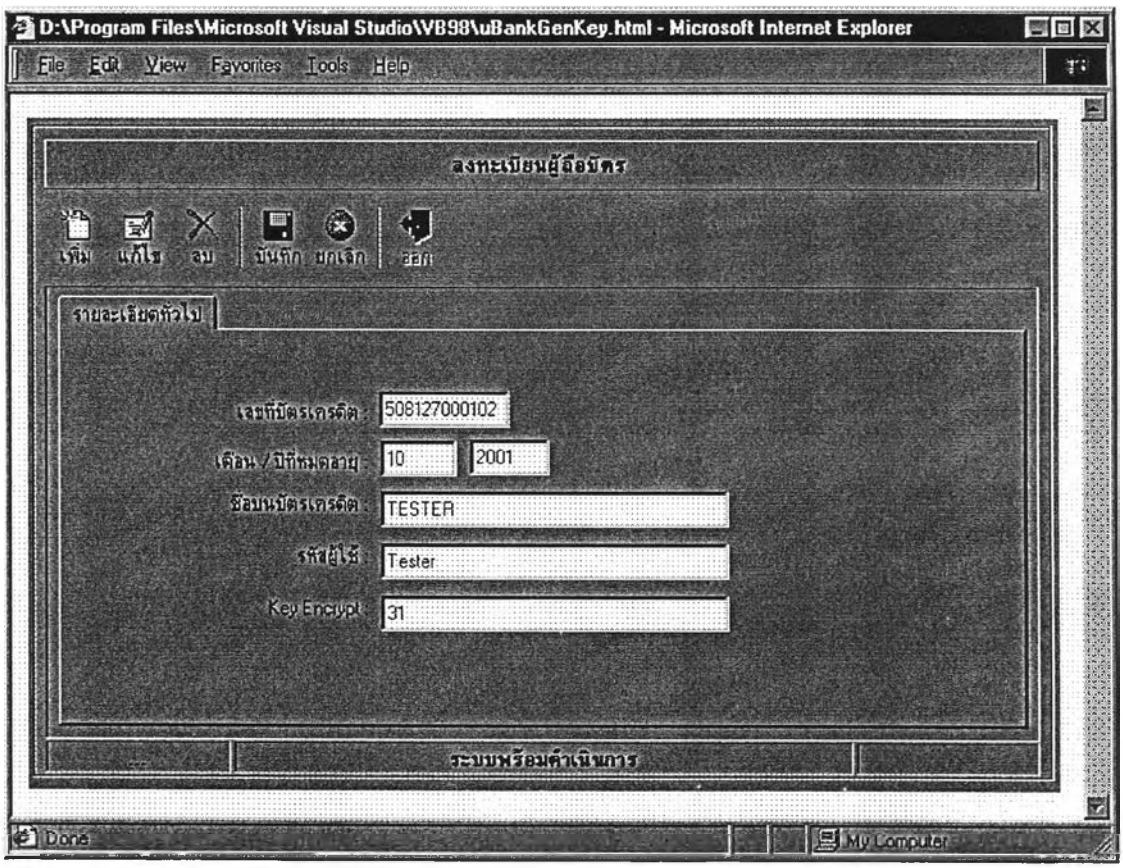
บทที่ 4
ผลการทดลอง

ผลการทดลอง

4.1 การลงทะเบียนสำหรับผู้ถือบัตร



รูปที่ 4.1 หน้าจอสำหรับการลงทะเบียนของผู้ถือบัตร

ผู้ถือบัตรสามารถเข้ามาลงทะเบียนเพื่อขอใช้บริการการชำระเงินด้วยบัตรเครดิตผ่านระบบการค้าอิเล็กทรอนิคส์ โดยระบุเลขที่บัตรเครดิต , เดือน / ปีที่บัตรหมดอายุ , ชื่อที่ปรากฏบนหน้าบัตร และรหัสผู้ใช้ที่ต้องการ

หน้าที่หลักของหน้าจอนี้

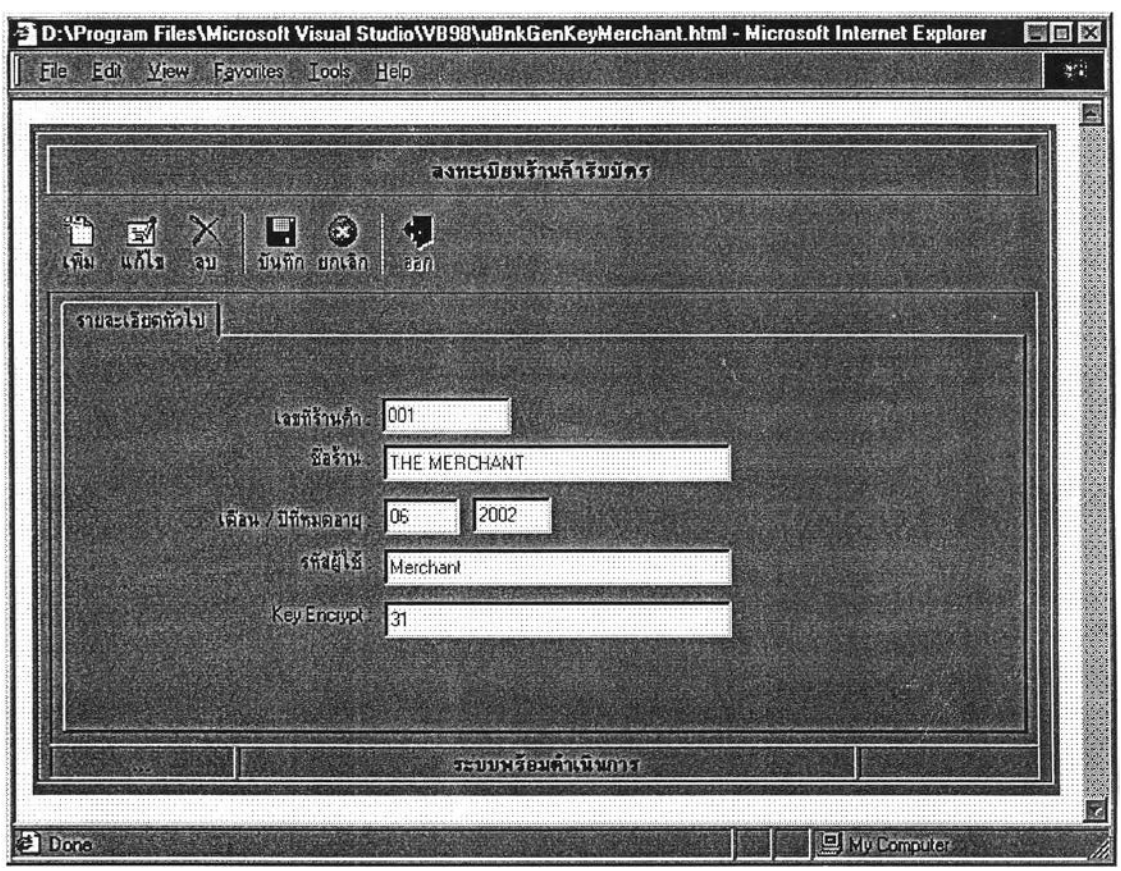
1. การตรวจสอบว่าผู้ลงทะเบียนเป็นผู้ถือบัตรเครดิตตัวจริง (Authentication)
   การตรวจสอบนั้นสามารถตรวจสอบได้จาก ข้อมูล 3 อย่างคือ
   - เลขที่บัตรเครดิต (Credit Card Number)
   - วันที่บัตรหมดอายุ (Expire Date)

- ชื่อผู้ถือบัตรที่ปรากฏอยู่บนบัตร (Name on Card)

ซึ่งข้อมูลทั้ง 3 อย่าง จะปรากฏอยู่บนบัตรเครดิต ถ้าผู้ลงทะเบียน กรอกข้อมูลทั้ง 3 ส่วน ได้ถูกต้องก็แสดงว่าเป็นผู้ถือบัตรตัวจริง

2. การตรวจสอบ User ที่ผู้ลงทะเบียนกำหนดว่ามีผู้ใช้แล้วหรือไม่
   ถ้ามีการกำหนดซ้ำ จะบอกไม่ได้ว่า จะใช้ Key ใดในการ Decrypt
3. การตรวจสอบกุญแจสำหรับการเข้ารหัส (Key Encryption) ว่าใช้ได้หรือไม่
   ในการเข้ารหัส แบบ RSA Security นั้น การกำหนด Key สำหรับการ Encrypt จะต้องเป็นตัวเลขที่ Relative Prime กับ (P-1)(Q-1) ซึ่งถ้า Key ที่ผู้ลงทะเบียนกำหนด ไม่เป็น Relative Prime แล้ว Key นั้นจะไม่สามารถนำมาใช้ได้
4. การสร้างรหัส (Generate Key Pair) สำหรับการถอดรหัส (Decrypt) เพื่อใช้ยืนยันตัวตนของผู้ถือบัตร

4.2 การลงทะเบียนสำหรับร้านค้ารับบัตร



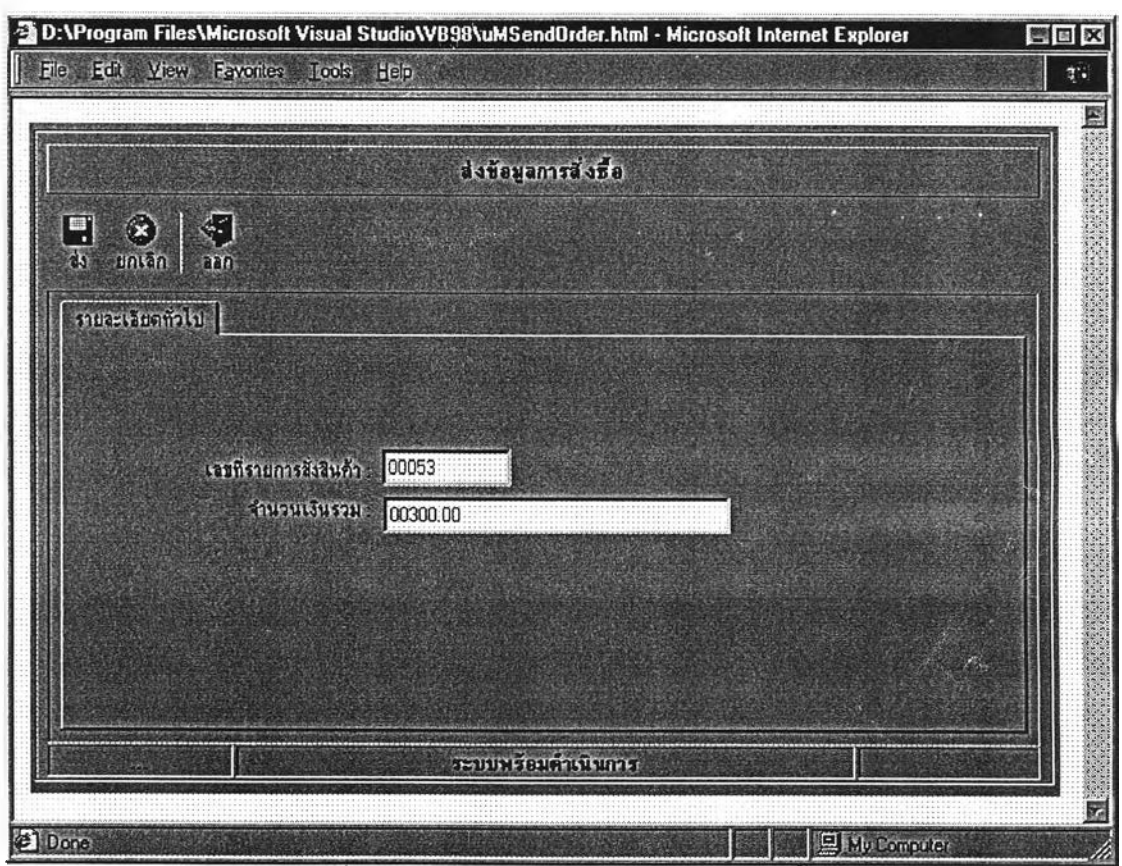
รูปที่ 4.2 หน้าจอสำหรับการลงทะเบียนของร้านค้ารับบัตร

ร้านค้ารับบัตรสามารถเข้ามาลงทะเบียนเพื่อขอใช้บริการการชำระเงินด้วยบัตรเครดิตผ่านระบบการค้าอิเล็กทรอนิคส์ โดยระบุชื่อร้านค้า เมื่อทำการบันทึกข้อมูล จะมีการสร้างเลขที่ร้านค้า , เดือน / ปีที่หมดอายุ และ รหัสเก็บไว้ในฐานข้อมูลของบริษัทผู้ออกบัตร เพื่อใช้ในการตรวจสอบตัวตนของร้านค้ารับบัตรต่อไป

หน้าที่หลักของหน้าจอนี้

1. การตรวจสอบว่าผู้ลงทะเบียนเป็นผู้ถือบัตรเครดิตตัวจริง (Authentication) การตรวจสอบนั้นสามารถตรวจสอบได้จาก
   - ชื่อร้านค้ารับบัตร
2. การตรวจสอบ User ที่ผู้ลงทะเบียนกำหนดว่ามีผู้ใช้แล้วหรือไม่ ถ้ามีการกำหนดซ้ำ จะบอกไม่ได้ว่า จะใช้ Key ใดในการ Decrypt
3. การตรวจสอบกุญแจสำหรับการเข้ารหัส (Key Encryption) ว่าใช้ได้หรือไม่
4. การสร้างรหัส (Generate Key Pair) สำหรับการถอดรหัส (Decrypt) เพื่อใช้ยืนยันตัวตนของร้านค้ารับบัตร

4.3 การส่งข้อมูลสั่งซื้อ



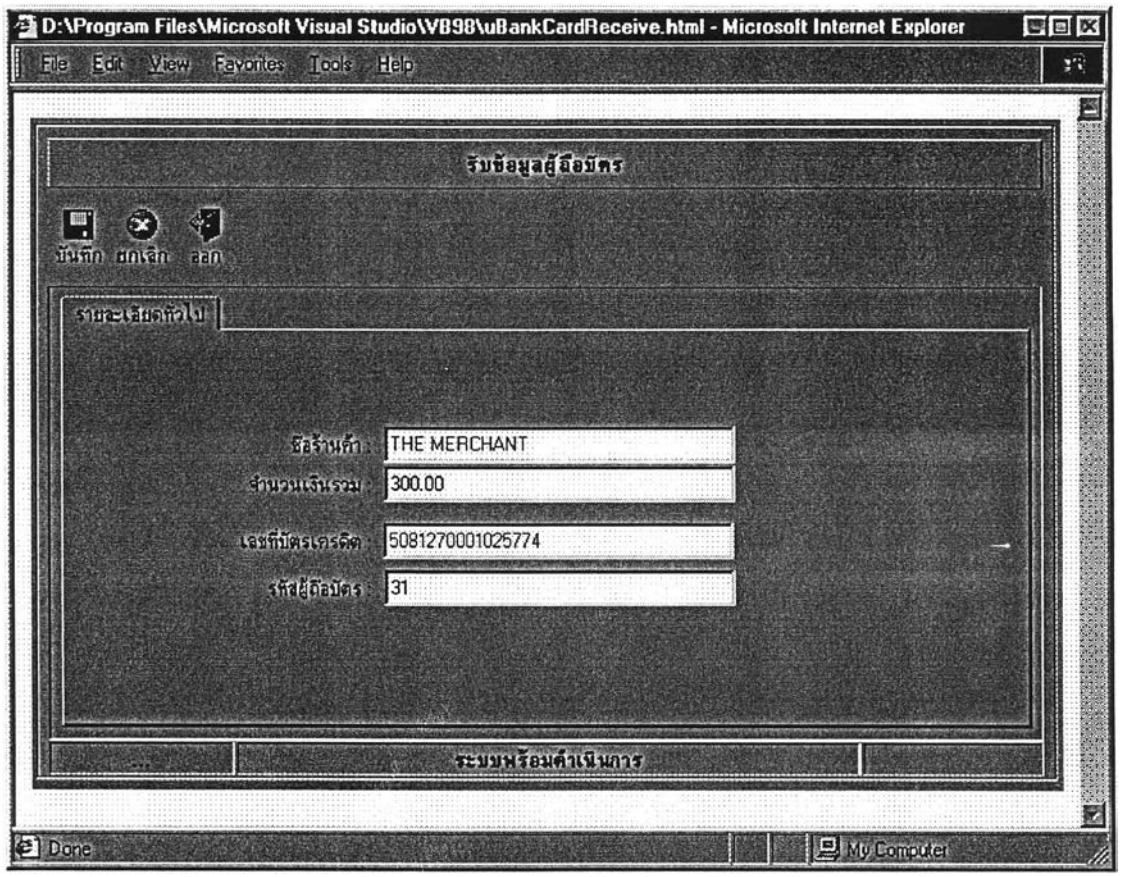
รูปที่ 4.3 หน้าจอสำหรับการส่งข้อมูลการสั่งซื้อ

ร้านค้ารับบัตรจะสร้างหน้าจอการรับรายการซื้อสินค้า เมื่อผู้ซื้อเลือกการชำระเงินด้วยบัตรเครดิตแบบขอให้มีการตรวจสอบตัวตน (ร้านค้ารับบัตรและผู้ถือบัตร) ร้านค้ารับบัตรจะต้องส่งรหัสของร้านค้ารับบัตร พร้อมด้วยรหัสร้านค้า , เลขที่ของการสั่งซื้อและจำนวนเงินรวม ไปยังบริษัทผู้ออกบัตร เพื่อทำการตรวจสอบตัวตนร้านค้ารับบัตร หากร้านค้ารับบัตรเป็นร้านที่มีสิทธิทำรายการ คือเป็นร้านที่ได้ลงทะเบียนไว้แล้ว บริษัทผู้ออกบัตรจะเปิดหน้าจอให้ผู้ถือบัตรบันทึกข้อมูลการชำระเงินต่อไป

หน้าที่หลักของหน้าจอนี้

1. เมื่อลูกค้าเข้ามาในร้าน หรือ เข้ามาที่ Web Site ของร้านค้า ร้านค้าจะต้องกำหนดเลขที่การสั่งซื้อสำหรับการซื้อขายครั้งนั้น เพื่อนำไปใช้ในการเข้ารหัสข้อมูล
   การกำหนดเลขที่การสั่งซื้อกำหนดโดย
   1.1 รหัสร้านค้า
   1.2 เลขที่การสั่งซื้อ
   1.3 จำนวนเงินรวมทั้งหมด
   รหัสร้านค้า คือ รหัสที่ใช้บอกว่าเป็นการซื้อสินค้าจากร้านไหน เช่น 001 เป็นต้น
   เลขที่การสั่งซื้อ คือ รหัสบอกว่ารายการซื้อสินค้าลำดับใด เช่น 00053 เป็นต้น
   จำนวนเงินรวมที่ลูกค้าซื้อในครั้งนั้น เช่น เงิน 300 บาท จะได้ 00300.00 เป็นต้น
   นำตัวเลขทั้ง 3 มาต่อกัน เป็นข้อมูลการสั่งซื้อครั้งนั้น เช่น
   Order ID : 0010005300300.00
2. การถอดรหัสข้อมูล
   หลังจากที่ธนาคารหรือบริษัทบัตรเครดิตได้ข้อมูลจากร้านค้า ซึ่งประกอบด้วย รหัสร้านค้า และ Cipher Text ธนาคารหรือบริษัทบัตรเครดิตจะใช้รหัสร้านค้าที่ได้ไปค้นหาในฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต เพื่อหากุญแจสำหรับการถอดรหัส (Key Decrypt) เพื่อใช้ถอดรหัส Cipher Text ซึ่งวิธีการจะทำย้อนกลับกับ การเข้ารหัสแต่จะใช้กุญแจสำหรับการถอดรหัส (Key Decrypt) ที่เข้ากับรหัสร้านค้าที่ร้านค้าส่งมา และได้กลับมาเป็น Plain Text ธนาคารหรือบริษัทบัตรเครดิตแยกข้อมูลรหัสร้านค้า เลขที่การสั่งซื้อ และจำนวนเงิน
3. การตรวจสอบความถูกต้องของข้อมูล

4.4 การบันทึกข้อมูลทางการเงินของผู้ถือบัตร



รูปที่ 4.4 หน้าจอสำหรับการบันทึกข้อมูลทางการเงินของผู้ถือบัตร

เมื่อร้านค้ารับบัตรได้รับการตรวจสอบตัวตนแล้ว ผู้ถือบัตรจะได้รับหน้าจอตามภาพ 4.4 จากบริษัทผู้ออกบัตร เพื่อขอให้บันทึกข้อมูลทางการเงิน โดยผู้ถือบัตรจะต้องตรวจสอบชื่อร้านค้าและจำนวนเงินรวมว่าเป็นข้อมูลที่ถูกต้องตามที่ผู้ถือบัตรได้สั่งสินค้า จึงจะบันทึกข้อมูลเลขที่บัตรเครดิตและรหัสของผู้ถือบัตรลงไป

จากการทดลอง

1. ในการเข้ารหัสข้อมูลนั้นจะใช้ข้อมูล 2 ข้อมูลคือ

   1.1 Order ID 16 หลัก คือ 0010005300300.00

   1.2 Credit Card Number 16 หลัก คือ 5081270001025774

   ข้อมูลทั้ง 2 รายการจะถูกแปลงเป็น Cipher Text ส่งให้บริษัทผู้ออกบัตร

2. การถอดรหัสข้อมูล

   หลังจากที่ธนาคารหรือบริษัทบัตรเครดิตได้ข้อมูลจากร้านค้าซึ่งประกอบด้วย รหัสร้านค้า และ Cipher Text ธนาคารหรือบริษัทบัตรเครดิตจะใช้รหัสร้านค้าที่ได้ไปค้นหาใน

ฐานข้อมูลของธนาคารหรือบริษัทบัตรเครดิต เพื่อหากุญแจสำหรับการถอดรหัส (Key Decrypt) เพื่อใช้ถอดรหัส Cipher Text ซึ่งวิธีการจะทำย้อนกลับกับ การเข้ารหัสแต่จะใช้กุญแจสำหรับการถอดรหัส (Key Decrypt) ที่เข้ากับรหัสร้านค้าที่ร้านค้าส่งมาและได้กลับมาเป็น Plain Text ธนาคารหรือบริษัทบัตรเครดิตแยกข้อมูลรหัสร้านค้า เลขที่การสั่งซื้อ และจำนวนเงิน

3. การตรวจสอบความถูกต้องของข้อมูล

   หลังจาก Decrypt ข้อมูล Cipher Text ออกมาเป็นช่วงข้อมูลต่างได้แล้ว ข้อมูลที่ธนาคารต้องตรวจสอบคือ

   3.1 เลขที่บัตรเครดิต (Credit Card Number)

   ตรวจสอบในฐานข้อมูลว่าเลขที่บัตรเครดิตมีจริงหรือไม่

   3.2 ตรวจสอบการซ้ำของรายการสั่งซื้อ (Transaction)

   ธนาคารสามารถตรวจสอบได้จากฐานข้อมูล โดยค้นหารหัสร้านค้าและเลขที่การสั่งซื้อ

4.5 การวิเคราะห์ผลการวิจัยในประเด็นอื่น ๆ ดังนี้

1. การเปรียบเทียบระบบที่ทำการทดลองกับระบบที่ใช้ในเชิงพาณิชย์ในปัจจุบัน ซึ่งในที่นี้เลือกเปรียบเทียบกับ SET

2. การวิเคราะห์จุดอ่อนทางด้านความปลอดภัยของระบบที่ทำการทดลอง

1. การเปรียบเทียบระบบที่ทำการทดลองกับระบบที่ใช้ในเชิงพาณิชย์ในปัจจุบัน สรุปในรูปของตาราง ตามตารางที่ 4.1 ดังนี้

ตารางที่ 4.1 ตารางสรุปข้อเปรียบเทียบระหว่างระบบที่ทำการทดลองกับ SET

หัวข้อที่ทำการเปรียบเทียบ	ลักษณะที่แตกต่างของแต่ละโพรโตคอล	
	ระบบที่ทดลอง	SET
จำนวนฝ่ายที่เกี่ยวข้อง	3 ฝ่าย (ผู้ซื้อ ผู้ขาย และธนาคาร)	3 ฝ่าย (ผู้ซื้อ ผู้ขาย และธนาคาร)
ใบรับรองดิจิตอล	-	ทุกฝ่ายที่เกี่ยวข้องต้องมี
การตรวจสอบ	บริษัทผู้ออกบัตรเป็นตัวกลางการตรวจสอบผู้ถือบัตรและร้านค้ารับบัตร	ต้องมี CA ตรวจสอบทุกฝ่ายที่เกี่ยวข้อง
การป้อนข้อมูลบัตรเครดิต	ผู้ซื้อต้องป้อนทุกครั้ง โดยป้อนที่หน้าจอของคนกลาง จึงทำรายการจากเครื่องคอมพิวเตอร์เครื่องใด ๆ ก็ได้	ข้อมูลบัตรฯ ถูกเก็บไว้ใน E-Wallet จึงป้อนเก็บไว้เพียงครั้งเดียว แต่จะต้องป้อนที่เครื่องคอมพิวเตอร์ที่มี E-Wallet เท่านั้น
การจำกัดการเข้าถึง	-ธนาคารผู้ออกบัตรฯไม่ทราบรายละเอียดการซื้อ รักษาความเป็นส่วนตัวของลูกค้า -ผู้ขายไม่ทราบข้อมูลบัตรเครดิตลูกค้า รักษาความปลอดภัย	-ธนาคารผู้ออกบัตรฯไม่ทราบรายละเอียดการซื้อ รักษาความเป็นส่วนตัวของลูกค้า -ผู้ขายไม่ทราบข้อมูลบัตรเครดิตลูกค้า รักษาความปลอดภัย
การใช้ข้อมูลร่วมกัน	- ป้องกันบุคคลที่ 3 ไม่ให้เข้าถึงข้อมูลได้ - ข้อมูลบัตรเครดิตถูกส่งให้บริษัทผู้ออกบัตรเครดิต บริษัทผู้ออกบัตรเครดิตไม่ทราบรายละเอียดรายการซื้อขาย - ร้านค้ารับบัตรไม่ทราบเลขที่บัตรเครดิตของผู้ถือบัตร	คำสั่งซื้อที่เข้ารหัสแล้วถูกส่งให้ผู้ขาย ส่วนข้อมูลบัตรเครดิตที่เข้ารหัสแล้วถูกส่งให้ธนาคารผู้ออกบัตรเครดิต
การพิสูจน์ตัวตนของลูกค้าและยอดเครดิตแบบทันที	สนับสนุน	สนับสนุน

หัวข้อที่ทำการเปรียบเทียบ	ลักษณะที่แตกต่างของแต่ละโพรโตคอล	
	ระบบที่ทดลอง	SET
การเข้ารหัสข้อมูลบัตรเครดิต	เข้ารหัสรายละเอียดคำสั่งซื้อกับข้อมูลบัตรรวมกัน จึงมีความแข็งแรงน้อยกว่า	เข้ารหัสคำสั่งซื้อกับข้อมูลบัตรฯ แยกจากกัน และเนื่องจากข้อมูลบัตรฯ มีขนาดตายตัว จึงสามารถเข้ารหัสได้แข็งแรงกว่า
การทำงาน	ผู้ขายหรือร้านค้ารับบัตรจะถูกตรวจสอบตัวตนก่อนว่าเป็นผู้มีสิทธิทำรายการกับบริษัทผู้ออกบัตรหรือไม่ ถ้ามีผู้ซื้อจึงจะได้รับหน้าจอเพื่อทำการบันทึกข้อมูลทางการเงิน ข้อมูลทางการเงินจะถูกเข้ารหัสเช่นกัน และส่งไปยังบริษัทผู้ออกบัตรเพื่อตรวจสอบตัวตนของผู้ถือบัตร บริษัทผู้ออกบัตรฯจะถอดรหัสข้อมูลที่ได้รับจากผู้ซื้อ โดยใช้กุญแจสาธารณะของผู้ซื้อ ทำให้บริษัทผู้ออกบัตรกลายเป็นตัวกลางสำหรับการตรวจสอบตัวตนของคู่ค้าทั้ง 2 ฝ่าย การตรวจสอบการอนุมัติวงเงินกับธนาคารผู้ออกบัตรฯ ไม่รวมอยู่ในระบบนี้	คำสั่งซื้อของลูกค้าจะถูกเข้ารหัสโดยใช้กุญแจส่วนตัวของผู้ซื้อก่อนส่งไปยังผู้ขาย ส่วนข้อมูลบัตรเครดิตจะถูกเข้ารหัสเช่นกันก่อนส่งไปยังธนาคารของผู้ขาย โดยมีการเซ็นลายเซ็นดิจิตอลกำกับข้อมูลที่เข้ารหัสแล้วทั้ง 2 ส่วน ผู้ขายและธนาคารผู้ออกบัตรฯจะถอดรหัสข้อมูลที่ได้รับจากผู้ซื้อ โดยใช้กุญแจสาธารณะของผู้ซื้อ ทำให้ทุกฝ่ายสามารถตรวจสอบตัวตนของอีกฝ่ายหนึ่งได้ก่อนที่ผู้ขายจะยอมรับคำสั่งซื้อ ธนาคารของผู้ขายจะตรวจสอบการอนุมัติวงเงินกับธนาคารผู้ออกบัตรฯ หากได้รับการอนุมัติธนาคารของผู้ขายจะจ่ายเงินเข้าบัญชีของผู้ขาย ส่วนธนาคารผู้ออกบัตรฯ จะบันทึกรายการบัตรฯ เพื่อเรียกเก็บเงินจากผู้ซื้อต่อไป
ข้อเสีย	• เนื่องจากข้อกำหนดของกระทรวงการต่างประเทศของสหรัฐฯ ซึ่งกำหนดให้ใช้กุญแจที่มีความยาวเพียง 40 บิต ในการส่งข้อมูลระหว่างประเทศ และ 128 บิต สำหรับการส่งข้อมูลภายในประเทศ ทำให้เกิดความไม่แข็งแรงของการเข้ารหัส • ความปลอดภัยในแง่ของ Application อาจไม่มากพอ เครื่องคอมพิวเตอร์ที่มีประสิทธิภาพมากขึ้นในทุกวันจะใช้เวลาไม่มากในการค้นหารหัส อาจต้องใช้วิธีการอื่นช่วยให้ระบบมีประสิทธิภาพมากขึ้น เช่น SSL หรือ Firewalls	• ยังมีปัญหาความเข้ากันได้ของระบบ SET จากผู้ผลิตที่ต่างกัน • ระบบสำหรับผู้ขายและธนาคารมีราคาสูงผู้ขายส่วนมากจึงยอมที่จะรับความเสี่ยงบน SSL ซึ่งมีสัดส่วนเพียงเล็กน้อย ผู้ซื้อจะต้องเสียค่าใช้จ่ายเพื่อให้ได้มาซึ่งใบรับรองดิจิตอลทำให้มีผู้ใช้น้อย
ข้อดี	• ราคาถูก	• ความร่วมมือของบริษัทชั้นนำหลายแห่งทำให้ระบบมีประสิทธิภาพ เป็นที่ยอมรับในความปลอดภัย

2. การวิเคราะห์จุดอ่อนทางด้านความปลอดภัยของระบบที่ทำการทดลอง

พิจารณาจากภาพรวมของระบบ (รูปที่ 3.4) ที่ทำการทดลองแล้วใช้กรณีตัวอย่างเพื่อทดสอบระบบ ดังนี้

2.1 การปลอมเป็นร้านค้ารับบัตร

2.2 การปลอมเป็นผู้ถือบัตร

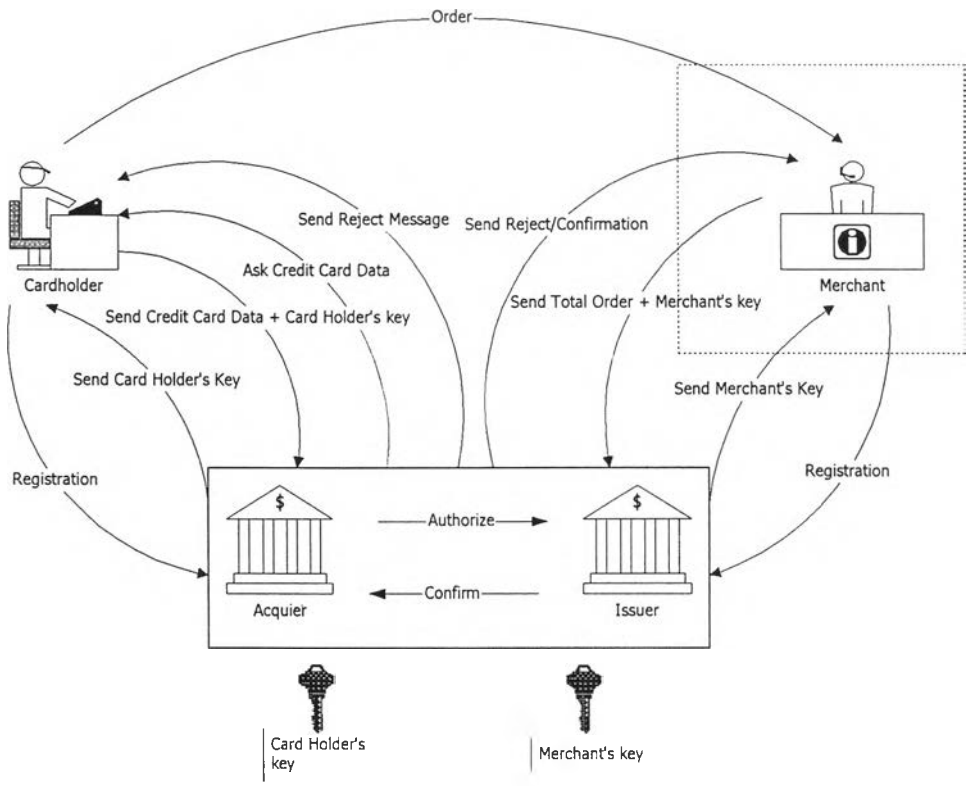
2.3 การปลอมเป็นร้านค้ารับบัตร และการปลอมเป็นผู้ถือบัตร

2.4 การปลอมเป็นบริษัทผู้ออกบัตร

2.5 การปลอมเป็นร้านค้า และการปลอมเป็นบริษัทผู้ออกบัตร

2.6 การส่งรายการที่ไม่เป็นความจริงจากร้านค้ารับบัตร

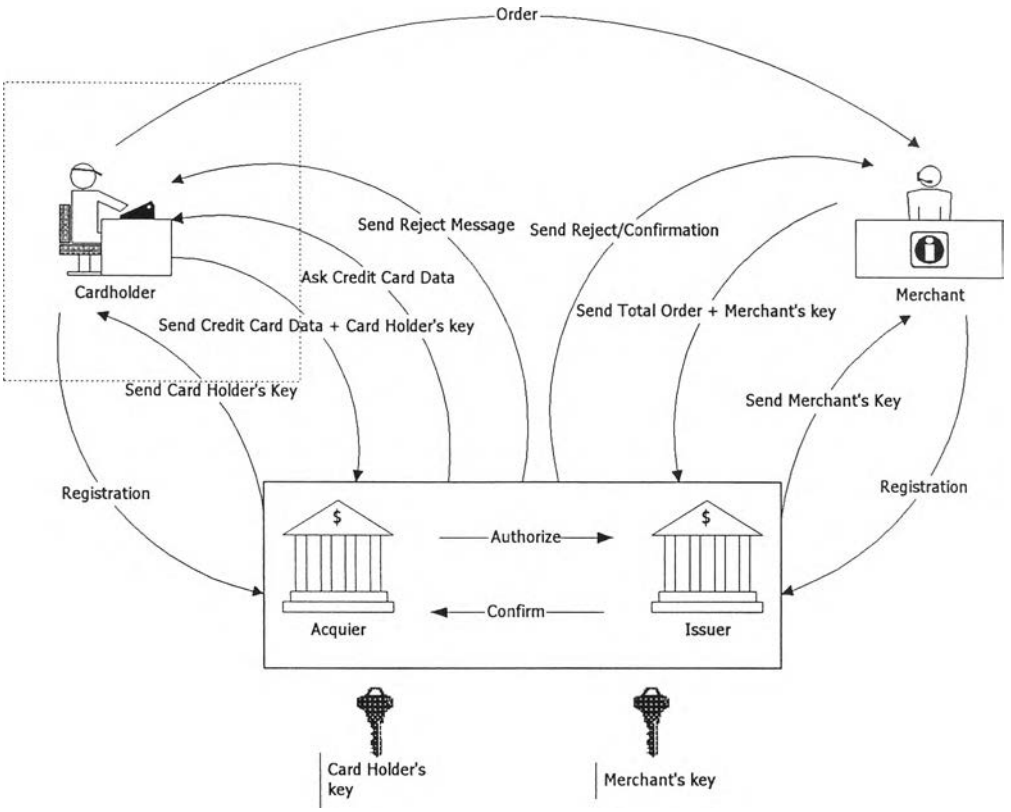
2.1 การปลอมเป็นร้านค้ารับบัตร



รูป 4.5 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นร้านค้ารับบัตร

ในกรณีที่เกิดการปลอมเป็นร้านค้ารับบัตรด้วยวิธีการ Spoofing หรือเป็นร้านค้ารับบัตรที่ไม่ได้ลงทะเบียน ผู้ซื้อซึ่งเป็นผู้ถือบัตรจะไม่เกิดความเสียหายเนื่องจากบริษัทผู้ออกบัตรซึ่งทำหน้าที่คนกลางจะมีการตรวจสอบตัวตนของร้านค้ารับบัตร และการบันทึกข้อมูลบัตรเครดิตนั้น ให้ทำที่หน้าจอของบริษัทผู้ออกบัตรหรือคนกลาง

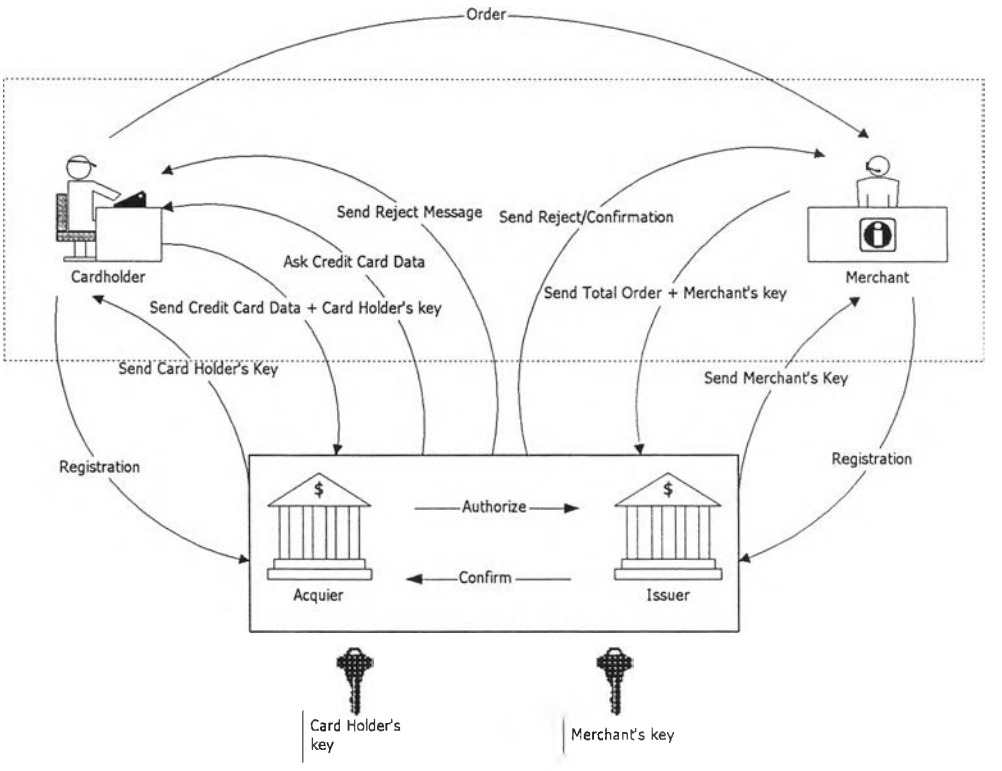
2.2 การปลอมเป็นผู้ถือบัตร



รูป 4.6 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นผู้ถือบัตร

ในกรณีที่เกิดการปลอมเป็นผู้ถือบัตร ด้วยวิธีการ Spoofing ผู้ขายจะไม่เกิดความเสียหาย เนื่องจากบริษัทผู้ออกบัตร ซึ่งทำหน้าที่คนกลางจะมีการตรวจสอบตัวตนของผู้ถือบัตรหลังจากรับข้อมูลบัตรเครดิต ถ้าไม่ถูกต้องจะส่งข้อความแจ้งผู้ขายเพื่อให้ร้านค้ารับบัตรทราบว่าบริษัทผู้ออกบัตรหรือคนกลางไม่รับรองผู้ซื้อในการซื้อขายครั้งนี้

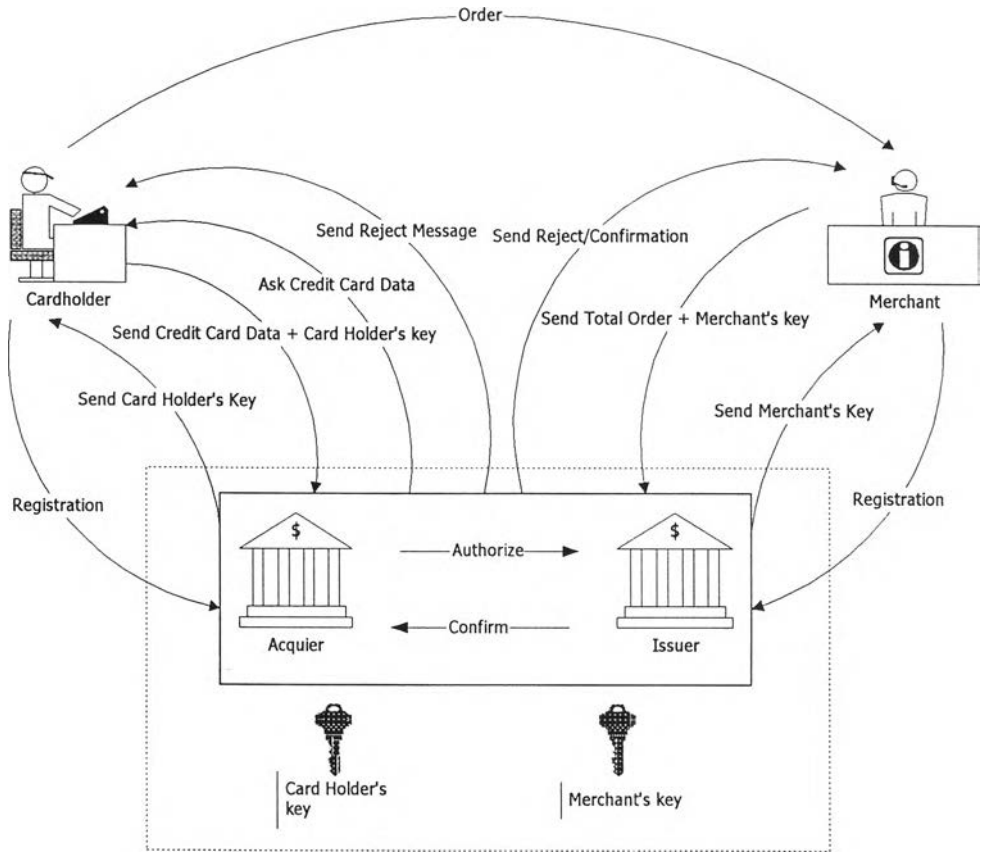
2.3 การปลอมเป็นร้านค้า และการปลอมเป็นผู้ถือบัตร



รูป 4.7 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นร้านค้า และการปลอมเป็นผู้ถือบัตร

ในกรณีที่เกิดการปลอมเป็นร้านค้า และการปลอมเป็นผู้ถือบัตร ด้วยวิธีการ Spoofing ต้องเป็นความร่วมมือของร้านค้ารับบัตรและผู้ถือบัตร ซึ่งอาจเป็นบุคคลคนเดียวกันหรือไม่ก็ได้ ความเสียหายต่อบริษัทผู้ออกบัตรหรือคนกลาง ขึ้นกับว่าการตัดบัญชีเกิดขึ้นในทันทีที่เกิดรายการค้าหรือไม่ และระบบภายในเองมีขั้นตอนในการตรวจสอบรายการค้าประจำวันอย่างไร แต่ทั้งนี้ความเสียหายจะไม่เกินกว่าวงเงินที่บัตรเครดิตนั้น ๆ มี

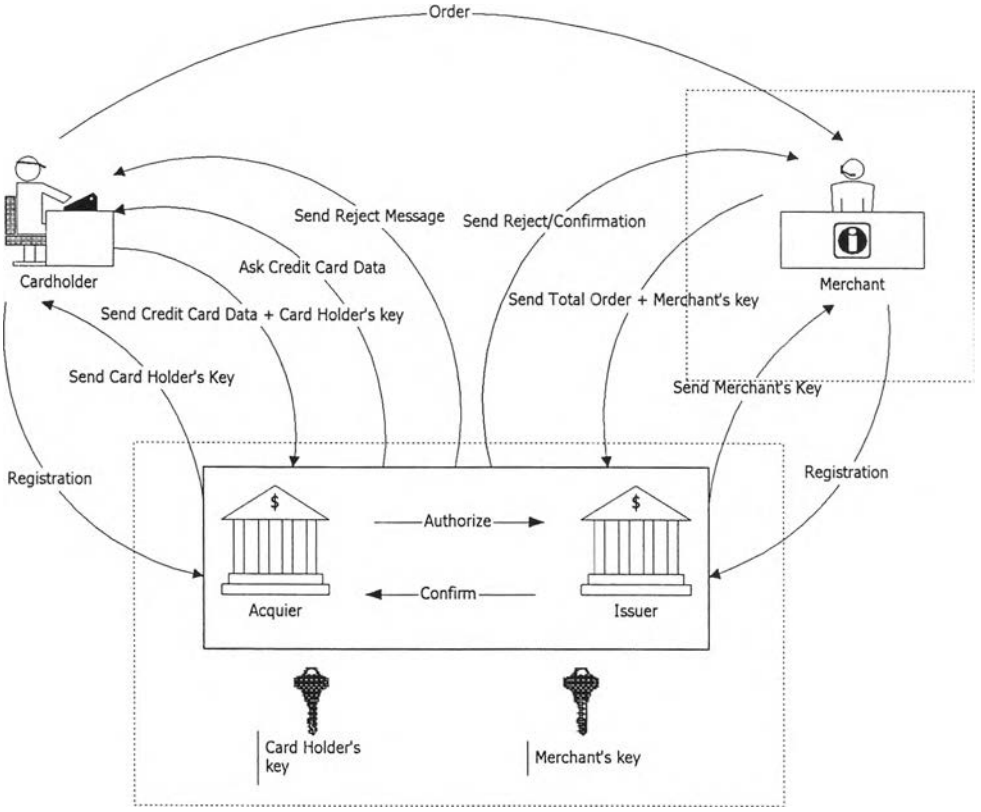
2.4 การปลอมเป็นบริษัทผู้ออกบัตร



รูป 4.8 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นบริษัทผู้ออกบัตร

ในกรณีที่เกิดการปลอมเป็นบริษัทผู้ออกบัตร ด้วยวิธีการ Spoofing ผู้ปลอมแปลงจะได้รับรหัสของร้านค้ารับบัตรและข้อมูลรวมของการสั่งซื้อแต่จะไม่สามารถอ่านรายการและทำรายการต่อได้

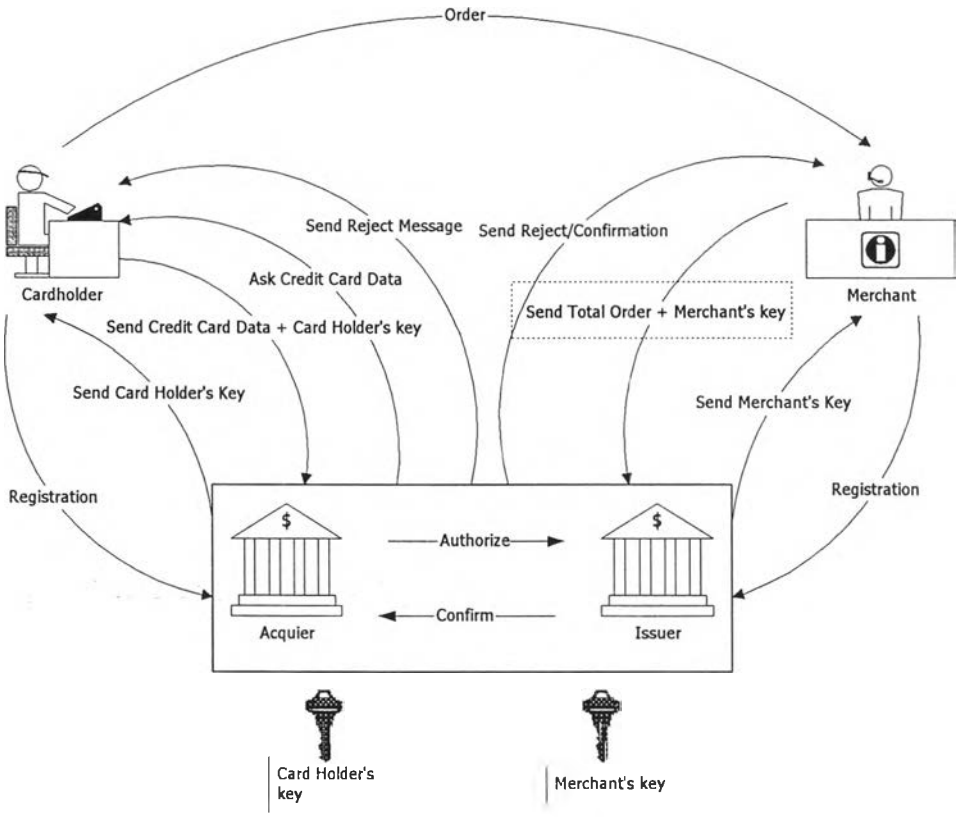
2.5 การปลอมเป็นร้านค้า และการปลอมเป็นบริษัทผู้ออกบัตร



รูป 4.9 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นร้านค้า และการปลอมเป็นบริษัทผู้ออกบัตร

ในกรณีที่เกิดการปลอมเป็นร้านค้า และการปลอมเป็นบริษัทผู้ออกบัตร ด้วยวิธีการ Spoofing ผู้ปลอมแปลงจะได้รับรหัสของลูกค้าและข้อมูลบัตรเครดิตไป สามารถไปทำรายการหลอกบริษัทรับบัตรได้

2.6 การส่งรายการที่ไม่ถูกต้องจากร้านค้ารับบัตรที่ลงทะเบียนอย่างถูกต้อง



รูป 4.10 ระบบที่ทำการทดลองเมื่อมีการส่งรายการที่ไม่ถูกต้องจากร้านค้ารับบัตรที่ลงทะเบียนอย่างถูกต้อง

ในกรณีที่เกิดการส่งรายการที่ไม่ถูกต้องจากร้านค้ารับบัตรที่ลงทะเบียนอย่างถูกต้อง ความเสียหายจะไม่เกิดขึ้น เนื่องจากก่อนผู้ถือบัตรจะบันทึกข้อมูลเกี่ยวกับบัตรเครดิต ผู้ถือบัตรจะเห็นยอดรวมเงินก่อน ถ้ายอดถูกต้องผู้ถือบัตรจึงจะบันทึกข้อมูลเกี่ยวกับบัตรเครดิตลงไป