้ทำการใช้งานโปรแกรม โดย code ทั้งหมดที่เขียนมานั้นจะทำงานเมื่อมีการกดปุ่ม HashMD5_Click code ทั้งหมดจึงถูกฝังไว้ใน event นี้

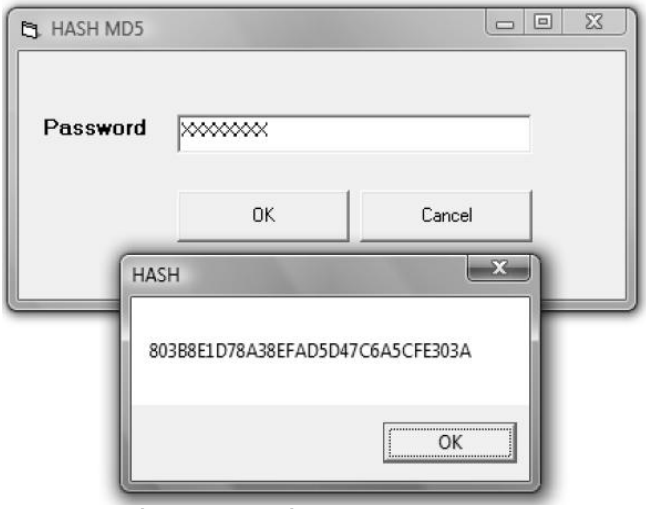
{Private Sub hashMD5_Click () txtOutput.Text = MD5_string (txtInput.Text) End Sub}

จากโปรแกรมที่สร้าง เมื่อกรอกรหัสผ่าน (Password) จะได้ค่าแฮชออกมา โดยกำหนดให้รหัสผ่านสามารถเป็นตัวอักษรภาษาอังกฤษ ตัวเลข (Alphanumeric Character) หรือสัญลักษณ์แอสกีอื่นๆ ก็ได้ โดยคำนึงถึงตัวพิมพ์ใหญ่และตัวพิมพ์เล็กด้วยจำนวนไม่เกิน 33 ตัว



ภาพที่ 4-1 โครงสร้าง form

ผลที่ได้จากการเข้าหัสแฮชด้วยวิธีการ MD5 จะได้ค่าแฮชที่เป็นลำดับของเลขฐานสิบหกจำนวน 32 ตัว ดังภาพที่ 4-2



ภาพที่ 4-2 ค่าแฮชที่ได้จากฟังก์ชันแฮช MD5

ซึ่งลำดับของค่าแฮชนี้ยาวเกินไปสำหรับการใช้งานจริงเพราะยากต่อการตรวจสอบ ดังนั้นเพื่อให้มีความสะดวกในการตรวจสอบว่าค่าแฮชชุดนี้ตรงกับค่าแฮชที่อ่านได้จากคิวอาร์โค้ดหรือไม่ และเพื่อเพิ่มความปลอดภัยจากการแปลงค่า ค่าดังกล่าวจึงถูกนำไปลดให้เหลือเพียงแค่ 8 ตัว ด้วยฟังก์ชัน Exclusive-or

ฟังก์ชัน Exclusive-or (XOR) เป็นการกระทำทางตรรกศาสตร์ โดยมีหลักการ คือ

1. มีข้อมูลนำเข้า (Input) ตั้งแต่ 2 ตัวแปรขึ้นไป เช่น A, B
2. จะให้ข้อมูลส่งออก (Output) เป็น 0 เมื่อข้อมูลนำเข้ามีค่าเหมือนกัน
3. จะให้ข้อมูลส่งออก เป็น 1 เมื่อข้อมูลนำเข้ามีค่าต่างกัน

ยกตัวอย่างดังตารางที่ 4-16

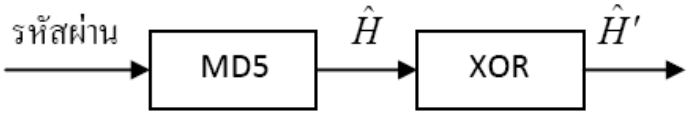
ตารางที่ 4-32 ตัวอย่างของค่า XOR

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

กระบวนการทั้งหมดสำหรับการสร้างค่าแฮชสามารถสรุปได้ดังภาพที่ 4-3 โดยมีวิธีการเข้าสมการดังนี้

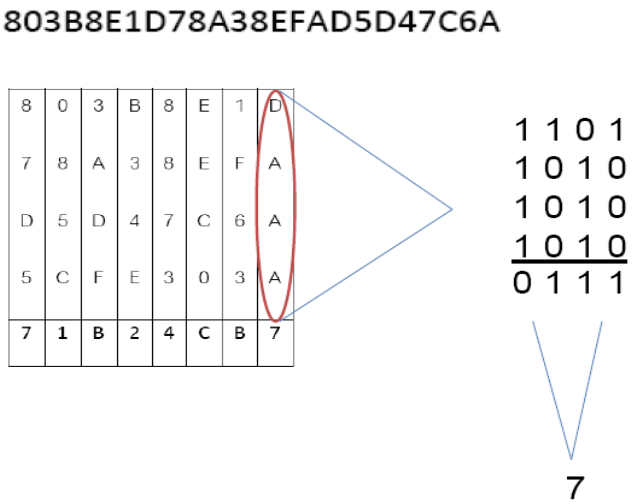
กำหนดให้ $\hat{H} = [h_{31}, h_{30}, h_{29}, ..., h_2, h_1, h_0]$ เป็นค่าที่ได้จากการเข้ารหัส MD5 โดย h_i แทนค่าแฮชลำดับที่ i และ $\hat{H}' = [h'_7, h'_6, h'_5, h'_4, h'_3, h'_2, h'_1, h'_0]$ เป็นค่าที่ได้จากการเข้ารหัส MD5 ไปลดรูปด้วยฟังก์ชัน Exclusive-or ทำให้เหลือเพียง 8 ตัวดังสมการ

$$h'_i = h_{i+24} \oplus h_{i+16} \oplus h_{i+8} \oplus h_i \qquad (1)$$



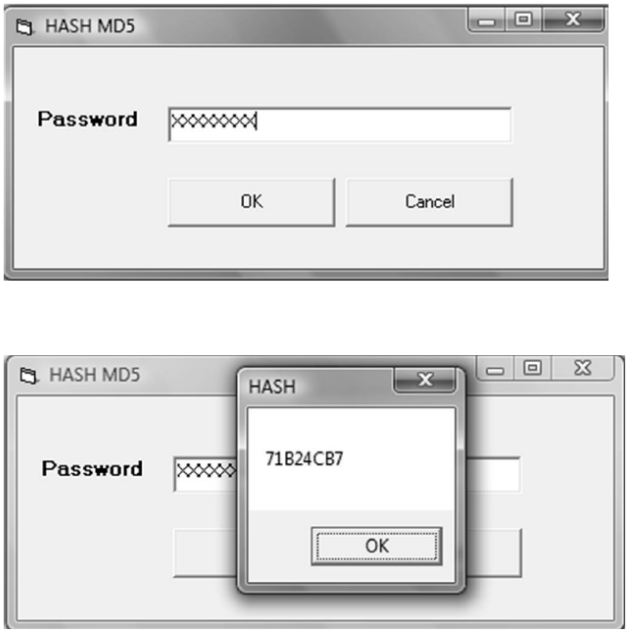
ภาพที่ 4-3 การสร้างค่าแฮชด้วยการเข้ารหัส MD5 และฟังก์ชัน Exclusive-or

ตัวอย่างเช่น ค่าที่ได้จากการเข้ารหัส MD5 คือ 803B8E1D78A38EFAD5D47C6A5CFE303A เมื่อใช้สมการที่ (1) จะได้ 71B24CB7 และจะแสดงผลดังภาพที่ 4-4



ภาพที่ 4-4 การลดรูปด้วยฟังก์ชัน Exclusive-or

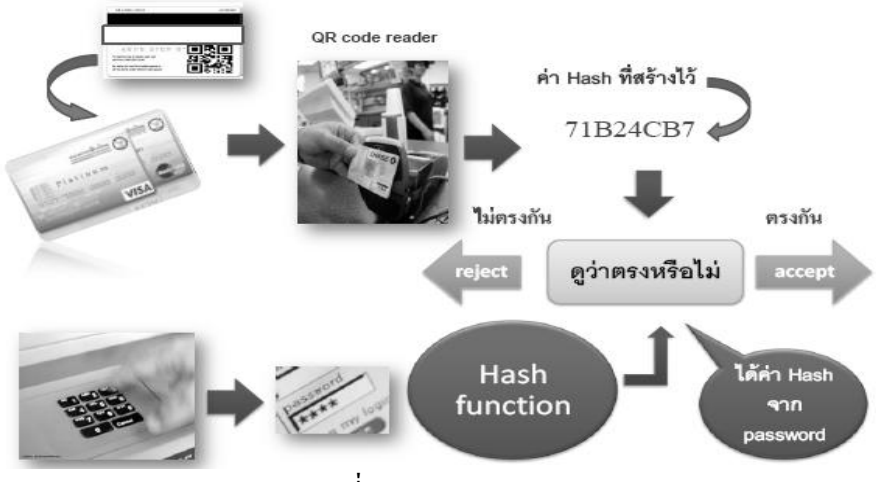
จากการปรับเอาท์พุตของค่าแฮชให้มี 8 ตัวนั้นทำให้การใช้งานจริงสะดวกมากขึ้น เพราะสามารถเปรียบเทียบค่าแฮชที่ปรากฏจากการสแกนคิวอาร์โค้ดกับการรหัสผ่านได้ง่ายขึ้นและมีความถูกต้องดังภาพที่ 4-5



ภาพที่ 4-5 การแสดงผลค่า Hash

4.2.2 ทดลองสร้างนวัตกรรมต้นแบบ

นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ด (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) มีหลักการเบื้องต้นคือ ส่วนที่หนึ่งเป็นการใช้ตัวอ่านรหัสคิวอาร์เพื่ออ่านภาพที่ถูกกำหนดไว้ด้านหลังของบัตร ส่วนที่สองประกอบด้วยการเข้ารหัสแบบทางเดียวเพื่อยืนยันรหัสผ่านที่ผู้ใช้กำหนดไว้



ภาพที่ 4-6 ภาพรวมระบบ

จากภาพที่ 4-6 สัญลักษณ์จะแสดงไว้ด้านหลังบัตรแทนแถบแม่เหล็ก และลายเซ็นของผู้ถือบัตรเครดิต ซึ่งเก็บรหัสแฮชจากข้อมูลเบื้องต้นของผู้ถือบัตร โดยข้อมูลดังกล่าวอาจเป็นรหัสผ่าน (Password) โดยที่ผู้ใช้ทราบรหัสผ่านของตนเองแต่จะไม่ทราบรหัสแฮชและฟังก์ชันแฮชที่ทำให้ได้มาซึ่งรหัสดังกล่าว เพราะธนาคารเท่านั้นที่จะเป็นผู้ใช้ฟังก์ชันแฮชและสร้างรหัสแฮชแล้วบันทึกไว้บนคิวอาร์โค้ด

ภาพที่ 4-7 การเปลี่ยนคิวอาร์โค้ดเป็นค่าแฮชด้วยการสแกน

ในการใช้งานแต่ละครั้งซอฟต์แวร์การเข้ารหัสทางเดียวจะเปลี่ยนรหัสผ่านของผู้ถือบัตรเป็นรหัสแฮชเพื่อเปรียบเทียบกับรหัสแฮชที่บันทึกไว้ด้วยคิวอาร์โค้ดที่พิมพ์ไว้บนบัตร ตามภาพที่ 4-7 ดังนั้นถ้าแปลงรหัสแล้วตรงกันก็จะสามารถยืนยันความเป็นเจ้าของบัตรได้ และแม้ว่าบัตรหายหรือถูกโจรกรรม ตราบใดที่ผู้ไม่หวังดีไม่ทราบรหัสผ่านก็ไม่สามารถสร้างรหัสแฮชที่ถูกต้องได้

4.3 การทดสอบประสิทธิภาพของระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิต

4.3.1 การวัดความปลอดภัยของระบบ

(1) ใช้วิธีการคำนวณจากการนับ (Counting)

โดยปกติแล้วการโจมตีระบบรักษาความปลอดภัยที่ใช้ค่าแฮชจากการผ่านการเข้ารหัสทางเดียวนั้นจะสามารถทำได้ภายใต้สมมติฐานที่ผู้โจมตีสามารถหาค่าแฮชได้โดยอาจได้มาจากการอ่านรหัสคิวอาร์โดยตรงหรือการดักข้อมูลในกรณีใดกรณีหนึ่งซึ่งสามารถแบ่งได้เป็นสองวิธี ได้แก่ 1) การหาค่ารหัสผ่านจากค่าแฮชเดิมซึ่งจะกล่าวถึงในหัวข้อถัดไป และ 2) การสุ่มรหัสผ่านที่ให้ค่าแฮชเดียวกันหรือทำให้เกิดการชนกัน (Collision)

เมื่อพิจารณาถึงการสุ่มรหัสผ่านที่ให้ค่าแฮชเดียวกันจะพบว่าโดยเฉลี่ยแล้วค่าแฮชเดียวกันสามารถเกิดจากรหัสผ่านจำนวนหนึ่งซึ่งคำนวณได้จากอัตราส่วนระหว่าง รหัสผ่านทั้งหมดที่เป็นไปได้และค่าแฮชทั้งหมดที่เป็นไปได้ดังนี้

ค่ารหัสผ่านทั้งหมดที่เป็นไปได้หรือข้อมูลนำเข้า (Input) เท่ากับ $X^Y = 94^{33} =$ 129,783,406,392,333,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000

โดยให้ X = จำนวนอักขระที่เป็นไปได้ (ในการป้อนรหัส) ทั้งหมด 94 รูปแบบ นับรวมอักขระพิมพ์ใหญ่และพิมพ์เล็กในภาษาอังกฤษ ตัวเลข และอักขระเครื่องหมายอื่น ๆ

Y = จำนวนหลักที่สามารถป้อนได้ (ในช่องกรอกรหัส) ทั้งหมด 33 หลัก

และค่าแฮชทั้งหมดที่เป็นไปได้หรือข้อมูลส่งออก (Output) เท่ากับ $X^Y = 16^8 = 4,294,967,296$

โดยให้ X = จำนวนรูปแบบตัวอักษรที่ออกมาในรูปแบบเลขฐาน 16 ซึ่งมี 16 รูปแบบ

Y = จำนวนหลักทั้งหมด 8 หลัก

ดังนั้นอัตราส่วนระหว่าง รหัสผ่านทั้งหมดที่เป็นไปได้และค่าแฮชทั้งหมดที่เป็นไปได้จะเท่ากับ

$$\frac{4,294,967,296}{129,783,406,392,333,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000}$$

หรือเท่ากับ

0.00000000000000000000000000000000000000000000000000330933469492732

ซึ่งเป็นค่าที่ต่ำมาก อย่างไรก็ตามเมื่อพิจารณาส่วนกลับของค่าดังกล่าวจะหมายถึงจำนวนของรหัสผ่านทั้งหมดโดยเฉลี่ยที่ให้ค่าแฮชเดียวกันซึ่งมีค่าสูงถึง

30,217,554,045,918,700,000,000,000,000,000,000,000,000,000,000,000,000.00

นั่นก็หมายความว่ามีรหัสผ่านมากมายที่ให้ค่าแฮชซ้ำกัน เมื่อพิจารณาต่อไปถึงความน่าจะเป็นที่สุ่มค่าแฮชแล้วได้ค่าที่ต้องการนั้น เนื่องจากรูปแบบของค่าแฮชที่เป็นไปได้มีถึง4,294,967,296 รูปแบบ ความน่าจะเป็นที่จะสุ่มเจอในหนึ่งครั้งนั้นมีเพียง 0.00000000023283064365387 0 หรือในกรณีที่เลวร้ายที่สุด (worst case) อาจต้องสุ่มถึง

129,783,406,362,116,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000, 000,000 ครั้ง

ถึงจะพบรหัสผ่านตรงกัน ถ้าคอมพิวเตอร์เครื่องหนึ่งสามารถคำนวณค่าแฮชค่าหนึ่งที่ได้จากการสุ่มรหัสผ่านในระยะเวลา 1 นาโนวินาที ก็ต้องใช้เวลาถึง

129,783,406,362,116,000,000,000,000,000,000,000,000,000,000,000,000,000,000 วินาที

หรือ

4,115,404,818,687,070,000,000,000,000,000,000,000,000,000,000,000 ปี ซึ่งเป็นระยะเวลาที่มากเกินไปในทางปฏิบัติ อย่างไรก็ตามระยะเวลาดังกล่าวยังคงเป็นระยะเวลาในกรณีที่เลวร้ายที่สุด แต่ถ้าคำนวณต่อไปถึงระยะเวลาในกรณีเฉลี่ยจะเท่ากับ

2,057,702,409,343,535,000,000,000,000,000,000,000,000,000,000,000 ปีซึ่งยังคงเป็นระยะเวลาที่มากเกินไปเช่นเดียวกัน

(2) อ้างอิงจากผลงานวิจัยที่เกี่ยวข้อง

ความปลอดภัยในการใช้บัตรเครดิตที่เพิ่มมากขึ้นจากนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตในกรณีที่มีผู้ไม่หวังดีลักลอบดักข้อมูล แต่ข้อมูลที่ได้ไปที่อยู่ในรูปของค่าแฮช ซึ่งค่าแฮชจะไม่สามารถเรียกกลับคืนเป็นรหัสผ่านนั้นได้ ผู้ไม่หวังดีก็ไม่สามารถใช้บัตรเครดิตนั้นได้ ซึ่งตรงกับที่ Essam Abdel-azeem และคณะ [42] ได้กล่าวไว้ว่าฟังก์ชันแฮชในวิทยาการเข้ารหัสลับถูกนำมาใช้ประโยชน์ในเรื่องของการลงลายเซ็นดิจิทัล และการพิจารณาการพิสูจน์ตัวตนได้ โดยที่ฟังก์ชันแฮชเป็นฟังก์ชันแบบทางเดียวซึ่งไม่สามารถหาฟังก์ชันผกผันได้ ดังนั้นรหัสที่ได้จากฟังก์ชันแฮชจะไม่สามารถนำมาใช้ในการเรียกคืนรหัสดั้งเดิมกลับมาได้ อีกทั้งฟังก์ชันแฮชยังมีคุณสมบัติปลอดการชนซึ่งให้ความปลอดภัยสูงเพราะความเป็นไปได้ที่รหัสผ่านสองชุดจะให้ค่าแฮชเหมือนกันมีน้อยมากจนเกือบเป็นไปไม่ได้ ดังนั้นนวัตกรรมการยืนยันตัวตนของผู้ใช้บัตรเครดิตจึงทำให้มีความปลอดภัยในการใช้บัตรเครดิตสูงขึ้น

4.3.2 การทดลองใช้งานอุปกรณ์จำลอง

1. ทำการทดสอบบนบัตรเสมือนที่มีโครงสร้างทางกายภาพใกล้เคียงกับบัตรเครดิตจริง

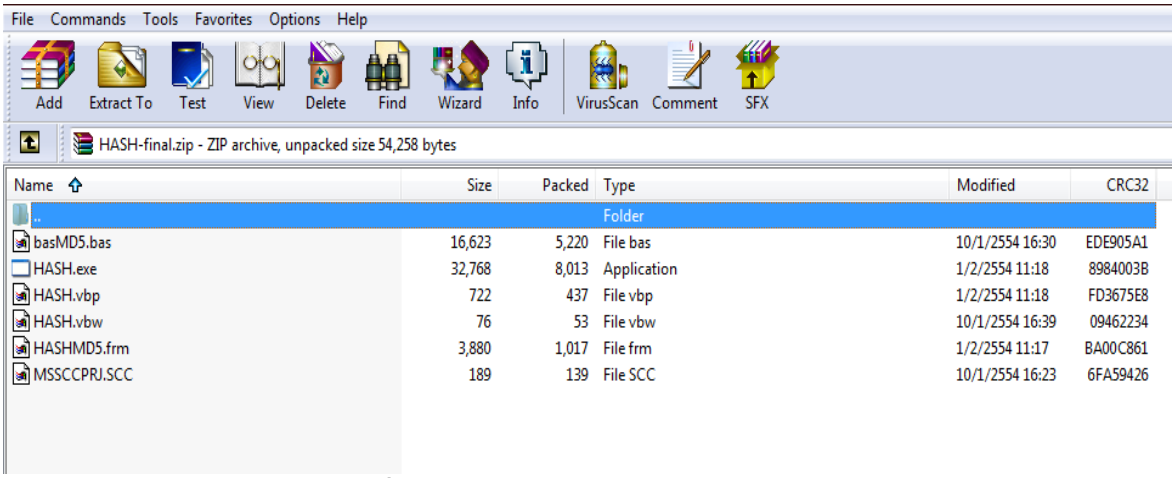
2.อุปกรณ์การอ่านรหัสตอบสนองอย่างรวดเร็ว (QR-Code) ใช้โปรแกรมสำเร็จรูปแบบเดียวกับโปรแกรมของโทรศัพท์เคลื่อนที่

3. ขั้นตอนวิธีการเข้ารหัสทางเดียว พัฒนาโปรแกรมบนเครื่องคอมพิวเตอร์ และใช้ฟังก์ชันในการเข้ารหัส โดยตั้งอยู่บนพื้นฐานของฟังก์ชันแฮช ซึ่งใช้เพียงรูปแบบเดียวเท่านั้น

4. การป้อนรหัส (Password) เพื่อแปลงเป็นค่า Hash นั้น ใช้คีย์บอร์ดขนาดเล็ก เชื่อมต่อด้วยสัญญาณบลูทูธ เพื่อความสะดวกในการป้อนรหัส และปกปิดบุคคลภายนอก

- จัดเตรียมอุปกรณ์

1. ติดตั้งซอฟต์แวร์การเข้ารหัสลงบนเครื่องคอมพิวเตอร์เพื่อใช้ในการเปลี่ยนรหัสผ่าน (Password) เป็นรหัสแฮชดังภาพที่ 4-8



ภาพที่ 4-8 ลักษณะซอฟต์แวร์การเข้ารหัส

2. ต่อเครื่องคีย์บอร์ดขนาดเล็กด้วยสัญญาณบลูทูธ (Bluetooth) เพื่อใช้ในการป้อนรหัสผ่านแทนการใช้แป้นพิมพ์ปกติ

ภาพที่ 4-9 คีย์บอร์ดสัญญาณบลูทูธ

3. บัตรเครดิตจำลองที่มีสัญลักษณ์คิวอาร์โค้ด

ภาพที่ 4-10 บัตรเครดิตจำลอง

4. อุปกรณ์ในการอ่านค่าคิวอาร์โค้ด เพื่อความสะดวกในที่นี้ใช้โทรศัพท์มือถือที่ติดตั้งโปรแกรมอ่านค่า

ภาพที่ 4-11 อุปกรณ์การอ่านค่าคิวอาร์โค้ด

- ลักษณะการใช้งาน

ภาพที่ 4-12 กระบวนการใช้งาน

เมื่อใช้มีการใช้บัตรเครดิตที่มีสัญลักษณ์คิวอาร์โค้ดแสดงไว้ทดแทนแถบแม่เหล็ก หรือลายเซ็นของผู้ถือบัตร ผู้ขายจะสแกนสัญลักษณ์คิวอาร์โค้ดด้วยเครื่องอ่าน และแสดงค่าแฮชที่เก็บไว้ออกมาผ่านเครื่องอ่านนั้น ทางด้านผู้ใช้บัตรจะป้อนรหัสส่วนตัวที่สร้างไว้ด้วยเครื่องคีย์บอร์ดขนาดเล็ก และเมื่อรหัสเข้าสู่ระบบซอฟต์แวร์การเข้ารหัสแล้วจะแปลงค่ารหัสนั้นเป็นค่าแฮช เพื่อเปรียบค่าแฮชที่ได้จากสัญลักษณ์คิวอาร์โค้ด ถ้าค่าแฮชทั้ง 2 ชุดตรงกัน ก็สามารถยืนยันตัวตนของผู้ใช้บัตรได้

4.4 การศึกษาการยอมรับต่อระบบนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว

การเก็บข้อมูลแบ่งเป็น 2 ลักษณะคือ

1. เลือกกลุ่มตัวอย่างแบบเจาะจง ใช้วิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) และแบบสอบถามเป็นเครื่องมือในการเก็บข้อมูล โดยการสัมภาษณ์เชิงลึกจากตัวแทนกรรมการบริหารฝ่ายบัตรเครดิตของธนาคาร

ชื่อ : นายอาจหาญ เพ็ชรดี
สถานที่ทำงาน : ธนาคารกสิกรไทย
ตำแหน่งงาน : ผู้อำนวยการฝ่ายบริหาร
ผลิตภัณฑ์และการตลาดบัตรเครดิต

2. เลือกกลุ่มตัวอย่างแบบไม่อาศัยความน่าจะเป็น (Non-Probability Sampling) วิธีการคัดเลือกตัวอย่างแบบสะดวก (Convenience Sampling) โดยการสัมภาษณ์ และทดลองใช้งานนวัตกรรมจำลองจากร้านค้าที่มีการใช้จ่ายผ่านบัตรเครดิต

ชื่อ : นางสาวขจีวรรณ ศรีรักษ์
อาชีพ : ค้าขายเครื่องสำอางค์สมุนไพร
สถานที่ทำงาน : ห้างสรรพสินค้าเดอะ
มอลล์ สาขาท่าพระ ชั้น จี

การดูวิดีโอสาธิตการใช้งาน ดังภาพที่ 4-13 จากนั้นให้ทำแบบสอบถามประเมินความพึงพอใจจำนวน 50 คน

ภาพที่ 4-13 วิดีโอสาธิตการใช้งาน

ลักษณะคำถามจะเกี่ยวกับตัวแปรที่ใช้ในการศึกษาจากบทที่ 3 ทั้งหมด 5 ข้อ คือ ความมีประโยชน์ ความง่ายต่อการใช้งาน ความน่าเชื่อถือ ความน่าสนใจ และ ความต้องการที่จะใช้บริการนวัตกรรม

4.4.1 ผลการศึกษาด้านการยอมรับในนวัตกรรม

1. ผลจากการสัมภาษณ์

- ตัวแทนกรรมการบริหารฝ่ายบัตรเครดิตของธนาคาร

สอบถามด้านความเป็นไปได้ในการนำนวัตกรรมนี้ไปสู่เชิงพาณิชย์

“เทคโนโลยีเรื่องนี้มีความเป็นไปได้ในการนำไปใช้ และถือว่าเป็นเรื่องใหม่ที่น่าสนใจ เพิ่มความปลอดภัยในการใช้บัตรเครดิตให้กับลูกค้ามากขึ้น แต่ในรายละเอียดมีข้อจำกัดด้านการลงทุน เพราะอาจจะต้องเปลี่ยนเครื่องอ่านบัตรของทั้งระบบ (ร้านค้าต่างๆ) และการลงทุนในธุรกิจนี้ ธนาคารใดธนาคารหนึ่งไม่สามารถใช้โดยลำพังได้ จะต้องเป็นการร่วมมือกันของทุกธนาคารที่มีการทำธุรกรรมทางการเงินกันทั้งประเทศ ดังนั้นจะต้องมีการประชุม และออกข้อตกลงร่วมกันในรายละเอียดอีกที”

- ร้านค้าที่มีการใช้จ่ายผ่านบัตรเครดิต

สอบถามด้านความสะดวกในการใช้งาน

"การใช้งานง่าย ไม่ซับซ้อน ไม่ได้เพิ่มภาระในการให้บริการ"

จากการสัมภาษณ์ ส่วนของตัวแทนผู้ลงทุนในธุรกิจบัตรเครดิต มีความสนใจในตัวนวัตกรรม แต่ธนาคารเพียงแห่งเดียวไม่สามารถตัดสินใจการดำเนินการใดได้ ต้องอาศัยการร่วมมือกันของธนาคารทุกแห่ง ที่มีการทำธุรกรรมผ่านบัตรเครดิต ซึ่งจำเป็นต้องมีการคำนวณด้านความคุ้มค่าในการลงทุน และสอบถามความร่วมมือกับธนาคารอื่นๆเพิ่มเติม ในส่วนของร้านค้าการใช้งานนวัตกรรมไม่ได้ทำให้เกิดความยุ่งยาก หรือเพิ่มภาระ และไม่มีปัญหาถ้าจะมีการเปลี่ยนแปลงรูปแบบการยืนยันตัวตนในการใช้บัตรเครดิต

2.ผลจากแบบสอบถาม

(1) ประโยชน์ของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว

ตารางที่ 4-33 ความคิดเห็นด้านประโยชน์ของนวัตกรรม

ประโยชน์ของนวัตกรรม						
ระดับ	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	รวม(คน)
จำนวน(คน)	37	11	2	-	-	50
ร้อยละ	74	22	4	-	-	100.0

ผล : กลุ่มตัวอย่างได้แสดงความคิดเห็นว่านวัตกรรมนี้มีประโยชน์มากที่สุด จำนวน 37 คน คิดเป็นร้อยละ 74 รองลงมาคิดว่ามีประโยชน์มาก จำนวน 11 คน คิดเป็นร้อยละ 22

(2) ความง่ายในการใช้งานนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว

ตารางที่ 4-34 ความคิดเห็นด้านความง่ายในการใช้งานของนวัตกรรม

ความง่ายในการใช้งานของนวัตกรรม						
ระดับ	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	รวม(คน)
จำนวน(คน)	27	16	6	-	1	50
ร้อยละ	54	32	12	-	2	100.0

ผล : กลุ่มตัวอย่างได้แสดงความคิดเห็นว่านวัตกรรมนี้ง่ายต่อการใช้งานมากที่สุด จำนวน 27 คน คิดเป็นร้อยละ 54 รองลงมาคิดว่าง่ายต่อการใช้งานมาก จำนวน 16 คน คิดเป็นร้อยละ 32

(3) ความน่าเชื่อถือของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว

ตารางที่ 4-35 ความคิดเห็นด้านความน่าเชื่อถือของนวัตกรรม

ความน่าเชื่อถือของนวัตกรรม						
ระดับ	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	รวม(คน)
จำนวน(คน)	12	22	15	1	-	50
ร้อยละ	24	44	30	2	-	100.0

ผล : กลุ่มตัวอย่างได้แสดงความคิดเห็นว่านวัตกรรมนี้มีความน่าเชื่อถือมาก จำนวน 22 คน คิดเป็นร้อยละ 44 รองลงมาคิดว่ามีความน่าเชื่อถือปานกลาง จำนวน 15 คน คิดเป็นร้อยละ 30

(4) ความน่าสนใจของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว

ตารางที่ 4-36 ความคิดเห็นด้านความน่าสนใจของนวัตกรรม

ความน่าสนใจของนวัตกรรม						
ระดับ	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	รวม(คน)
จำนวน(คน)	21	22	7	-	-	50
ร้อยละ	42	44	14	-	-	100.0

ผล : กลุ่มตัวอย่างได้แสดงความคิดเห็นว่านวัตกรรมนี้มีความน่าสนใจมาก จำนวน 22 คน คิดเป็นร้อยละ 44 รองลงมาคิดว่ามีความน่าสนใจมากที่สุด จำนวน 21 คน คิดเป็นร้อยละ 42

(5) ความตั้งใจที่จะใช้บริการนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ดและการเข้ารหัสแบบทางเดียว หรือแนะนำให้บุคคลอื่น

ตารางที่ 4-37 ความคิดเห็นด้านความตั้งใจที่จะใช้บริการนวัตกรรม

ความตั้งใจที่จะใช้บริการนวัตกรรม หรือแนะนำให้บุคคลอื่น						
ระดับ	มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด	รวม(คน)
จำนวน(คน)	23	22	5	-	-	50
ร้อยละ	46	44	10	-	-	100.0

ผล : กลุ่มตัวอย่างได้แสดงความคิดเห็นว่ามากที่สุดที่จะใช้บริการนวัตกรรมนี้ หรือแนะนำให้บุคคลอื่น จำนวน 23 คน คิดเป็นร้อยละ 46 รองลงมามีความตั้งใจมากที่จะใช้บริการนวัตกรรมนี้ หรือแนะนำให้บุคคลอื่น จำนวน 22 คน คิดเป็นร้อยละ 44

สรุปผลการศึกษา : หลังการใช้งานจริง หรือการดูวิดีโอสาธิตการใช้งานแล้วทำแบบสอบถาม จากข้อคำถามทั้ง 5 ข้อ กลุ่มตัวอย่างมีความพึงพอใจนวัตกรรมเฉลี่ยอยู่ในระดับมากที่สุด จากการถามคำถามในเรื่องความมีประโยชน์ ความง่ายต่อการใช้งาน และมีความตั้งใจที่จะใช้บริการนวัตกรรม เฉลี่ยในระดับมาก จากการถามคำถาม ในเรื่องความน่าเชื่อถือ และความน่าสนใจ ซึ่งในด้านความน่าเชื่อถือนั้น เป็นที่น่าสังเกตว่า ระดับรองลงมาของข้อนี้อยู่ที่ระดับปานกลาง ต่างจากระดับรองลงมาของ ความน่าสนใจ ที่อยู่ในระดับมากที่สุดซึ่งแสดงให้เห็นว่านวัตกรรมนี้ยังไม่สามารถสร้างความน่าเชื่อถือให้กับกลุ่มตัวอย่างได้อย่างเต็มที่ แต่นวัตกรรมก็ยังมีความน่าสนใจที่

จะชักจูงใจให้ทดลองใช้ ดังนั้นจะต้องเพิ่มในเรื่องของความน่าเชื่อถือมากขึ้นเป็นพิเศษ และเพิ่มรูปแบบของผลิตภัณฑ์ให้น่าสนใจขึ้นด้วย

บทที่ 5
การศึกษาความเป็นไปได้ของผลิตภัณฑ์ในเชิงธุรกิจ

5.1 จากการศึกษาด้านความต้องการ และการยอมรับ

จากการวิเคราะห์ข้อมูลในการวิจัยเรื่องนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) ใน 2 เรื่อง คือ 1. ศึกษาความคิดเห็นของผู้บริโภคในความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต โดยแต่ละส่วนจะวิเคราะห์จากข้อมูลพื้นฐานของกลุ่มตัวอย่างและการทดสอบสมมติฐานที่ได้ตั้งไว้ และ 2. ศึกษาความพึงพอใจของผู้บริโภคต่อนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) ในลักษณะการใช้งานจริง หรือการดูวิดีโอสาธิตการใช้งาน จากนั้นให้ทำแบบสอบถามประเมินความพึงพอใจ โดยใช้แบบสอบถามเป็นเครื่องมือในการวิเคราะห์ ซึ่งลักษณะคำถามเกี่ยวกับตัวแปรที่ใช้ในการศึกษา ทั้งหมด 5 ข้อ คือ ความมีประโยชน์ ความง่ายต่อการใช้งาน ความน่าเชื่อถือ ความน่าสนใจ และ ความตั้งใจที่จะใช้บริการนวัตกรรม ซึ่งพบว่านวัตกรรมมีแนวโน้มที่น่าสนใจ คือ ผู้บริโภคมีความต้องการสูง และมีทัศนคติที่ดีต่อนวัตกรรม ดังนั้นความเป็นไปได้ของผลิตภัณฑ์นี้ในเชิงธุรกิจเป็นไปในทางที่ดี

5.2 จากการวิเคราะห์ด้วยเครื่องมือต่างๆ

จากแนวโน้มความต้องการในการใช้บัตรเครดิตที่เพิ่มมากขึ้น อีกทั้งจากการสำรวจความต้องการพบว่า มีความกังวลในด้านความปลอดภัยสูง และต้องการระบบรักษาความปลอดภัยที่มากขึ้น ดังนั้นจึงมีโอกาสที่จะเสนอนวัตกรรมใหม่ๆในการตอบสนองความต้องการดังกล่าวได้ แต่เมื่อจะนำนวัตกรรมเข้าสู่เชิงพาณิชย์ อันดับแรกควรต้องมีการวิเคราะห์ และวางแผนให้เหมาะสม เพราะคู่แข่งที่มาจากสถาบันต่างๆ ที่ให้บริการด้านบัตรเครดิต ต่างก็พยายามคิดหาวิธีการยืนยันตัวตนของผู้ใช้บริการขึ้นหลากหลายวิธี เพื่อสร้างความเชื่อมั่นให้กับผู้ใช้บริการ และขยายฐานลูกค้าให้มากขึ้นจากความต้องการ โอกาส และเทคโนโลยีที่ก้าวหน้าอย่างรวดเร็วนั่นเอง ซึ่งสามารถวิเคราะห์แนวโน้มของตลาดได้ผ่านเครื่องมือดังต่อไปนี้

5.2.1 SWOT

เป็นการวิเคราะห์ข้อมูลที่พิจารณาความเป็นไปได้ทางการตลาด 4 ด้าน [49] คือ Strengths, Weaknesses, Opportunities, Threats ซึ่งแบ่งเป็นส่วนที่มาจากสภาวะภายนอก (External Environment) และสภาวะภายใน (Internal Environment)

ตารางที่ 5-1 การวิเคราะห์ด้วย SWOT

- สภาวะภายนอก (External Environment)

Opportunities (โอกาส)	- สามารถนำไปประยุกต์ใช้กับงานด้านอื่นๆ ที่ให้ต้องการและให้ความสำคัญเรื่องการยืนยันตัวตนได้ไม่จำกัด - สามารถขยายตลาดการใช้ได้อย่างแพร่หลายในทุกภาคส่วนธุรกิจ
Threats (อุปสรรค)	- อาจจะต้องใช้เวลาในการทำให้เกิดการยอมรับเนื่องจากเป็นวิธีการรูปแบบใหม่ - อาจจะเกิดการเลียนแบบจากคู่แข่งได้ ถ้าการให้บริการได้ผลดี และเป็นที่ยอมรับ

- สภาวะภายใน (Internal Environment)

Strengths (จุดแข็ง)	- เพิ่มความแปลกใหม่ในการใช้บริการผ่านบัตรเครดิตที่ปลอดภัย - ใช้งานได้ง่าย ไม่ซับซ้อน ยุ่งยาก - สามารถเพิ่มยอดการใช้บัตรเครดิตได้มากยิ่งขึ้น ถ้าผู้บริโภคเกิดความมั่นใจในความปลอดภัย
Weaknesses (จุดอ่อน)	- ความแปลกใหม่ในรูปแบบการใช้งาน และลักษณะการให้บริการทำให้ผู้ลงทุนเกิดความไม่มั่นใจ - มีทางเลือกอื่นๆในการให้บริการหลายทาง ทำให้ต้องอาศัยการทำการตลาดที่ดี เพื่อสร้างความเชื่อมั่น และการยอมรับในตัวนวัตกรรม

5.2.2 Market Trend แนวโน้มของตลาด

ผู้ลงทุนของนวัตกรรมนี้ คือ สถาบันผู้ให้บริการบัตรเครดิต เช่น ธนาคาร และบริษัทผู้ประกอบธุรกิจบัตรเครดิต จากข้อมูลของธนาคารแห่งประเทศไทย [2] พบว่า ปัจจุบันมีสถาบันผู้ให้บริการบัตรเครดิตในประเทศไทยจำนวน 24 แห่ง แบ่งเป็น ธนาคารพาณิชย์ไทย 10 แห่ง สาขาของธนาคารต่างประเทศ 2 แห่ง และบริษัทผู้ประกอบธุรกิจบัตรเครดิต จำนวน 12 แห่ง ดังตารางที่ 5-2 โดยแต่ละแห่งต่างก็มีสาขาตัวแทนการให้บริการกระจายอยู่ทั่วประเทศ

ตารางที่ 5-2 สถาบันผู้ให้บริการบัตรเครดิต

ลักษณะผู้ให้บริการบัตรเครดิต	**จำนวน (แห่ง)**
ธนาคารพาณิชย์ไทย	10
สาขาของธนาคารต่างประเทศ	2
บริษัทผู้ประกอบธุรกิจบัตรเครดิต	12
รวม	24

ที่มา : ธนาคารแห่งประเทศไทย

เมื่อมาดูแนวโน้มของการขยายตลาดทางด้านบัตรเครดิตแสดงให้เห็นว่า มีผู้ใช้บัตรเครดิตเป็นจำนวนมาก และมีแนวโน้มที่เพิ่มมากขึ้น ดูได้จากข้อมูลของธนาคารแห่งประเทศไทย พบว่า จำนวนบัญชีผู้ใช้บริการบัตรเครดิตในเดือนกรกฎาคม 2554 มีจำนวน 14,796,851 บัญชี ซึ่งเพิ่มขึ้นประมาณร้อยละ 8 จากช่วงเวลาเดียวกันของปีก่อน คือ 13,618,990 บัญชี โดยแบ่งเป็น บัตรเครดิตธนาคารพาณิชย์ไทย 6,048,125 บัตร สาขาธนาคารพาณิชย์ต่างประเทศในประเทศไทย 1,489,541 บัตร และ บริษัทประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงิน 7,259,185 บัตร ซึ่งเพิ่มขึ้นในทุกๆ กลุ่มสถาบัน ดังตารางที่ 5-3

ตารางที่ 5-3 จำนวนบัญชีผู้ใช้บริการบัตรเครดิต

จำนวนบัญชีผู้ใช้บริการบัตรเครดิต		
ลักษณะของผู้ออกบัตร	จำนวนบัญชีทั้งหมดสิ้นสุดเดือนกรกฎาคม 2553	จำนวนบัญชีทั้งหมดสิ้นสุดเดือนกรกฎาคม 2554
1. บัตรเครดิตธนาคารพาณิชย์ไทย	5,436,822	6,048,125
2. สาขาธนาคารพาณิชย์ต่างประเทศในประเทศไทย	1,382,187	1,489,541
3. บริษัทประกอบธุรกิจบัตรเครดิตที่มิใช่สถาบันการเงิน	6,799,981	7,259,185
รวม	13,618,990	14,796,851

ที่มา : ธนาคารแห่งประเทศไทย

และจากข้อมูลของศูนย์วิจัยกสิกรไทยที่ได้สำรวจพฤติกรรมการจับจ่ายใช้สอย และพฤติกรรมการชำระบัตรเครดิตของผู้ถือบัตรเครดิต [50] เพื่อนำมาวิเคราะห์ถึงแนวโน้มของธุรกิจบัตรเครดิต โดยสำรวจระหว่างวันที่ 20 พ.ค.-17 มิ.ย. 2554 จากกลุ่มตัวอย่างทั้งสิ้น 725 คน เป็นการสัมภาษณ์แบบเจาะจงเฉพาะผู้ที่ใช้บัตรเครดิตจับจ่ายสินค้าและบริการ โดยกระจายไปตามสถานที่ต่างๆ เช่น สถานที่ทำงาน และห้างสรรพสินค้าทั่วไปในเขตกรุงเทพมหานคร เป็นต้น พบว่า มีผู้ใช้จ่ายผ่านบัตรเครดิตเพิ่มมากขึ้น และมีร้านค้าที่รับบัตรเครดิตในการใช้จ่ายเพิ่มขึ้นจากเดิมมาก โดยมีพฤติกรรมการใช้จ่ายส่วนใหญ่ 23.1% ใช้ในการชำระค่าสินค้าในซูเปอร์มาร์เกต รองลงมาคือ การใช้จ่ายในร้านอาหาร 20.2% ค่าน้ำมันรถ 19.4% เครื่องแต่งกาย 15.1% ค่าที่พักโรงแรมและท่องเที่ยว 12.6% และอื่นๆ เช่น ดูหนัง ค่ารักษาพยาบาล เป็นต้น คิดเป็น 9.6% ของผู้ตอบแบบสอบถามทั้งหมด

จากข้อมูลข้างต้นแสดงให้เห็นว่าการเติบโตของธุรกิจบัตรดิตยังมีอยู่อย่างต่อเนื่อง และมีแนวโน้วที่จะเพิ่มสูงขึ้น อีกทั้งการใช้บัตรเครดิตยังอยู่ในทุกๆด้านของชีวิตประจำวัน เพราะเป็นเครื่องมือทางการเงินที่มีความสะดวกสบาย ประกอบกับผู้ประกอบการบัตรเครดิตต่างออกสิทธิประโยชน์มากมายในการใช้บัตรเครดิตชำระค่าสินค้าหรือบริการได้มาก จึงเป็นการจูงใจในการใช้บัตรเครดิตเพิ่มขึ้น

5.2.3 Target Market ตลาดกลุ่มเป้าหมาย

จากการศึกษาความเป็นไปได้ในการดำเนินธุรกิจด้านบัตรเครดิต พบว่า ตลาดเป้าหมายสำหรับใช้บริการนวัตกรรมการป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิตนั้น ประกอบด้วยผู้ประกอบการจากธุรกิจบัตรเครดิต แบ่งเป็น ธนาคารพาณิชย์ไทย 10 แห่ง สาขาของธนาคารต่างประเทศ 2 แห่ง และบริษัทผู้ประกอบธุรกิจบัตรเครดิต จำนวน 12 แห่ง

5.3 การวางแผนกลยุทธ์ออกสู่เชิงพาณิชย์

5.3.1 กลยุทธ์ทางการตลาด

การตลาด คือ กิจกรรมของธุรกิจที่กำหนดขึ้นเพื่อที่จะวางแผนราคา ส่งเสริมการขาย การจัดจำหน่าย คุณค่าผลิตภัณฑ์ การบริหาร และความคิดไปยังตลาดเป้าหมาย เพื่อที่จะบรรลุวัตถุประสงค์ โดยกิจกรรมดังกล่าวจะประกอบไปด้วยส่วนประสมทางการตลาด ซึ่งเป็นตัวแปรทางการตลาดที่สามารถควบคุมได้ ที่นำมาใช้เพื่อตอบสนองความต้องการของตลาดเป้าหมาย

ในการกำหนดส่วนประสมทางการตลาดนั้น จะต้องคำนึงถึงความจำเป็น และความต้องการซื้อผลิตภัณฑ์ โดยทั่วไปแล้วนิยมแบ่งออกเป็นกลยุทธ์ทางการตลาดที่เรียกว่า 4Ps (The Four Ps of The Marketing Mix) ซึ่งประกอบด้วยรายละเอียดดังต่อไปนี้

(1) การวางกลยุทธ์ด้านสินค้าและบริการ (Product/Service)

นำเสนอรูปแบบการการยืนยันตัวตนในการใช้บัตรเครดิตรูปแบบใหม่ ผ่านการติดตั้งโปรแกรม และอุปกรณ์เสริม ให้กับธนาคาร หรือสถาบันที่ออกบัตรเครดิต เพื่อตอบสนองความต้องการเรื่องการยืนยันตัวตนในการใช้บัตรเครดิตเพิ่มความปลอดภัยแก่ผู้ใช้บริการบัตรเครดิตให้มีมากยิ่งขึ้น ซึ่งสามารถเพิ่มฐานของลูกค้าได้ถ้าผู้บริโภคมีความเชื่อมั่นในเรื่องความปลอดภัยมาก โดยเป็นรูปแบบการใช้งานที่ง่าย/ไม่ซับซ้อน และสะดวกมากกว่าการใช้งานแบบเดิม ที่ต้องเซ็นชื่อกำกับ หรือสามารถนำไปใช้งานร่วมกับลักษณะการใช้งานแบบเดิมก็ได้ โดยการออกรูปแบบบัตรให้มีลักษณะน่าสนใจแตกต่างจากรูปแบบปกติ

(2) การวางกลยุทธ์ด้านราคา (Price)

เนื่องจากลูกค้าหลักของการใช้นวัตกรรมการยืนยันตัวตนคือผู้ประกอบธุรกิจบัตรเครดิต ดังนั้นการตกลงเรื่องราคาสามารถยืดหยุ่นได้ตามข้อตกลงในสัญญาการให้บริการของระบบการยืนยันตัวตน แบ่งเป็น การค่าติดตั้งระบบ และให้คำปรึกษา คิดครั้งเดียว จำนวน 100,000 บาท และส่วนแบ่งค่าธรรมเนียมในการใช้บัตรเครดิตผ่านระบบนวัตกรรมนี้คิดเป็น 1% ของการใช้ 1 ครั้ง

โดยราคาดังกล่าวเป็นการคำนวณจากการลงทุนในระบบนวัตกรรมนี้ รวมถึงข้อมูลการลงทุนในธุรกิจบัตรเครดิตของธนาคาร คือ บัตรเครดิตโดยทั่วไปมีต้นทุนในการผลิตบัตรเครดิตราคาประมาณใบละ 20-30 บาท [14] ส่วนประกอบที่มีราคาสูงคือส่วนของสติกเกอร์ประเภทพิเศษที่เรียกว่า โฮโลแกรม (แผ่นสะท้อนแสง) เพื่อป้องกันการปลอมแปลงบัตร ซึ่งเมื่อบัตรเครดิตได้มีการนำนวัตกรรมยืนยันตัวตนด้วยคิวอาร์โค้ดและการเข้ารหัสแบบทางเดียวมาเสริมจะไม่ทำให้ราคาเพิ่มขึ้น และได้เปรียบเรื่องราคาเมื่อเทียบกับอุปกรณ์เพิ่มความปลอดภัยแบบอื่น นวัตกรรมนี้จะมีต้นทุนต่ำ เพราะการสร้างคิวอาร์โค้ดไม่มีต้นทุน เนื่องจากสามารถสร้างได้ด้วยโปรแกรมที่หาได้ทั่วไป ในส่วนของโปรแกรมอ่านค่าคิวอาร์โค้ด ก็สามารถติดตั้งได้ในโทรศัพท์เคลื่อนที่ เมื่อเทียบกับเครื่องมืออื่นๆ ที่ต้องเสียค่าใช้จ่ายในการติดตั้งซอฟต์แวร์ และฮาร์ดแวร์ เพื่ออ่านข้อมูลในบัตร ดังนั้นการลงทุนในการผลิตบัตรจึงไม่เปลี่ยนแปลง แต่ในช่วงแรกที่มีการเปลี่ยนแปลงบัตรจากบัตรเครดิตแบบเดิม มาเป็นบัตรเครดิตที่มีนวัตกรรมการยืนยันตัวตนเพิ่มขึ้นมา โดยเป็นการเปลี่ยนแปลงบัตรให้กับลูกค้าเดิม อาจจะทำให้มีต้นทุนเพิ่มขึ้นได้

(3) การวางกลยุทธ์ด้านสถานที่ (Place) โดยคำนึงถึง 2 เรื่อง คือ

1. ช่องทางการจัดจำหน่าย (Chanel of Distribution)

ดำเนินการขายโดยตรง (Direct Sale) และแนะนำให้ความรู้ความเข้าใจเกี่ยวกับระบบ และกระบวนการทำงานของนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตให้แก่ผู้ประกอบการหรือหน่วยงานที่เกี่ยวข้องกับการให้บริการบัตรเครดิตที่เป็นกลุ่มเป้าหมายของนวัตกรรมนี้ เช่น ธนาคาร และผู้ประกอบธุรกิจด้านบัตรเครดิต

2. การกระจายตัวสินค้า (Product of Distribution)

โดยเริ่มต้นจากกลุ่มของธนาคารในประเทศ ขยายไปยังสถาบันต่างๆที่ออกบัตรเครดิตจนถึงธนาคารต่างประเทศ และกลายเป็นการใช้งานรูปแบบเดียวกันทั้งระบบ

(4) การวางกลยุทธ์ด้านการส่งเสริมสินค้า (Promotion)

เนื่องจากนวัตกรรมนี้เป็นนวัตกรรมรูปแบบใหม่ที่ต้องอาศัยการทำการตลาดเพื่อให้ผู้ลงทุนเกิดการยอมรับ และเชื่อมั่นในระบบ ดังนั้นจึงต้องเริ่มจากการแนะนำนวัตกรรมให้เป็นที่รู้จักก่อน จากนั้นจึงส่งเสริมความรู้และเข้าใจในการใช้งาน รวมถึงภาพลักษณ์และประโยชน์ที่จะได้รับจากการใช้งาน เพื่อทราบถึงข้อดีของนวัตกรรม และเกิดการใช้อย่างแพร่หลาย โดยมีวิธีคือ

- ประชาสัมพันธ์รูปแบบการให้บริการกับผู้ลงทุนที่เกี่ยวข้องกับบัตรเครดิต โดยอาจจะออกงานกิจกรรมด้านนวัตกรรม หรืองานเกี่ยวกับการเงิน การธนาคารต่างๆ เพื่อทำความรู้จักและคุ้นเคยกับนักลงทุน และผู้ที่สนใจ

- โฆษณาออกสื่อต่างๆ เช่น เว็บไซต์ ที่ผู้ลงทุนสามารถเข้าถึงได้ โดยใช้รูปแบบการสื่อสารที่เข้าใจง่าย เช่น ภาพ หรือวิดีโอเคลื่อนไหว เพื่อง่ายในการทำความเข้ารูปแบบของระบบการให้บริการ
- กำหนดระยะเวลาให้เปลี่ยนรูปแบบของการใช้บริการบัตรเครดิตเป็นระบบใหม่ฟรีจากผู้ลงทุนให้กับลูกค้าที่สนใจได้เปลี่ยนบัตรและทดลองใช้ระบบใหม่ ภายใน 30 วัน นับจากวันเปิดตัวการให้บริการ

5.4 การวางแผนการลงทุน

เป็นการประมาณการการลงทุนในส่วนที่เพิ่มขึ้นมาจากการใช้งานบัตรเครดิตในรูปแบบปกติ คือ ส่วนที่เป็นระบบโปรแกรม และส่วนที่เป็นอุปกรณ์เพิ่มเติม โดยแหล่งของเงินทุนมาจาก 2 แหล่ง คือ เงินทุนส่วนตัว และเงินกู้ โดยจะศึกษาความเป็นไปได้ในการนำนวัตกรรมการยืนยันตัวตนออกใช้งานเชิงพาณิชย์ ได้อาศัยหลักการประเมินความเป็นไปได้ของการนำเอาอุปกรณ์ไปใช้ในการเพิ่มความปลอดภัยให้ลูกค้าบัตรเครดิตของธนาคาร โดยหลักการประเมินความเป็นไปได้ของโครงการประกอบด้วยขั้นตอนต่อไปนี้

5.4.1 การวิเคราะห์ต้นทุนโครงการ

การวางแผนงบลงทุนของการพัฒนานวัตกรรมการยืนยันตัวตนนี้ได้มีการแบ่งส่วนการใช้จ่าย ดังนี้

- ค่าโปรแกรม

- การลงทุนเรื่องการออกแบบโปรแกรมซอฟต์แวร์และสิทธิในการใช้งาน (Software License) 200,000 บาท

- ค่าอุปกรณ์เพิ่มเติม ได้แก่

- เครื่องคอมพิวเตอร์รับสัญญาณบลูทูธ (ในกรณีที่อุปกรณ์เดิมไม่สามารถรับสัญญาณบลูทูธได้) เครื่องละ 20,000 บาท โดยในระยะแรกจะติดตั้ง 10 สถานที่ให้บริการ รวมเป็นค่าใช้จ่าย 200,000 บาท
- คีย์บอร์ดขนาดเล็กเชื่อมต่อด้วยสัญญาณบลูทูธ (Bluetooth) เอาไว้กดรหัสผ่าน เครื่องละ 700 บาท รวม 10 เครื่อง เป็นเงิน 7,000 บาท

รวมค่าอุปกรณ์เพิ่มเติมที่ติดตั้งในสถานที่ให้บริการนำร่อง 10 แห่งคือ 207,000 บาท

- ค่าบุคลากร

- ค่าจ้างพนักงานในการติดตั้ง อุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์ รวมทั้งการทดสอบการติดตั้งระบบ โดยจำเป็นต้องจ้างพนักงานไอทีเพื่อมาติดตั้งอุปกรณ์ที่สถานที่ให้บริการ (ร้านค้า) และทำการทดสอบระบบการใช้งานก่อนให้บริการลูกค้า ซึ่งค่าใช้จ่ายส่วนนี้จะคิดเป็นรายครั้งที่จ้างไปติดตั้ง ประมาณครั้งละ 3,000 บาท ในสถานที่ให้บริการ 10 แห่ง รวมเป็นค่าใช้จ่าย 30,000 บาท

- ค่าใช้จ่ายอื่นๆ

ค่าใช้จ่ายอื่นๆ ประกอบด้วย ค่าฝึกอบรมการใช้งาน ค่าใช้จ่ายทางการตลาด ค่าซ่อมบำรุง และค่าใช้จ่ายเบ็ดเตล็ด ประมาณ 200,000 บาท ซึ่งสามารถสรุปได้ ดังนี้

- ค่าใช้จ่ายในการฝึกอบรมการใช้งาน

เนื่องจากนวัตกรรมการยืนยันตัวตนต้องมีการใช้งานเพิ่มเติมจากที่เคยใช้งานอยู่เดิมพนักงานประจำสถานที่ให้บริการ อาจจะไม่เข้าใจวิธีการใช้งาน จึงต้องมีการฝึกสอนการใช้งานระยะสั้นๆ เพื่อให้พนักงานสามารถใช้เป็นอุปกรณ์ได้อย่างคล่องแคล่ว

- ค่าพัฒนาและปรับปรุงระบบ

ในกรณีที่มีอุปกรณ์ชำรุดจะต้องเสียค่าใช้จ่ายเพิ่มเติมในการจ้างพนักงานไอทีเข้าไปดูแลซ่อมแซม และมีการพัฒนาโปรแกรมให้ทันสมัยอยู่เสมอ

สรุปเงินลงทุน ต่อ 1 สถานที่ให้บริการ คือ 637,000 บาท ดังตารางที่ 5-4

ตารางที่ 5-4 ประมาณเงินลงทุนต่อ 1 พื้นที่ให้บริการ

รายการ	**เงินลงทุน (บาท)**
ค่าโปรแกรม	200,000
ค่าอุปกรณ์เพิ่มเติม	207,000
ค่าบุคลากร	30,000
ค่าใช้จ่ายอื่นๆ	200,000
รวม	637,000

5.4.2 การประมาณมูลค่าการลงทุน

การประมาณมูลค่าการลงทุนที่เกิดจากการขายนวัตกรรมการยืนยันตัวตน ซึ่งเป็นโปรแกรมการใช้งาน พร้อมสิทธิในการใช้โปรแกรม ให้กับธนาคารที่สนใจนำไปใช้เป็นอุปกรณ์เสริมเพื่อเพิ่มความปลอดภัยในการใช้งานบัตรเครดิตของผู้รับบริการ โดยเป็นการประมาณมูลค่าการลงทุนจากการขายนวัตกรรมการยืนยันตัวตนพร้อมทั้งอุปกรณ์และการติดตั้ง โดยตั้งราคาให้คำนึงถึงค่าใช้จ่ายในการลงทุน ซึ่งในส่วนนี้จะประกอบด้วย

- ค่าการออกแบบโปรแกรมและสิทธิในการใช้งาน 200,000 บาท
- ค่าอุปกรณ์เพิ่มเติม ได้แก่ เครื่องคอมพิวเตอร์รับสัญญาณบลูทูธ และคีย์บอร์ดขนาดเล็กเชื่อมต่อด้วยสัญญาณบลูทูธ จุดละ 207,000 บาท
- ค่าบุคลากรติดตั้งอุปกรณ์และลงโปรแกรม จุดละ 30,000 บาท
- ค่าใช้จ่ายอื่นๆ ประมาณ 200,000 บาท

ตารางที่ 5-5 การประมาณมูลค่าการลงทุน

ลำดับ	**รายการ**	**ทุน (ประมาณ)**	**เงินกู้**	**รวม (ประมาณ)**
1.	การวิจัยและศึกษาความเป็นไปได้ในการสร้างนวัตกรรม	300,000	-	300,000
2.	การเก็บข้อมูล	200,000	-	200,000
3.	ดำเนินการทางธุรกิจ - ค่าโปรแกรม - ค่าอุปกรณ์เพิ่มเติม		750,000 (637,000)	750,000

	- ค่าบุคลากร - ค่าใช้จ่ายอื่นๆ(การส่งเสริมการขาย, การโฆษณา)			
4.	จดทะเบียนทรัพย์สินทางปัญญา		250,000	250,000
	รวมมูลค่าการลงทุนทั้งหมด	**500,000 (33%)**	**1,000,000 (67%)**	**1,500,000 (100%)**

5.5 การคุ้มครองทรัพย์สินทางปัญญา

ระบบการยืนยันตัวตนด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียว เป็นรูปแบบนวัตกรรมการเพิ่มความปลอดภัยลักษณะใหม่ จึงเสี่ยงต่อการลอกเลียนแบบ ทั้งทางด้านเทคโนโลยีและรูปแบบการใช้งาน ดังนั้นเพื่อป้องกันปัญหาการลอกเลียนแบบดังกล่าว จึงต้องมีการคุ้มครองทรัพย์สินทางปัญญาขึ้น โดยระบบการยืนยันตัวตนด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียวจะจดทะเบียนคุ้มครองลิขสิทธิระบบการทำงาน ซึ่งตามนิยามลิขสิทธิตามที่กรมทรัพย์สินทางปัญญา [51] กล่าวไว้ว่า ลิขสิทธิ คือ “สิทธิแต่เพียงผู้เดียวที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ริเริ่มโดยการใช้สติปัญญาความรู้ ความสามารถ และความวิริยะอุตสาหะของตนเองในการสร้างสรรค์ โดยไม่ลอกเลียนงานของผู้อื่น โดยงานที่สร้างสรรค์ต้องเป็นงานตามประเภทที่กฎหมายลิขสิทธิให้คุ้มครอง โดยผู้สร้างสรรค์จะได้รับความคุ้มครองทันทีที่สร้างสรรค์โดยไม่ต้องจดทะเบียน” โดยกฎหมายลิขสิทธิให้ความคุ้มครองแก่งานสร้างสรรค์ 9 ประเภทตามที่กฎหมายกำหนด ได้แก่

1. งานวรรณกรรม (หนังสือ จุลสาร สิ่งพิมพ์ คำปราศรัย โปรแกรมคอมพิวเตอร์ ฯลฯ)
2. งานนาฏกรรม (ท่ารำ ท่าเต้น ฯลฯ)
3. งานศิลปกรรม (จิตรกรรม ประติมากรรม ภาพพิมพ์ ภาพถ่าย ศิลปประยุกต์ ฯลฯ)
4. งานดนตรีกรรม (ทำนองและเนื้อร้อง ฯลฯ)
5. งานสิ่งบันทึกเสียง (เทป ซีดี)
6. งานโสตทัศนวัสดุ (วีซีดี ดีวีดี หรืองานที่มีภาพหรือมีทั้งภาพและเสียง)
7. งานภาพยนตร์

8. งานแพร่เสียงแพร่ภาพ

9. งานอื่นใดในแผนกวรรณคดี วิทยาศาสตร์ หรือศิลปะ

ซึ่งระบบการยืนยันตัวตนด้วยคิวอาร์โค้ด และการเข้ารหัสแบบทางเดียวจัดอยู่ในประเภทที่ 1 คือ “งานวรรณกรรม” [อ้างอิงจาก พระราชบัญญัติลิขสิทธิ พ.ศ. 2537] กล่าวไว้ว่า วรรณกรรม หมายความว่า งานนิพนธ์ที่ทำขึ้นทุกชนิด เช่น หนังสือ จุลสาร สิ่งเขียน สิ่งพิมพ์ ปาฐกถา เทศนา คำปราศรัย สุนทรพจน์ และให้หมายความรวมถึงโปรแกรมคอมพิวเตอร์ด้วย ซึ่งหมายถึง คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่นำไปใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างหนึ่งอย่างใด ทั้งนี้ ไม่ว่าจะเป็นภาษาโปรแกรมคอมพิวเตอร์ในลักษณะใด โดยนวัตกรรมยืนยันตัวตนด้วยคิวอาร์โค้ดและการเข้ารหัสแบบทางเดียวมีการป้องกันดังนี้

1. ป้องกันการลอกเลียนแบบภาพรวมของระบบ รวมถึงวิธีการใช้คิวอาร์โค้ด ร่วมกับ การเข้ารหัสแบบทางเดียว ห้ามนำไปใช้ในลักษณะอื่น หรือดัดแปลงไปใช้กับงานประเภทอื่น ก่อนที่จะได้รับความยินยอมจากผู้พัฒนาเท่านั้น

2. กรณีที่มีการลงทุนกับผู้ลงทุนใช้นวัตกรรมเกิดขึ้น

- ในด้านการติดตั้งระบบ และลักษณะการใช้งาน ผู้ลงทุนจะต้องติดต่อกับผู้พัฒนาโดยตรงเท่านั้น

- ในด้านการเผยแพร่ ไม่เปิดเผยขั้นตอนการได้มาซึ่งรหัสต่อสาธารณะ เพื่อป้องกันการนำไปทำซ้ำ หรือลอกเลียนแบบ รวมทั้งการโฆษณาตามสื่อต่างๆ สิ่งพิมพ์ หรือวิธีการใดๆ จะต้องได้รับการตรวจสอบ และความยินยอมจากผู้พัฒนาก่อนทุกครั้ง

บทที่ 6

สรุปผลการศึกษาและข้อเสนอแนะ

6.1 สรุปผลการศึกษา

จากการศึกษาข้อมูล ทฤษฎี และแนวคิดจากแหล่งต่างๆ นำมาสู่แนวคิดการพัฒนานวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR-Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) โดยการทดสอบสมมติฐานเรื่องทัศนคติ และความต้องการ พบว่ากลุ่มตัวอย่างมีความสนใจ และมีความต้องการในระบบรักษาความปลอดภัยของบัตรเครดิตเฉลี่ยในระดับมาก จากกลุ่มตัวอย่างทั้งหมด 107 คน นอกจากนั้นการทดสอบการยอมรับในระบบนวัตกรรมจากการสุ่มตัวอย่างจากกลุ่มตัวอย่างเดิมจำนวน 50 คน พบว่ามีความความพึงพอใจเฉลี่ยในระดับมาก แต่มีข้อเสนอแนะเพิ่มเติมในเรื่องของการสร้างความน่าเชื่อถือและรูปลักษณ์ของนวัตกรรมให้น่าสนใจมากยิ่งขึ้น

จากการรวบรวมข้อมูลข้างต้นพบว่าการนำคิวอาร์โค้ดมาใช้ นอกจากจะมีคุณสมบัติการเก็บข้อมูลที่หลากหลาย การใช้งานที่ง่ายตามที่ต้องการแล้ว ยังมีรูปลักษณ์ที่แปลก และสามารถช่วยเพิ่มความน่าสนใจในนวัตกรรมนี้ได้

โดยสรุปข้อเด่นในการใช้ คิวอาร์โค้ด ร่วมกับ ฟังก์ชันแฮช มาสู่นวัตกรรมนี้ได้ คือ

1. การใช้ฟังก์ชันแฮชในการสร้างรหัสลับ เมื่อใช้งานจะต้องเอาข้อมูลแฮชออกมาดูคิวอาร์โค้ดจะแสดงให้เห็นค่าแฮชเพื่อใช้ในการเปรียบเทียบ หรือตรวจสอบความถูกต้องได้ทันทีโดยกระบวนการทั้งหมดเป็นแบบออฟไลน์ไม่ต้องพึ่งพาเครือข่ายคอมพิวเตอร์ แต่เครื่องมืออื่นจะต้องส่งข้อมูลเพื่อตรวจสอบความถูกต้องที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) ผ่านเครือข่ายคอมพิวเตอร์เท่านั้น

2. มีความคงทนต่อความเสียหาย คือ สามารถค้นคืนข้อมูลได้แม้บัตรเครดิตมีความเสียหาย แต่เครื่องมืออื่นๆ เช่น แถบแม่เหล็ก จะเสียหายได้ง่ายถ้ามีตัวกระตุ้น เช่น การเก็บไว้ใกล้กับแม่เหล็ก แถบแม่เหล็กที่บัตรก็จะเสียหายทำให้ข้อมูลหาย หรือเพี้ยนไป ไม่สามารถอ่านข้อมูลได้ แต่คิวอาร์โค้ดไม่มีผลต่อแม่เหล็ก และถึงแม้โค้ดเสียหายไปบางส่วนก็สามารถค้นคืนข้อมูลทั้งหมดได้

3. ราคาถูก เพราะในการสร้างคิวอาร์โค้ดไม่มีต้นทุน เนื่องจากสามารถสร้างได้ด้วยโปรแกรมที่หาได้ทั่วไป และสามารถติดตั้งโปรแกรมอ่านได้ในโทรศัพท์เคลื่อนที่ เมื่อเทียบกับเครื่องมืออื่นๆ ที่ต้องเสียค่าใช้จ่ายในการติดตั้งซอฟต์แวร์ และฮาร์ดแวร์ เพื่ออ่านข้อมูลในบัตร

4. ลดความเสี่ยงต่อการโจรกรรมข้อมูลทางสายหรือที่คอมพิวเตอร์แม่ข่ายเพราะไม่มีการตรวจสอบข้อมูลผ่านเครือข่ายคอมพิวเตอร์

5. คิวอาร์โค้ดจะสามารถบรรจุข้อมูลได้มาก และหลากหลายรูปแบบ นอกจากตัวอักษรอาจเป็นลักษณะของรูป หรือ สัญลักษณ์อื่นๆ ที่บาร์โค้ดไม่สามารถบรรจุได้ ซึ่งในที่นี้นำมาเก็บข้อมูลที่นำไปเข้าฟังก์ชันแฮช แปลงค่าเป็นรหัสแฮชเพื่อความปลอดภัย ซึ่งถ้านำข้อมูลนั้นไปบรรจุด้วยวิธีอื่นๆ เช่น แถบแม่เหล็ก ก็เท่ากับว่ายอมให้บุคคลอื่นดึงข้อมูลทั้งหมดมาดูได้ คือมีช่องทางในการดึงข้อมูลทั้งหมดออกมา ซึ่งในนั้นอาจจะมีข้อมูลบางส่วนที่ทางธนาคารอยากจะเก็บไว้เป็นความลับก็ได้ ทำให้มีความปลอดภัยน้อยลง

6.2 ปัญหาและอุปสรรค

1. เนื่องจากนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยคิวอาร์โค้ดและการเข้ารหัสแบบทางเดียว เป็นแนวคิดใหม่ ทำให้ความน่าเชื่อถือที่นักลงทุนมีต่อนวัตกรรมนี้ ค่อนข้างน้อย จึงจำเป็นที่ต้องต้องหาข้อมูลมาสนับสนุนและอธิบายการทำงานของระบบนี้ให้ชัดเจน

2. การใช้อุปกรณ์ในการทดสอบการทำงาน มีข้อจำกัดในเรื่องของเครื่องอ่านค่าคิวอาร์โค้ดที่ต้องใช้อุปกรณ์ที่มีกล้องถ่ายรูปสแกนสัญลักษณ์เพื่ออ่านค่าแฮช โดยในการทดลองใช้นวัตกรรมต้นแบบ ใช้การอ่านค่าแฮชผ่านโทรศัพท์มือถือสมาร์ทโฟนที่มีกล้องถ่ายรูป และติดตั้งโปรแกรมการอ่านค่าคิวอาร์โค้ด แต่ในการใช้งานจริงร้านค้าอาจจะไม่มีโทรศัพท์มือถืออ่านค่าคิวอาร์โค้ดได้ ดังนั้นอาจจะต้องคำนึงถึงเรื่องต้นทุนการใช้อุปกรณ์การอ่านเพิ่มขึ้นมาด้วย

3. การเก็บข้อมูลจากกลุ่มตัวอย่าง เป็นการเก็บจากกลุ่มที่อยู่ในพื้นที่ของกรุงเทพมหานครเท่านั้น ซึ่งความคิดเห็นของกลุ่มคนในพื้นที่อื่นอาจมีความแตกต่างได้ ดังนั้นผลที่ได้อาจจะไม่ใช่ความคิดเห็นของประชากรทั้งหมด ซึ่งถ้าต้องการผลของตัวแทนทั้งประเทศ จะต้องมีการเก็บตัวอย่างเพิ่มเติม

4. จากการสัมภาษณ์ ส่วนของตัวแทนผู้ลงทุนในธุรกิจบัตรเครดิต มีความสนใจในตัวนวัตกรรม แต่ธนาคารเพียงแห่งเดียวไม่สามารถตัดสินใจการดำเนินการใดได้ ต้องอาศัยการร่วมมือกันของธนาคารทุกแห่ง ที่มีการทำธุรกรรมผ่านบัตรเครดิต ออกเป็นข้อตกลงร่วมกันในการใช้งานระบบใหม่ ซึ่งจำเป็นต้องมีการคำนวณด้านความคุ้มค่าในการลงทุน และสอบถามความร่วมมือกับ

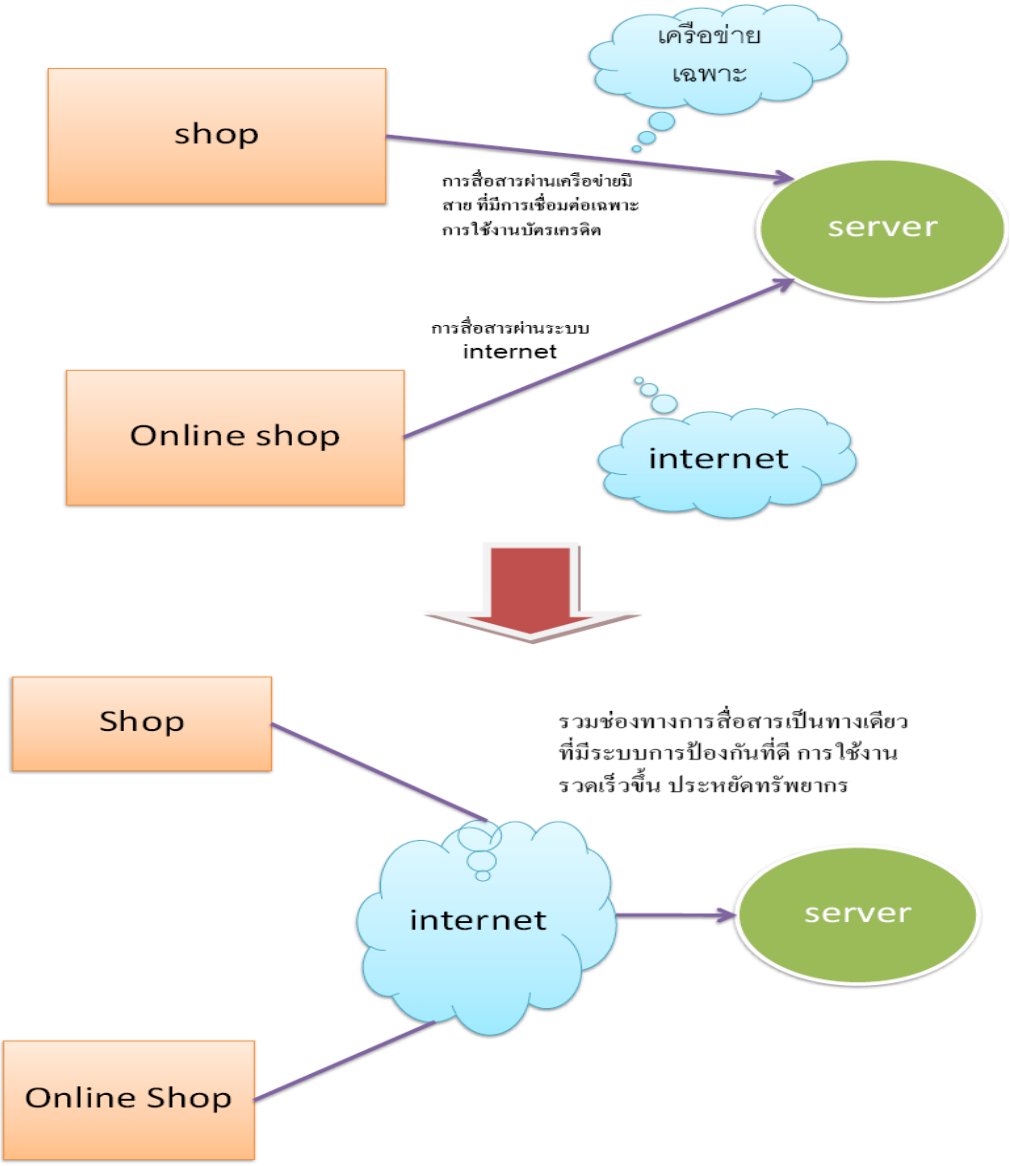
ธนาคารอื่นๆเพิ่มเติม ในส่วนของร้านค้าการใช้งานนวัตกรรมไม่ได้ทำให้เกิดความยุ่งยาก หรือเพิ่มภาระ และไม่มีปัญหาถ้าจะมีการเปลี่ยนแปลงรูปแบบการยืนยันตัวตนในการใช้บัตรเครดิต

6.3 ข้อเสนอแนะ และการวิจัยต่อในอนาคต

จากการศึกษาความเป็นไปได้ในการนำนวัตกรรมเข้าสู่เชิงพาณิชย์ เพื่อนำไปสู่การพัฒนาระบบที่ช่วยยืนยันตัวตนของผู้ใช้บริการบัตรเครดิต และเพิ่มความปลอดภัยในการใช้งานบัตรเครดิตนั้น จะเห็นได้ว่านอกจากการสอบถามความสนใจของผู้ลงทุนในธุรกิจนี้แล้ว การศึกษาทัศนคติ และการยอมรับจากกลุ่มผู้ใช้งานจริงก็มีความสำคัญ เพราะเป็นส่วนประกอบในการตัดสินใจว่าการดำเนินธุรกิจในนวัตกรรมนี้มีแนวโน้มไปในทางที่ดีหรือไม่ สมควรจะลงทุนหรือไม่ ทั้งนี้เพื่อเป็นการเพิ่มความมั่นใจในการนำระบบการยืนยันตัวตนนี้ไปประยุกต์ใช้งานต่อสำหรับนักลงทุน หรือผู้ประกอบการด้านบัตรเครดิต นอกจากนั้นยังทำให้ทราบถึงความต้องการเพิ่มเติมข้อเสนอแนะอื่นๆหลังจากการใช้งาน นำไปสู่การพัฒนาระบบการยืนยันตัวตนที่ดีมากยิ่งขึ้น

นอกจากนั้นการนำคิวอาร์โค้ดมาใช้งานในนวัตกรรมนี้ เป็นเพียงการนำมาเก็บค่าแฮชเพื่อใช้แสดงการยืนยันตัวตนเท่านั้น แต่ด้วยคุณสมบัติของคิวอาร์โค้ดที่มากมาย เช่น เก็บข้อมูลได้มาก สามารถเก็บข้อมูลในรูปแบบที่หลากหลาย ดังที่ได้กล่าวไว้ในบทที่ 2 ทำให้การพัฒนานวัตกรรมขั้นต่อไปสามารถนำข้อดีของคิวอาร์โค้ดด้านอื่นๆมาประยุกต์ใช้ เพื่อเพิ่มความปลอดภัยในการใช้บัตรเครดิต หรือเพิ่มประสิทธิภาพในการทำงานของบัตรเครดิตให้น่าสนใจได้มากขึ้น

การวิจัยต่อในอนาคตอาจจะดูในเรื่องของเครือข่ายการใช้งานบัตรเครดิตดังภาพที่ 6-1 คือ ดูความเป็นไปได้ในการใช้งานกับเครือข่ายอินเตอร์เนต ซึ่งจะสามารถลดงบประมาณในการติดตั้งอุปกรณ์เฉพาะซึ่งเสี่ยงต่อการโจรกรรมข้อมูลทางสาย หรือ Server ที่จะทำงานหนักเมื่อมีการส่งข้อมูลในช่วงเวลาเดียวมากๆ ดังนั้นในอนาคตอาจจะไม่มีตัวของฮาร์ดแวร์ (Hardware) ที่ใช้ในการอ่านข้อมูล แต่มาเป็นรูปแบบของซอฟแวร์ (Software) แทน ทำให้ประหยัดค่าใช้จ่ายมากกว่า อีกทั้งการสื่อสารแบบไร้สายในอนาคตจะได้รับการพัฒนาให้มีประสิทธิภาพมากขึ้น ทำให้สะดวกต่อการใช้เทคโนโลยี และให้ความปลอดภัยมากขึ้นในการซื้อของผ่านระบบออนไลน์ เพราะสามารถระบุตัวตนได้



ภาพที่ 6-1 แสดงการเปลี่ยนผ่านระบบเครือข่ายของการใช้งานในร้านค้า และระบบออนไลน์

นอกจากนั้นคิวอาร์โค้ดที่มีความเร็วในการสื่อสารสูงกว่าบาร์โค้ดธรรมดา คือ มีประสิทธิภาพในการอ่านได้อย่างรวดเร็ว และมีความจุมากกว่า ในอนาคตอาจจะประยุกต์เพิ่มคุณสมบัติของบัตรเครดิตด้วยคิวอาร์โค้ด เช่น เพิ่มข้อมูลอื่นๆ นอกจากค่าแฮชได้

รายการอ้างอิง

[1] ศูนย์วิจัยกสิกรไทย. สงกรานต์ปี 2554 คึกคัก คาดมูลค่าการใช้จ่ายผ่านบัตรเครดิตเดือนเมษายนเติบโตร้อยละ15.0-16.0. 17, 3080 (12 เมษายน 2554).

[2] ธนาคารแห่งประเทศไทย. การให้บริการบัตรเครดิตแยกตามประเภทบัตรเครดิต. [ออนไลน์]. 2554. แหล่งที่มา: http://www2.bot.or.th/statistics/ReportPage.aspx?reportID=269&language=th [2554, กรกฎาคม 30]

[3] ศูนย์พยากรณ์เศรษฐกิจและธุรกิจ มหาวิทยาลัยหอการค้าไทย. สำรวจพฤติกรรมการใช้จ่ายและความคิดเห็นเกี่ยวกับหนี้บัตรเครดิตของประชาชน. [ออนไลน์]. 2550. แหล่งที่มา: http://utcc2.utcc.ac.th/localuser/cebf /download.php?display=cbp [2553, ตุลาคม 29]

[4] สำนักงานตำรวจแห่งชาติ. สถิติการรับแจ้งและจับกุมกลุ่มคดีอาญาที่น่าสนใจ จำแนกตามประเภทคดีที่รับแจ้ง ทั่วราชอาณาจักร ช่วงปี พ.ศ. 2543-2552, 2553.

[5] สำนักงานตำรวจแห่งชาติ. สถิติการรับแจ้งและจับกุมกลุ่มคดีประทุษร้ายต่อทรัพย์ จำแนกตามประเภทคดีที่รับแจ้ง ทั่วราชอาณาจักร ช่วงปี พ.ศ. 2543-2552, 2553.

[6] ณัฐจิตต์ บูราณทวีคูณ. QR Code QR cool รหัสมหัศจรรย์การตลาด. นิตยสาร The marketeer. ฉบับที่ 122, เมษายน 2553.

[7] ลัญฉกร วุฒิสิทธิกุลกิจ และคณะ. วิทยาการรหัสลับเบื้องต้น. พิมพ์ครั้งที่ 1 กรุงเทพมหานคร : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2548.

[8] Del I. Hawkins et al. Consumer behavior: building marketing strategy. Boston: McGraw-Hill Irwin, 9th ed, c2004.

[9] Robert G.C., Stage-gate Systems: A new Tool for Managing New Products. Business Honrizons, 1990.

[10] Crawford, C. Merle and Anthony DiBenedetto. New Products Management. 9th ed. McGraw Hill, 2008.

[11] Davis, F. D., Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly 13(3): 319–340. 1989

[12] มนัสวี มาลา. พฤติกรรมการใช้บัตรเครดิตของผู้บริโภคในเขตกรุงเทพมหานคร. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชาบริหารธุรกิจ มหาวิทยาลัยราชภัฏธนบุรี. 2549.

[13] เมลดา วงษ์วิกิจการ. เหตุผลในการตัดสินใจเลือกใช้บัตรเครดิตของพนักงานธนาคารกรุงเทพ จำกัด (มหาชน). วิทยานิพนธ์ปริญญามหาบัณฑิต, คณะศิลปศาสตร์ มหาวิทยาลัยเกษตรศาสตร์. 2547.

[14] นิตยสารผู้จัดการ. บัตรเครดิต : บริโภคยิ่งมากยิ่งกำไรสูง.[ออนไลน์]. 2535. แหล่งที่มา: http://www.gotomanager.com/news/printnews.aspx?id=6514 [2554, กรกฎาคม 30]

[15] สุรเชษฐ์ ชีรวินิจ. โกงสะบัด โกงกันสะบัตร (โกงกันสะบัดกับบัตรเครดิต). บริษัท คอมฟอร์ม จำกัด. กรุงเทพมหานคร: พิมพ์ครั้งที่ 1, 2541.

[16] ธนาคารกสิกรไทย. ประวัติธนาคาร. [ออนไลน์]. แหล่งที่มา : http://www.kasikornbank.com /TH/AboutUs/CompanyBackground/Pages/CompanyBackground.aspx [2553, ตุลาคม 29]

[17] นิตยสาร Positioning. ซิตี้แบงก์จับมือการบินไทย ออกบัตรเครดิตซิตี้แบงก์รอยัล ออร์คิด พลัส แพลตตินั่ม ซีเล็คท์. [ออนไลน์]. 2549. แหล่งที่มา: http://www.positioningmag.com /prnews/prnews.aspx?id=53876. [2553, ตุลาคม 29]

[18] วิชิต วานิชธนันกูล. ระบบรักษาความปลอดภัยของการชำระเงินด้วยบัตรเครดิต. สารนิพนธ์ปริญญามหาบัณฑิต, สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ. 2548.

[19] Etienne Gerts. Toward an Improved EMV Credit Card Certification. Master's Thesis, Software Engineering Research Group Department of Software Technology Faculty EEMCS, Delft University of Technology Delft, the Netherlands, 2007

[20] วิชาการดอทคอม. Bar code ในแถบแม่เหล็กบนบัตรเครดิต. [ออนไลน์]. 2550. แหล่งที่มา: http://www.vcharkarn .com/vcafe/115937 [2553, ตุลาคม 29]

[21] บัตรอิเล็กทรอนิกส์กลาง. Smart Card. [ออนไลน์]. 2552. แหล่งที่มา: http://www.dld.go.th/ict/th/index.php?option=com_content&view=article&id=54:-smart-card&catid=46:general&Itemid=55 [2553, ตุลาคม 29]

[22] ecebs Advanced Smartcard Technologies. What is a Smart Card ?. [online]. 2011. Available form: http://www.ecebs.com/what-is-a-smart-card-a220 [2554, กรกฎาคม 30]

[23] พันธ์ศักดิ์ ศรีทรัพย์. สมาร์ทการ์ด : บัตรอเนกประสงค์สำหรับวันนี้และอนาคต. วารสารไมโครคอมพิวเตอร์ (ธันวาคม 2540)

[24] Wireless Smart Card. เทคโนโลยี ไวร์เลส สมาร์ทการ์ด. [ออนไลน์]. 2552. แหล่งที่มา: http://www.it.co.th/computerdetail.php?n_id=28 [2553, ตุลาคม 29]

[25] True Innovation Awards 2010. บัตรเครดิตรุ่นใหม่ซ่อนหมายเลขบัตรได้. [ออนไลน์]. 2553. แหล่งที่มา: http://www.trueinnovationaward.com/ blog/?tag =electronic-stripe [2553, ตุลาคม 30]

[26] ชมรมผู้ตรวจสอบภายในธนาคารและสถาบันการเงิน. 7อันดับ ภัยอินเทอร์เน็ตในประเทศไทย. [ออนไลน์]. 2550. แหล่งที่มา: http://www.bfiia.org/index.php?lay=show&ac=article &Id=537975&Ntype=2 [2553, ตุลาคม 30]

[27] ชมรมผู้ตรวจสอบภายในธนาคารและสถาบันการเงิน. การทุจริตบัตรเครดิตโดยการดูดข้อมูลบัตรเครดิตผ่านทางสายโทรศัพท์. [ออนไลน์]. 2549. แหล่งที่มา: http://www.bfiia.org/index.php? lay=show&ac= article&Id=5324681&Ntype=2 [2553, ตุลาคม 30]

[28] เตือน"สมาร์ทการ์ด" ล่อใจ"แฮกเกอร์". [ออนไลน์]. 2553. แหล่งที่มา: http://www.itmelody.com/free_tip/AR_ ViewItem.php?id=144 [2553, ตุลาคม 30]

[29] วารสารชมรมตรวจสอบและป้องกันการทุจริตฉบับ 1 สมาคมธนาคารไทย. ข่าวสารการทุจริต [ออนไลน์]. 2553. แหล่งที่มา: http://tba.or.th/club/fmc/index.php?option=com_content &view=article&id=16:case-272553-&catid=2:fnews1&Itemid=3) [2553, ตุลาคม 30]

[30] ศราวุธ ดีหมื่นไวย์. เจาะข้อมูล 'บัตรเครดิต' ภัยร้ายที่ทวีความรุนแรง. หนังสือพิมพ์เดลินิวส์ (16 กรกฎาคม 2552): 4.

[31] สิริพร จิตต์เจริญธรรม เสาวภา ปานจันทร์ และ เลอศักดิ์ ลิ้มวิวัฒน์กุล. ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ ตัวตน. [ออนไลน์]. 2547. แหล่งที่มา: http://www.thaicert.nectec.or.th/paper/authen/authentication _guide.php [2553, ตุลาคม 30]

[32] Global Technology. มารู้จักมาตรฐาน PCI DSS. [ออนไลน์]. 2552. SRAN e-Newsletter ฉบับเดือนสิงหาคม 2552. แหล่งที่มา:http://www.gbtech.co.th/th/about-us/cert-pci-dsshipaa [2554, กรกฎาคม 31]

[33] พิชัย นิลทองคำ. ประมวลกฎหมายอาญา. ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ .สำนักพิมพ์วิญญูชน. น.669

[34] ชัยกาล พิทยาเกษม และคณะ. แนะนำเรื่องเทคโนโลยีบาร์โค้ด 2 มิติ. ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย. 2549.

[35] Wiseness system co.,ltd. Bar Code. [ออนไลน์]. 2549. แหล่งที่มา: http://www.barcode-wiseness.com [2553, ตุลาคม 30]

[36] ดร.สุวิทชัย คุ้มปีติ. รหัสแถบ (Bar Code). วารสารคอมพิวเตอร์ สมาคมคอมพิวเตอร์แห่งประเทศไทย 15,75 (2531)

[37] ผศ.ดนุวศิน เจริญ. บทความ : รหัสแถบยุคใหม่ (รหัสตอบสนองอย่างรวดเร็ว) กับการพัฒนาธุรกิจในประเทศไทย.[ออนไลน์]. 2553. แหล่งที่มา: http://r64.wikidot.com/qr-code [2553, ตุลาคม 29]

[38] QR Code Generator. RS Error Correction Summary. [online]. 2011. Available form: http://www.cognable.com/view/25/1.xhtml [2554, กรกฎาคม 30]

[39] Pieter de Bruyne., NEW TECHNOLOGIES IN CREDIT CARD AUTHENTICATION., Institute for Communications Technology., pp. 1-5. 1990.

[40] Young Sil Lee., Online Banking Authentication System using Mobile-OTP with QR-code., 2010 National Research Foundation Project., pp. 644-648. 2010.

[41] Sida Lin & Qi Xie., A secure and efficient mutual authentication protocol using hash function. 2009 International Conference on Communications and Mobile Computing., pp. 545-548. 2009.

[42] Essam Abdel-azeem et al., Cryptographic Security Evaluation of MD4 Hash Function. PROCEEDINGS OF THE THIRTEENTH NATIONAL RADIO SCIENCE CONFERENCE., pp.1-10. 1996.

[43] Chuanhua Zhou & Baohua Zhao., Study of One-way Hash Function to Digital Signature Technology., IEEE@2006., pp. 1503-1506. 2006.

[44] Kuan-Chieh Liao et al., A One-Time Password Scheme with QR-Code Based on Mobile Phone. 2009 Fifth International Joint Conference on INC, IMS and IDC., pp. 2069-2071. 2009.

[45] Guenther Starnberger, Lorenz Froihofer and Karl M.Goeschka., QR-TAN:Secure Mobile Transaction Authentication., 2009 International Conference on Availability, Reliability and Security., pp. 578-583. 2009.

[46] Jung Eun Kim. A Secure on-line credit card transaction method based on Kerberos Authentication protocol. Bachelor of Engineering, Computer Engineering Kyungil University, South Korea, 1999

[47] วุฒิชัย เชื้อวงศ์พรหม. การใช้บัตรเครดิตในสังคมไทย. วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชาไทยศึกษา มหาวิทยาลัยรามคำแหง. 2543.

[48] Del I. Hawkins et al., Consumer behavior: building marketing strategy, Boston : McGraw-Hill Irwin, 9th ed, c2004.

[49] Philip Kotler, Kevin Lane Keller., Marketing Management, Pearson Education International 13th edition, 2009

[50] ทิศทางเศรษฐกิจ-สินค้าแพงเปลี่ยนพฤติกรรมผู้ถือบัตรเครดิต, หนังสือพิมพ์ โลกวันนี้. ปีที่ 12 ฉบับที่ 3094 (11 กรกฎาคม 2554)

[51] กรมทรัพย์สินทางปัญญา. ลิขสิทธิ์ .[ออนไลน์]. แหล่งที่มา: http://www.ipthailand.go.th/ipthailand/index.php?option=com_content&task=section&id=21&Itemid=198 [2553, ตุลาคม 29]

ภาคผนวก

ภาคผนวก ก

ภาคผนวก ก

แบบสอบถามเรื่อง ศึกษาความคิดเห็นของผู้บริโภคในความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต

คำชี้แจง

แบบสอบถามนี้เป็นส่วนหนึ่งของการทำวิจัย เพื่อศึกษาความคิดเห็นของผู้บริโภคในความต้องการต่อระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต ของนิสิตปริญญาโท หลักสูตรธุรกิจเทคโนโลยีและการจัดการนวัตกรรม จุฬาลงกรณ์มหาวิทยาลัย ซึ่งจัดทำขึ้นเพื่อเก็บรวบรวมข้อมูล และประมวลผลเป็นงานเชิงวิชาการไม่มีวัตถุประสงค์เพื่อประโยชน์อื่นใด และท่านได้รับเลือกให้เป็นกลุ่มตัวอย่างในการวิจัยครั้งนี้ จึงขอความกรุณาจากท่านช่วยตอบแบบสอบถามตามความเป็นจริงมากที่สุด โดยไม่มีการเผยแพร่ข้อมูลส่วนบุคคลและจะปกปิดข้อมูลไว้เป็นความลับ แบบสอบถาม (Questionnaire) แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 เป็นการสอบถามเกี่ยวกับตัวแปรที่ใช้ในการศึกษา

ส่วนที่ 2 เป็นพฤติกรรมการใช้บัตรเครดิต

ส่วนที่ 3 เป็นการสอบถามข้อมูลทั่วไป

เกณฑ์การให้คะแนน 5 = มากที่สุด 4 = มาก 3 = ปานกลาง

2 = น้อย 1 = น้อยที่สุด

<u>ส่วนที่ 1 ปัจจัยการรับรู้ในเรื่องต่างๆของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต</u>

1. **ความมีประโยชน์**	5	4	3	2	1
คุณคิดว่าการป้องกันการปลอมแปลงลายเซ็นมีความจำเป็น					
คุณคิดว่าบัตรเครดิตจะต้องมีระบบป้องกันการปลอมแปลงให้มากกว่าที่มีอยู่					
คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความคุ้มค่าในการสมัครใช้บริการบัตรเครดิต					
คุณคิดว่าระบบการป้องกันการปลอมแปลงลายเซ็นจะเป็นทางเลือกใหม่ในการป้องกันความปลอดภัยในการใช้บัตรเครดิต					

2. **ความง่ายในการใช้งาน**	5	4	3	2	1
คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นไม่เป็นอุปสรรคกับการใช้งานบัตรเครดิตที่มีอยู่					
คุณคิดว่าต้องสามารถเข้าถึงระบบป้องกันการปลอมแปลงลายเซ็น ได้ทุกที่ ทุกเวลา					
คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นต้องมีขั้นตอนสะดวก และกระชับ ง่ายต่อการใช้งาน					

3. **ความน่าเชื่อถือ**	5	4	3	2	1
คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นสามารถนำไปใช้ได้จริง					
คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นจะสามารถลดความเสี่ยงต่อการถูกโจรกรรมได้					

4. **ทัศนคติต่อเทคโนโลยี**	5	4	3	2	1
คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นมีความน่าสนใจ					
คุณคิดว่าเทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความมั่นใจในการทำธุรกรรมทางการเงิน					

5. **ความตั้งใจในการใช้บริการ**	5	4	3	2	1
คุณตั้งใจว่าจะใช้เทคโนโลยีระบบการป้องกันการปลอมแปลงลายเซ็นในอนาคต					
คุณคิดว่าจะแนะนำให้เพื่อน หรือคนรู้จักใช้ระบบการป้องกันการปลอมแปลงลายเซ็น					

<u>ส่วนที่ 2 พฤติกรรมการใช้บัตรเครดิต ให้ผู้ตอบแบบสอบถามแสดงความคิดเห็นหรือข้อเสนอแนะ</u>

6. **ท่านมีบัตรเครดิตหรือไม่**

( ) มี ( ) ไม่มี (ข้ามไปตอบข้อที่ 9)

7. **ความถี่ในการใช้บัตรเครดิต (ต่อเดือน)**

( ) ไม่มีการใช้ (ข้ามไปตอบข้อที่ 9) ( ) 1 – 5 ครั้ง
( ) 6 – 10 ครั้ง ( ) มากกว่า 10 ครั้งขึ้นไป

8. **ท่านใช้บัตรเครดิตในเรื่องใดบ่อยครั้งที่สุด**

( ) ใช้ซื้อสินค้าอุปโภคบริโภค เช่น อาหาร ข้าวของเครื่องใช้ เครื่องแต่งกาย
( ) ใช้ชำระค่าสาธารณูปโภค เช่น ค่าโทรศัพท์ ค่าน้ำ ค่าไฟ ค่าประกันภัย
( ) ใช้เบิกเงินสดล่วงหน้า
( ) อื่นๆ (โปรดระบุ).....

(สำหรับท่านที่ไม่ใช้บัตรเครดิต)

9. **สาเหตุที่ท่านไม่ใช้บัตรเครดิต**

( ) ไม่มั่นใจในเรื่องความปลอดภัย (การปลอมแปลง,การโจรกรรม)
( ) ไม่อยากมีหนี้สิน
( ) ไม่สะดวก ยุ่งยากในการใช้งาน (ทั้งในเรื่องการสมัคร และการชำระค่าบริการ)
( ) อื่นๆ(โปรดระบุ).....

10. **ข้อเสนอแนะ**

.....
.....
.....

ส่วนที่ 3 ข้อมูลทั่วไป

11. **เพศ**

( ) ชาย ( ) หญิง

12. **อายุ**

( ) 20-29 ( ) 30-39 ( ) 40-49
( ) 50-59 ( ) 60-69 ( ) 70 ขึ้นไป

13. **สถานภาพ**

( ) โสด ( ) สมรส ( ) หม้าย/หย่า

14. ระดับการศึกษา

( ) ต่ำกว่าปริญญาตรี ( ) ปริญญาตรี
( ) ปริญญาโท ( ) สูงกว่าปริญญาโท

15. อาชีพ

( ) พนักงานบริษัทเอกชน ( ) ข้าราชการ
( ) พนักงานรัฐวิสาหกิจ ( ) ธุรกิจส่วนตัว

16. รายได้ต่อเดือน

( ) 15,000 -25,000 ( ) 25,001-35,000
( ) 35,001-45,000 ( ) 45,001-55,000
( ) 55,001 ขึ้นไป

ขอขอบพระคุณทุกท่านเป็นอย่างสูงที่กรุณาให้ความร่วมมือในการตอบแบบสอบถามนี้

ภาคผนวก ข

ภาคผนวก ข

แบบสอบถามเรื่อง ศึกษาการยอมรับของผู้บริโภคต่อนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption)

คำชี้แจง

แบบสอบถามนี้เป็นส่วนหนึ่งของการทำวิจัย เพื่อศึกษาการยอมรับของผู้บริโภคต่อนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตด้วยรหัสตอบสนองอย่างรวดเร็ว (QR Code) และการเข้ารหัสแบบทางเดียว (One-way Encryption) ของนิสิตปริญญาโท หลักสูตรธุรกิจเทคโนโลยีและการจัดการนวัตกรรม จุฬาลงกรณ์มหาวิทยาลัย ซึ่งจัดทำขึ้นเพื่อเก็บรวบรวมข้อมูลและประมวลผลเป็นงานเชิงวิชาการไม่มีวัตถุประสงค์เพื่อประโยชน์อื่นใด และท่านได้รับเลือกให้เป็นกลุ่มตัวอย่างในการวิจัยครั้งนี้ จึงขอความกรุณาจากท่านช่วยตอบแบบสอบถามตามความเป็นจริงมากที่สุด โดยไม่มีการเผยแพร่ข้อมูลส่วนบุคคลและจะปกปิดข้อมูลไว้เป็นความลับ

แบบสอบถาม (Questionnaire) แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 เป็นการสอบถามเกี่ยวกับระบบการทำงานของนวัตกรรม

ส่วนที่ 2 เป็นการสอบถามข้อมูลทั่วไป

เกณฑ์การให้คะแนน 5 = มากที่สุด 4 = มาก 3 = ปานกลาง

2 = น้อย 1 = น้อยที่สุด

<u>ส่วนที่ 1 ปัจจัยการรับรู้ในเรื่องต่างๆของระบบป้องกันการปลอมแปลงลายเซ็นของบัตรเครดิต</u>

1. **ความมีประโยชน์**	5	4	3	2	1
คุณคิดว่าการป้องกันการปลอมแปลงลายเซ็นมีความจำเป็น					
คุณคิดว่าบัตรเครดิตจะต้องมีระบบป้องกันการปลอมแปลงให้มากกว่าที่มีอยู่					
คุณคิดว่าระบบป้องกันการปลอมแปลงลายเซ็นทำให้เกิดความคุ้มค่าในการสมัครใช้บริการบัตรเครดิต					
คุณคิดว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตจะเป็นทางเลือกใหม่ในการป้องกันความปลอดภัยในการใช้บัตรเครดิต					

2. **ความง่ายในการใช้งาน**	5	4	3	2	1
คุณคิดว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตไม่เป็นอุปสรรคกับการใช้งานบัตรเครดิตที่มีอยู่					
คุณคิดว่าสามารถเข้าถึงนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตได้ทุกที่ ทุกเวลา					
คุณคิดว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตมีขั้นตอนสะดวก และกระชับ ง่ายต่อการใช้งาน					

3. **ความน่าเชื่อถือ**	5	4	3	2	1
คุณคิดว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตสามารถนำไปใช้ได้จริง					

	5	4	3	2	1
คุณคิดว่านวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตจะสามารถลดความเสี่ยงต่อการถูกโจรกรรมได้					

4. **ทัศนคติต่อเทคโนโลยี**	5	4	3	2	1
คุณคิดว่าเทคโนโลยีนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตมีความน่าสนใจ					
คุณคิดว่าเทคโนโลยีนวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตทำให้เกิดความมั่นใจในการทำธุรกรรมทางการเงิน					

5. **ความตั้งใจในการใช้บริการ**	5	4	3	2	1
คุณตั้งใจว่าจะใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิตในอนาคต					
คุณคิดว่าจะแนะนำให้เพื่อนหรือคนรู้จัก รับรู้/ใช้นวัตกรรมการยืนยันตัวตนของผู้ใช้บริการบัตรเครดิต					

<u>ส่วนที่ 2 ข้อมูลทั่วไป</u>

6. **เพศ**

( ) ชาย ( ) หญิง

7. **อายุ**

( ) 20-29 ( ) 30-39 ( ) 40-49

( ) 50-59 ( ) 60 ขึ้นไป

8. **ระดับการศึกษา**

( ) ต่ำกว่าปริญญาตรี ( ) ปริญญาตรี

( ) ปริญญาโท ( ) สูงกว่าปริญญาโท

9. **ลักษณะอาชีพ/ลักษณะร้านค้า**

อาชีพ

( ) พนักงานบริษัทเอกชน ( ) ข้าราชการ

( ) พนักงานรัฐวิสาหกิจ ( ) ธุรกิจส่วนตัว

ร้านค้า

( ) ร้านสินค้าบริโภค (เช่น อาหาร ขนม ฯลฯ)

( ) ร้านสินค้าอุปโภค(เช่น เสื้อผ้า รองเท้า กระเป๋า ฯลฯ)

( ) มินิมาร์ท

10. **รายได้ต่อเดือน**

( ) 15,000 -25,000 ( ) 25,001-35,000

( ) 35,001-45,000 ( ) 45,001-55,000

( ) 55,001 ขึ้นไป

ขอขอบพระคุณทุกท่านเป็นอย่างสูงที่กรุณาให้ความร่วมมือในการตอบแบบสอบถามนี้

ภาคผนวก ค

ภาคผนวก ค

สถิติการรับแจ้งและจับกุมกลุ่มคดีอาญาที่น่าสนใจ จำแนกตามประเภทคดีที่รับแจ้ง ทั่วราชอาณาจักร พ.ศ. 2544-2553

สถิติการรับแจ้งและจับกุมกลุ่มคดีอาญาที่น่าสนใจ จำแนกตามประเภทคดีที่รับแจ้ง ทั่วราชอาณาจักร พ.ศ. 2544 - 2553
STATISTICS OF REPORTED AND ARRESTED FOR THE CRIMES OF INTEREST GROUP BY TYPE OF REPORTED CASES, WHOLE KINGDOM: 2001 - 2010

ประเภทคดี	2544 (2001)	2545 (2002)	2546 (2003)	2547 (2004)	2548 (2005)	2549 (2006)	2550 (2007)	2551 (2008)	2552 (2009)	2553 (2010)	Type of cases
					รับแจ้ง (Reported)						
รวม	43,739	48,155	41,077	37,613	41,283	44,037	44,158	43,054	43,266	39,947	Total
โจรกรรมรถจักรยานยนต์	18,362	19,499	18,949	15,819	17,523	20,478	19,851	20,039	21,023	19,455	Motorcycle theft
โจรกรรมรถยนต์	3,087	3,270	2,747	3,197	2,820	2,841	2,976	2,712	3,043	2,605	Car theft
โจรกรรมวัว-กระบือ	310	376	385	289	225	205	132	78	87	88	Cattle theft
โจรกรรมเครื่องมือเกษตร	405	283	253	274	366	323	280	230	121	125	Agricultural insturments theft
ปล้น-ชิงรถยนต์โดยสาร	2	1	6	1	2	-	-	3	1	-	Bus robbery
ปล้น-ชิงรถยนต์แท็กซี่	39	51	34	22	8	3	5	8	9	8	Taxi robbery
ข่มขืนและฆ่า	13	10	8	11	5	6	8	2	12	9	Rape and kill
ลักพาเรียกค่าไถ่	12	18	20	9	12	11	21	16	5	7	Kidnapping
ฉ้อโกง	6,776	7,194	6,772	6,605	8,245	7,338	7,812	7,260	7,231	6,886	Cheation and fraud
ยักยอกทรัพย์	14,733	17,453	11,903	11,386	12,077	12,834	12,983	12,708	11,734	10,764	Misappropriation
					จับ (Arrested)						
รวม	11,860	11,545	6,380	6,030	6,250	7,589	8,434	8,565	8,795	8,824	Total
โจรกรรมรถจักรยานยนต์	4,221	3,487	2,816	2,409	2,382	2,686	3,035	3,588	3,674	3,748	Motorcycle theft
โจรกรรมรถยนต์	291	302	230	201	194	186	240	272	257	270	Car theft
โจรกรรมวัว-กระบือ	98	118	84	61	41	78	56	41	25	39	Cattle theft
โจรกรรมเครื่องมือเกษตร	91	71	40	33	95	72	97	120	49	72	Agricultural insturments theft
ปล้น-ชิงรถยนต์โดยสาร	2	1	4	1	-	-	-	2	1	-	Bus robbery
ปล้น-ชิงรถยนต์แท็กซี่	15	19	17	11	3	-	2	5	7	5	Taxi robbery
ข่มขืนและฆ่า	10	8	6	8	4	5	4	2	8	9	Rape and kill
ลักพาเรียกค่าไถ่	7	14	11	7	8	5	15	13	3	3	Kidnapping
ฉ้อโกง	2,470	2,304	1,591	1,522	1,700	1,806	1,982	1,796	1,889	1,857	Cheation and fraud
ยักยอกทรัพย์	4,855	5,221	1,581	1,777	1,823	2,751	2,983	2,726	2,882	2,721	Misappropriation

ที่มา: สำนักงานตำรวจแห่งชาติ
Source: Royal Thai Police
รวบรวมโดย: สำนักสถิติพยากรณ์ สำนักงานสถิติแห่งชาติ
Compiled by: Statistical Forecasting Bureau, National Statistical Office

ภาคผนวก ง

ภาคผนวก ง

สถิติการรับแจ้งและจับกุมกลุ่มคดีประทุษร้ายต่อทรัพย์ จำแนกตามประเภทคดีที่รับแจ้งทั่วราชอาณาจักร พ.ศ. 2544-2553

สถิติการรับแจ้งและจับกุมกลุ่มคดีประทุษร้ายต่อทรัพย์ จำแนกตามประเภทคดีที่รับแจ้ง ทั่วราชอาณาจักร พ.ศ. 2544 - 2553
STATISTICS OF REPORTED AND ARRESTED FOR THE GROUP OF CRIMES AGAINST PROPERTY BY TYPE OF REPORTED CASES, WHOLE KINGDOM: 2001 - 2010

ประเภทคดี	2544 (2001)	2545 (2002)	2546 (2003)	2547 (2004)	2548 (2005)	2549 (2006)	2550 (2007)	2551 (2008)	2552 (2009)	2553 (2010)	Type of cases
					รับแจ้ง (Reported)						
รวม	65,813	68,906	67,070	68,665	76,183	76,879	73,068	67,188	59,497	56,798	Total
ลักทรัพย์	56,029	57,413	52,988	54,457	60,881	63,649	62,007	57,457	50,412	48,780	Theft
วิ่งราวทรัพย์	2,107	2,952	3,669	3,715	4,451	3,782	2,906	2,817	2,446	2,081	Snatching
รีดเอาทรัพย์	11	12	13	16	62	14	23	17	14	14	Blackmail
กรรโชกทรัพย์	330	286	341	258	338	246	205	251	222	198	Extortion
ชิงทรัพย์ (รวม)	1,832	2,100	2,538	2,463	2,749	2,319	2,034	1,732	1,415	1,167	Robbery
บาดเจ็บ	536	557	644	634	594	582	463	424	358	287	Injury to victim
ไม่บาดเจ็บ	1,396	1,543	1,894	1,829	2,155	1,737	1,571	1,308	1,057	880	No injury to victim
ปล้นทรัพย์	669	841	1,712	1,571	1,408	1,244	932	711	579	471	Gang robbery
รับของโจร	318	298	298	261	363	340	244	207	185	203	Receiving stolen property
ทำให้เสียทรัพย์	4,417	4,804	5,511	5,824	5,961	5,275	4,712	3,998	4,244	3,874	Vandalism
					จับ (Arrested)						
รวม	33,819	31,691	24,629	24,464	25,848	28,691	30,849	30,800	25,736	26,840	Total
ลักทรัพย์	27,461	24,992	18,065	18,142	19,427	22,155	24,934	25,150	19,945	21,682	Theft
วิ่งราวทรัพย์	1,463	1,716	1,868	1,783	1,860	1,885	1,723	1,797	1,627	1,385	Snatching
รีดเอาทรัพย์	6	7	5	7	17	8	9	9	9	9	Blackmail
กรรโชกทรัพย์	228	200	164	134	162	141	116	146	131	119	Extortion
ชิงทรัพย์ (รวม)	1,019	1,051	1,059	1,032	1,042	1,068	1,029	951	892	811	Robbery
บาดเจ็บ	272	279	262	259	252	278	243	233	227	200	Injury to victim
ไม่บาดเจ็บ	747	772	797	773	790	790	786	718	665	611	No injury to victim
ปล้นทรัพย์	412	536	893	856	675	687	581	408	388	335	Gang robbery
รับของโจร	273	254	244	227	293	274	204	170	131	148	Receiving stolen property
ทำให้เสียทรัพย์	2,857	2,835	2,331	2,283	2,382	2,463	2,270	2,169	2,615	2,351	Vandalism

ที่มา: สำนักงานตำรวจแห่งชาติ
Source: Royal Thai Police
รวบรวมโดย: สำนักสถิติพยากรณ์ สำนักงานสถิติแห่งชาติ
Compiled by: Statistical Forecasting Bureau, National Statistical Office

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวนันทวัน สันทศนะสุวรรณ เกิดเมื่อวันที่ 29 ตุลาคม 2526 สำเร็จการศึกษาระดับมัธยมปลายจากโรงเรียนศึกษานารี และระดับปริญญาตรีสังคมสงเคราะห์ศาสตรบัณฑิต คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีการศึกษา 2549 จากนั้นได้เข้าศึกษาต่อในหลักสูตรธุรกิจเทคโนโลยีและการจัดการนวัตกรรม คณะบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย เมื่อภาคต้นปีการศึกษา 2552 ปัจจุบันทำงานที่ ธนาคารกสิกรไทย ในฝ่ายวิเทศพาณิชย์และแฟคตอริ่ง ตำแหน่ง เจ้าหน้าที่จัดเตรียมเอกสารธุรกิจต่างประเทศ