การออกแบบโพรโทคอลความมั่นคงปลอดภัยในการชำระเงินผ่านอุปกรณ์สื่อสารไร้สายที่มีการพิสูจน์ทราบตัวตนสองทาง

Designing Secure Mobile Payment Protocol with Mutual Authentication

สุรการ ดวงผาสุข และ ชาลี ธรรมรัตน์

คณะวิทยาการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยเทคโนโลยีมหานคร

51 หมู่1 ถนนเชื่อมสัมพันธ์แขวงกระทุ่มรายเขตหนองจอกกรุงเทพ 10530

Emails: surakarn@mut.ac.th และ chalee23@gmail.com

ABSTRACT – In current time, the transaction protocol over the wireless network has been very popular. Many researchers presented a payment protocol for goods or services. However, the research papers presented still lack of security features such as mutual authentication. The performance of the protocol is dropping due to a lot of messages sending in the network. This research proposed a new protocol and security features to solve the existing research in case of confidentiality, integrity, non-repudiation, and mutual authentication. The proposed protocol has a number of messages less than existing protocols so the proposed protocol takes less time to complete transaction. Moreover, this paper also utilizes hybrid encryption between asymmetric encryption and symmetric encryption with hash function to ensure the security of the system.
KEYWORDS -- Security Protocol, Payment Protocol, Mutual authentication, Cryptography Protocol, Mobile Payment

บทคัดย่อ – ปัจจุบันการทำธุรกรรมผ่านเครือข่ายไร้สายได้รับความนิยมเป็นอย่างมากเช่น การชำระค่าสินค้าหรือบริการ มีงานวิจัยจำนวนมากนำเสนอโพรโทคอลการชำระเงินค่าสินค้าหรือบริการ แต่อย่างไรก็ตามงานวิจัยที่นำเสนอเหล่านั้นยังขาดความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวตนสองทางและจำนวนข้อความที่มีจำนวนมากในการจบการทำงานของโพรโทคอล ส่งผลทำให้ประสิทธิภาพของโพรโทคอลดลงเพราะใช้เวลาเพิ่มขึ้น ดังนั้นงานวิจัยนี้จึงได้นำเสนอโพรโทคอลใหม่เพื่อแก้ปัญหางานวิจัยที่มีอยู่และมีคุณสมบัติความมั่นคงปลอดภัยเช่น การรักษาความลับของข้อมูล ความคงสภาพของข้อมูล การห้ามปฏิเสธความรับผิดชอบและการพิสูจน์ทราบตัวตนสองทาง โพรโทคอลที่นำเสนอข้อความที่มีจำนวนน้อยในการจบการทำงานของโพรโทคอล ส่งผลทำให้มีประสิทธิภาพและใช้เวลาน้อยกว่าโพรโทคอลที่มีอยู่ นอกจากนี้งานวิจัยที่นำเสนอใช้การเข้ารหัสลับแบบอสมมาตรและสมมาตร พร้อมทั้งฟังก์ชันแฮชเพื่อเพิ่มความมั่นคงปลอดภัยเพิ่มขึ้น
คำสำคัญ --โพรโทคอลความมั่นคงปลอดภัย, โพรโทคอลการชำระเงิน, การพิสูจน์ทราบตัวตนสองทาง, โพรโทคอลการเข้ารหัสลับ, การชำระเงินเครือข่ายสื่อสารไร้สาย

1. บทนำ

อุปกรณ์สื่อสารไร้สายปัจจุบันสนับสนุนการสื่อสารแบบ 3G และ 4G ทำให้การสื่อสารไร้สายรวดเร็วขึ้นกว่าในอดีต จึงทำให้มีแอพพลิเคชันที่เกี่ยวกับการชำระเงินผ่านอุปกรณ์สื่อสารไร้สายจำนวนมากถูกพัฒนาขึ้นมาใช้งาน ขณะที่ผู้ใช้งานสามารถชำระเงินได้ทุกที่ทุกเวลาและขณะเคลื่อนที่ได้

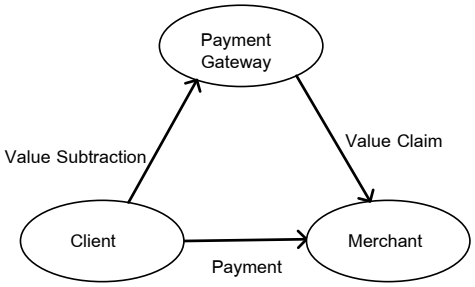
มีงานวิจัยจำนวนมากได้นำเสนอโพรโทคอลชำระค่าสินค้าหรือบริการผ่านอุปกรณ์สื่อสารไร้สาย แต่อย่างไรก็ตามงานวิจัยที่นำเสนอยังมีข้อด้อยเช่น การพิสูจน์ทราบตัวตนสองทาง ทำให้ผู้โจมตีสามารถปลอมเพื่อขโมยข้อมูลที่สำคัญ และจำนวนข้อความที่มีจำนวนมากจนทำให้ประสิทธิภาพโพรโทคอลลดลงเช่น เวลาที่ใช้การสิ้นสุดโพรโทคอลและทรัพยากรที่ใช้เพิ่มขึ้น

บทความวิจัยฉบับนี้มีโครงสร้างดังนี้ บทที่ 2 กล่าวถึงพื้นฐานงานที่เกี่ยวข้อง บทที่ 3 งานวิจัยที่นำเสนอ บทที่ 4 การวิเคราะห์และอภิปราย บทที่ 5 การวิเคราะห์ประสิทธิภาพของโพรโทคอล และบทที่ 6 สรุปผลการวิจัย

2. ทฤษฎีที่เกี่ยวข้อง

2.1 การชำระเงินค่าสินค้าหรือบริการ

การชำระเงินค่าสินค้าหรือบริการ [5, 10] โดยทั่วไปประกอบด้วย ลูกค้า (Customer) พ่อค้า (Merchant) ตัวกลางการชำระเงิน (Payment Gateway) สถาบันการเงินของลูกค้า (Issuer) และสถาบันการเงินของพ่อค้า (Acquirer) ซึ่งองค์ประกอบพื้นฐานของการทำธุรกรรมการชำระเงินเรียกว่า “Payment Gateway” ทำหน้าที่เป็นเสมือนตัวแทนการทำธุรกรรมระหว่างสถาบันการเงินของลูกค้าและพ่อค้า ซึ่งรูปแบบการทำธุรกรรมจะประกอบด้วย 3 ส่วนคือ คำสั่งชำระเงิน (Payment Request) การหักเงินจากบัญชี (Value Subtraction) และการเพิ่มเงินเข้าบัญชี (Value Claim) แสดงดังรูปที่ 1



รูปที่ 1 Primitive Transactions [5]

รายละเอียดของ Primitive Transactions มีดังต่อไปนี้

- Payment คือ การติดต่อซื้อขายสินค้าหรือบริการระหว่างลูกค้าและพ่อค้าซึ่ง Payment Request ลูกค้าจะเป็นผู้สั่งซื้อสินค้าหรือบริการและ Payment Response พ่อค้าจะเป็นผู้ส่งข้อความของใบเสร็จรับเงินให้แก่ลูกค้า
- Value Subtraction คือ การติดต่อระหว่างลูกค้าและสถาบันการเงินของลูกค้า (Payment Gateway) โดยลูกค้าส่งคำขอไปยังธนาคารของลูกค้าเพื่อทำการหักเงินจากบัญชีเรียกว่า Value-Subtraction Request ซึ่งธนาคารจะหักเงินในบัญชีของลูกค้าเมื่อได้รับข้อความเรียบร้อยและส่งคำยืนยัน Value-Subtraction Response กลับไปให้ลูกค้า
- Value Claim คือ การติดต่อระหว่างพ่อค้าและสถาบันการเงินของพ่อค้า (Payment Gateway) โดย Value-Claim Request พ่อค้าทำการร้องขอให้หักเงินจากบัญชีของลูกค้าที่สั่งซื้อสินค้าหรือบริการเข้าบัญชีของพ่อค้า แล้วส่งคำสั่งยืนยันการหักเงิน Value-Claim Response เมื่อได้รับการโอนเงินจากบัญชีของลูกค้า

2.2 งานวิจัยที่มีอยู่

2.2.1 A New Mobile Payment Protocol (GMPCP) By Using A New Key Agreement Protocol (GC)

Vahidalizadehdizaj *et al.* [7] ได้นำเสนอโพรโทคอลชำระค่าสินค้าหรือบริการผ่านอุปกรณ์สื่อสารไร้สาย โดยที่ลูกค้าเป็นศูนย์กลางในการชำระเงิน ได้นำวิทยาการเข้ารหัสลับแบบอสมมาตรและสมมาตร พร้อมทั้งฟังก์ชันแฮชมาใช้งาน นอกจากนี้โพรโทคอลยังมีคุณสมบัติความมั่นคงปลอดภัยเช่น ความเป็นส่วนตัวของแต่ละฝ่าย

2.2. 2. A New Mobile Payment Protocol (GMPCP) By Using A New Group Key Agreement Protocol (VTGKA)

Vahidalizadehdizaj *et al.* [8] ได้นำเสนอโพรโทคอลชำระค่าสินค้าหรือบริการผ่านอุปกรณ์สื่อสารไร้สายโดยที่ลูกค้าเป็นศูนย์กลางในการชำระเงิน ได้นำวิทยาการเข้ารหัสลับแบบอสมมาตรและสมมาตร รวมทั้งฟังก์ชันแฮชมาใช้งาน

2.2.3. A mobile payment mechanism with anonymity for cloud computing

YANG *et al.* [9] ได้นำเสนอโพรโทคอลชำระค่าสินค้าหรือบริการผ่านอุปกรณ์สื่อสารไร้สายที่เหมาะสมกับสภาพแวดล้อมบนคลาวด์ (Cloud) ได้นำวิทยาการเข้ารหัสลับแบบอสมมาตรและสมมาตร ตลอดจนฟังก์ชันแฮชมาใช้งาน นอกจากนี้โพรโทคอลยังมีคุณสมบัติความมั่นคงปลอดภัยเช่น ไม่ระบุตัวตนของแต่ละฝ่ายและการชำระเงินมีความยุติธรรม

2.3. การสร้างและกระจายเซสชันคีย์แบบออฟไลน์

Kungpisdan *et al.* [1] ได้นำเสนอวิธีการสร้างและกระจายคีย์แบบออฟไลน์ ซึ่งมีการสร้างและกระจายเซสชันคีย์โดยที่ไม่ต้องมีการส่งคีย์ดังกล่าวผ่านเครือข่าย [1] ซึ่งมีจุดเด่นที่เหนือกว่าเทคนิคการกระจายคีย์แบบออนไลน์ โดยเทคนิคการสร้างและกระจายคีย์แบบออฟไลน์ถูกเสนอ [2] [3] [4] [5] [6] โดยที่ Kungpisdan *et al.* ได้แนะนำเทคนิคการสร้างคีย์ที่ไม่เพียงแต่มีความปลอดภัยจากการโจมตีเท่านั้น แต่ยังสามารถทำงานได้แบบออฟไลน์ จากเทคนิคนี้จะเห็นว่าจะมีการส่งเพียงค่าตัวแปรที่เป็นค่าเริ่มต้นเพื่อนำไปใช้ในการสร้างคีย์และคีย์ที่ถูกสร้างขึ้นถูกนำมาใช้เพียงครั้งเดียวไม่มีการนำมาใช้ซ้ำและสามารถสร้างคีย์โดยโอกาสเกิดค่าคีย์ที่ซ้ำเป็นไปได้ยาก [1]

3. งานวิจัยที่นำเสนอ

หัวข้อนี้นำเสนอโพรโทคอลเพื่อแก้ไขปัญหาและข้อจำกัดของงานวิจัยที่มีอยู่ได้แก่ การพิสูจน์ทราบตัวตนสองทาง ความคงสภาพของข้อมูล การรักษาความลับของข้อมูล และการห้ามปฏิเสธความ รวมทั้งจำนวนข้อความที่มีจำนวนมากส่งผลทำให้โพรโทคอลมีประสิทธิภาพลดลง เช่น เวลาที่ใช้การสิ้นสุดโพรโทคอลและทรัพยากรที่ใช้งานเพิ่มขึ้น

3.1 นิยามและสมมติฐาน

จากข้อมูลในตารางที่ 1 แสดงสัญลักษณ์และรายละเอียดที่ใช้ในโพรโทคอลที่นำเสนอ

ตาราง 1. สัญลักษณ์และรายละเอียด

สัญลักษณ์	รายละเอียด
C	ลูกค้า ผู้ที่สั่งซื้อสินค้าหรือบริการจากพ่อค้า
M	พ่อค้า ผู้ที่ผู้ที่ขายสินค้าหรือบริการให้กับลูกค้า
PG	ตัวแทนการทำธุรกรรมระหว่างสถาบันการเงินของลูกค้าและพ่อค้า
I	สถาบันการเงินของลูกค้าซึ่งลูกค้าได้เปิดบัญชีไว้
A	สถาบันการเงินของพ่อค้าซึ่งพ่อค้าได้เปิดบัญชีไว้
$SK_{A\text{-}Bj}$	เซสชันคีย์ที่ใช้ร่วมกันระหว่าง A กับ B โดยที่ $j = 1$ ถึง m
ID_A	คือสิ่งที่ระบุว่าเป็น A
$\{m\}_{SKA\text{-}Bj}$	เป็นข้อความที่เข้ารหัสลับสมมาตรของข้อความ m ด้วยเซสชันคีย์ $SK_{A\text{-}Bj}$
$\{m\}_{Pri\text{-}A}$	เป็นข้อความที่เข้ารหัสลับแบบอสมมาตรของข้อความ m ด้วยกุญแจส่วนตัวของ A
$\{m\}_{Pub\text{-}A}$	เป็นข้อความที่เข้ารหัสลับแบบอสมมาตรของข้อความ m ด้วยกุญแจสาธารณะของ A
$h(m)$	คือค่าแฮชของข้อความ m
$h(m, SK_{A\text{-}Bj})$	เป็นรหัสพิสูจน์ทราบตัวตนข้อความ (MAC) ของข้อความ m ที่ใช้คีย์เซสชันคีย์ $SK_{A\text{-}Bj}$
OI	รายละเอียดการซื้อขายสินค้าหรือบริกการ เช่นTID, $Price$, OD และ T
TID	รหัสการซื้อขายสินค้าหรือบริกการ
$Price$	ราคารวมการซื้อขายสินค้าหรือบริกการ
OD	รายระเอียดสินค้าหรือบริกการ
T	วันเวลาขณะที่ร้องขอการชำระเงินค่าสินค้าหรือบริการ

สมมติฐานของโพรโทคอลที่นำเสนออธิบายได้ดังนี้

- *PG* จะต้องขอใบรับรองดิจิทัล (Digital Certificate) จากองค์กรที่น่าเชื่อถือ แล้วต่อจากนั้น *PG* ลงทะเบียนกับ *I* และ *A* เพื่อขอเป็นคนกลางในการชำระเงิน พร้อมทั้งทำการส่งกุญแจสาธารณะให้กับ *I* และ *A* ซึ่งจะดำเนินการผ่านช่องทางที่มั่นคงปลอดภัยเช่น TLS (Transport Transaction Layer Security) ส่วนกุญแจส่วนตัวของ *PG* เก็บจะมีการไว้กับตัวเอง
- *I* และ *A* จะต้องขอใบรับรองดิจิทัล (Digital Certificate) จากองค์กรที่น่าเชื่อถือ ต่อจากนั้นทั้ง *I* และ *A* จะทำการส่งกุญแจสาธารณะให้กับ *PG* ซึ่งจะดำเนินการผ่านช่องทางที่มั่นคงปลอดภัยเช่น TLS (Transport Transaction Layer Security) ในขั้นตอนที่ *PG* ลงทะเบียนกับ *I* และ *A* ส่วนกุญแจส่วนตัวของ *I* และ *A* เก็บไว้กับตัวเอง

3.2 โพรโทคอลการลงทะเบียนของลูกค้า

ก่อนใช้งานระบบที่นำเสนอ *C* จะต้องทำการติดตั้งโปรแกรมจากโพรโทคอลที่นำเสนอ หลังจากที่ติดตั้งเสร็จ *C* เปิดโปรแกรมแล้วทำการลงทะเบียนกับ *M*, *PG* และ *I* ซึ่งการลงทะเบียนดำเนินการผ่านช่องทางที่ปลอดภัยเช่น TLS (Transport Layer Security) วัตถุประสงค์ของการลงทะเบียนคือการแลกเปลี่ยนพารามิเตอร์ $\{DK_{A-B}, K_{A-B}, m\}$ ซึ่งกำหนดให้ K_{A-B} เรียกว่า Long-term key, DK_{A-B} เรียกว่า Distribution key และ *m* คือ ค่าสุ่มที่ระบุจำนวนของคีย์ที่ต้องการสร้างขึ้นโดยขั้นตอนการสร้างเซสชันคีย์โดยขั้นตอนการสร้างเซสชันคีย์แต่ละฝ่ายสามารถอธิบายได้ดังนี้

- *C* และ *M* แลกเปลี่ยนพารามิเตอร์ $\{DK_{C-M}, K_{C-M}, m\}$ ซึ่งหลังจากการแลกเปลี่ยน $\{DK_{C-M}, K_{C-M}, m\}$ กัน *C* และ *M* สามารถสร้างเซสชันคีย์ SK_{C-Mj}, *เมื่อ* $j = 1$ ถึง *n* โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.3
- *C* และ *PG* แลกเปลี่ยนพารามิเตอร์ $\{DK_{C-PG}, K_{C-PG}, m\}$ ซึ่งหลังจากการแลกเปลี่ยน $\{DK_{C-PG}, K_{C-PG}, m\}$ กัน *C* และ *PG* สามารถสร้างเซสชันคีย์ SK_{C-PGj}, เมื่อ $j = 1$ ถึง *n* โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.3
- *C* และ *I* แลกเปลี่ยนพารามิเตอร์ $\{DK_{C-I}, K_{C-I}, m\}$ ซึ่งหลังจากการแลกเปลี่ยน $\{DK_{C-I}, K_{C-I}, m\}$ กัน *C* และ *I* สามารถสร้างเซสชันคีย์ SK_{C-Ij}, เมื่อ $j = 1$ ถึง *n* โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.3

3.3 โพรโทคอลการชำระเงิน

หลังจากที่ C เลือกสินค้าหรือบริการเรียบร้อยแล้ว C ร้องข้อเพื่อชำระเงินค่าสินค้าหรือบริการรูปที่ 2 แสดงโพรโทคอลการชำระเงินรายละเอียดสามารถอธิบายดังข้างล่าง

M1: C → M: ID_C, $\{ID_C, h(OI), Price, \{ID_C, h(OI), Price\}_{SKC-PGj}\}_{SKC-Mj}$, $h(ID_C, h(OI), Price, SK_{C-Ij})$

M2: M → PG: ID_C, ID_M, $h(ID_M, h(\{\{ID_C, h(OI), Price\}_{SKC-Mj}\}_{SKC-PGj}))$, $\{\{ID_C, ID_M, h(OI), Price\}_{SKC-PGj}\}_{Pri-M}$

M3: PG → I: ID_C, $h(ID_C, h(OI), Price, SK_{C-Ij})$, $\{ID_C, h(OI), Price\}_{Pri-PG}\}_{Pub-I}$

M4: I → PG: *Yes/No*, $h(Yes/No, h(OI), SK_{C-Ij+1})$, $\{\{h(Yes/No, h(OI))\}_{Pri-I}\}_{Pub-PG}$

M5: PG → A: $\{\{ID_M, h(OI), Price\}_{Pri-PG}\}_{Pub-A}$

M6: A → PG: *Yes/No*, $\{\{Yes/No, ID_M, h(OI)\}_{Pri-A}\}_{Pub-PG}$

M7: PG → M: *Yes/No*, $\{\{Yes/No, h(OI)\}_{Pri-PG}\}_{Pub-M}$

M8: PG → C: *Yes/No*, $h(h(Yes/No, h(OI), SK_{C-Ij+1}), SK_{C-PGj+1})$

M1: *C* ส่งข้อความร้องขอการชำระเงินไปให้กับ *M* ประกอบด้วย ID_C, $\{ID_C, h(OI), Price, \{ID_C, h(OI), Price\}_{SKC-PGj}\}_{SKC-Mj}$, $h(ID_C, h(OI), Price, SK_{C-Ij})$ ข้อความ $\{ID_C, h(OI), Price, \{ID_C, h(OI), Price\}_{SKC-PGj}\}_{SKC-Mj}$ เป็นข้อความที่ใช้ยืนยันว่า *C* สร้างข้อความนี้ขึ้นมาเพราะ SK_{C-PGj} เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *PG* และ SK_{C-Mj} เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *M* ดังนั้น *C* ไม่สามารถปฏิเสธว่าไม่ได้สร้าง นอกจากนี้ข้อความ $h(ID_C, h(OI), Price, SK_{C-Ij})$ เป็นรหัสพิสูจน์ทราบตัวตนข้อความ (MAC) เป็นข้อความเพื่อยืนยันว่า *C* ส่งข้อความนี้ให้กับ *I* เพราะเซสชันคีย์ SK_{C-Ij} เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *I*

M2: เมื่อ *M* ได้รับข้อความจาก *C* แล้ว *M* นำข้อความ $\{ID_C, h(OI), Price, \{ID_C, h(OI), Price\}_{SKC-PGj}\}_{SKC-Mj}$ มาถอดรหัสลับด้วยแชสชันคีย์ SK_{C-Mj} แล้วทำการตรวจสอบ ID_C, $h(OI)$ และ *Price* ถ้าไม่ตรงกัน *M* สิ้นสุดการติดต่อสื่อสารทันที แต่ถ้าตรงกัน *M* ส่งข้อความ ID_C, ID_M, $h(ID_M, h(\{\{ID_C, h(OI), Price\}_{SKC-Mj}\}_{SKC-PGj}))$, $\{\{ID_C, ID_M, h(OI), Price\}_{SKC-PGj}\}_{Pri-M}$

ข้อความ $h(ID_M, h(\{\{ID_C, h(OI), Price\}_{SKC\text{-}Mj}\}_{SKC\text{-}PGj}))$ เพื่อยืนยันว่า M สร้างข้อความนี้และข้อความ $\{\{ID_C, ID_M, h(OI), Price\}_{SKC\text{-}PGj}\}_{Pri\text{-}M}$ เข้ารหัสลับด้วยกุญแจส่วนตัวของ PG เพื่อยืนยัน M ไม่สามารถปฏิเสธความรับผิดชอบว่าไม่ได้ส่งข้อความนี้ ต่อจากนั้น M ส่งข้อความทั้งหมดให้ PG

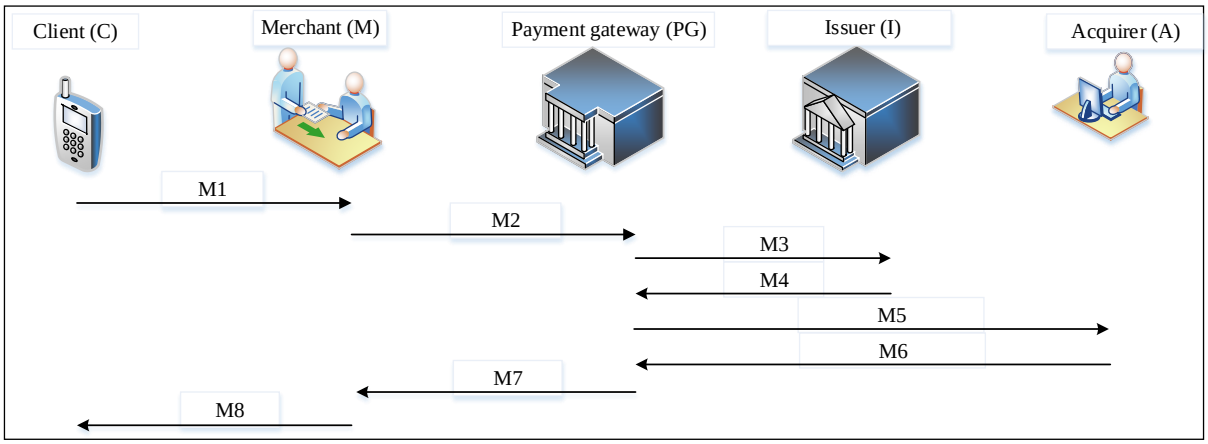
M3: เมื่อ PG ได้รับข้อความจาก M แล้ว PG นำข้อความ $\{\{ID_C, ID_M, h(OI), Price\}_{SKC\text{-}PGj}\}_{Pri\text{-}M}$ ถอดรหัสลับด้วยกุญแจสาธารณะของ M และถอดรหัสลับอีกครั้งด้วยเซสชันคีย์ $SK_{C\text{-}PGj}$ ที่ใช้งานร่วมกันระหว่าง C และ PG แล้วตรวจสอบ ID_C และ ID_M ถ้าไม่ตรง PG สิ้นสุดการติดต่อทันที แต่ถ้าตรง PG ส่งข้อความร้องขอตัดเงินจากบัญชีของ C โดยส่งข้อความ $ID_C, h(ID_C, h(OI), Price, SK_{C\text{-}Ij}), \{ID_C, h(OI), Price\}_{Pri\text{-}PG}\}_{Pub\text{-}I}$ ให้กับ I ซึ่งข้อความ $\{ID_C, h(OI), Price\}_{Pri\text{-}PG}\}_{Pub\text{-}I}$ ถูกเข้ารหัสลับด้วยกุญแจส่วนตัวของ PG และถูกเข้ารหัสลับด้วยกุญแจสาธารณะของ I เพื่อพิสูจน์ทราบตัวตนทั้ง PG และ I

M4: เมื่อ I ได้รับข้อความจาก PG แล้ว I นำข้อความ $\{ID_C, h(OI), Price\}_{Pri\text{-}PG}\}_{Pub\text{-}I}$ ถอดรหัสลับด้วยกุญแจส่วนตัวของ I ต่อจากนั้นนำข้อความที่ได้มาถอดรหัสลับด้วยกุญแจสาธารณะของ PG นำข้อความ $ID_C, h(OI)$ และ $Price$ เข้าฟังก์ชันแฮช พร้อมกับเซสชันคีย์ $SK_{C\text{-}Ij}$ เปรียบเทียบกับค่าแฮชข้อความและจำนวนเงินพอในการชำระเงิน $h(ID_C, h(OI), Price, SK_{C\text{-}Ij})$ ถ้าไม่ตรงหรือจำนวนเงินไม่พอการชำระ I ส่งข้อความ No กลับไปยัง PG แล้ว PG ส่งต่อให้กับ C ในข้อความ M8 แต่ถ้าตรงกันจะส่งข้อความ Yes กลับไปยัง PG โดย I จะส่งข้อความ $Yes/No, h(Yes/No, h(OI), SK_{C\text{-}Ij+1}), \{\{h(Yes/No, h(OI))\}_{Pri\text{-}I}\}_{Pub\text{-}PG}$ ให้กับ PG ข้อความ $h(Yes/No, h(OI), SK_{C\text{-}Ij+1})$ เป็นรหัสพิสูจน์ทราบตัวตนข้อความ (MAC) ระหว่าง C และ I ส่วนข้อความ $\{\{h(Yes/No, h(OI))\}_{Pri\text{-}I}\}_{Pub\text{-}PG}$ เป็นการพิสูจน์ทราบตัวตนระหว่าง I และ PG

M5: เมื่อ PG ได้รับข้อความจาก I แล้ว PG นำข้อความ $\{\{h(Yes/No, h(OI))\}_{Pri\text{-}I}\}_{Pub\text{-}PG}$ ถอดรหัสลับด้วยส่วนตัวของ PG และนำมาถอดรหัสลับอีกครั้งด้วยกุญแจสาธารณะของ I แล้วนำข้อความทั้งหมดมาเข้ารหัสลับด้วยกุญแจส่วนตัวของ PG และเข้ารหัสลับอีกครั้งด้วยกุญแจสาธารณะของ A ต่อจากนั้นส่งข้อความโอนเงินจาก I ไป A โดยส่งข้อความ $\{\{ID_M, h(OI), Price\}_{Pri\text{-}PG}\}_{Pub\text{-}A}$ ให้กับ A ซึ่งข้อความนี้เป็นการพิสูจน์ทราบตัวตนระหว่าง A และ PG

M6: หลังจากที่ A ได้รับข้อความ $\{\{ID_M, h(OI), Price\}_{Pri\text{-}PG}\}_{Pub\text{-}A}$ แล้ว A นำมาถอดรหัสลับด้วยกุญแจส่วนตัวของ A ต่อจากนั้นถอดรหัสลับด้วยกุญแจสาธารณะของ PG นำ $Price$ มาตรวจสอบกับจำนวนเงินที่โอนมาจาก I ถ้าไม่ตรงกัน A ส่งข้อความ No กลับให้ PG แต่ถ้าตรงกัน A ส่งข้อความ Yes กลับให้ PG โดยที่ A จะส่งข้อความ $Yes/No, \{\{Yes/No, ID_M, h(OI)\}_{Pri\text{-}A}\}_{Pub\text{-}PG}$ ให้กับ PG ข้อความ $\{\{Yes/No, ID_M, h(OI)\}_{Pri\text{-}A}\}_{Pub\text{-}PG}$ เป็นการพิสูจน์ทราบตัวตนระหว่าง A และ PG

M7: เมื่อ PG ได้รับข้อความจาก A แล้ว PG นำข้อความ $\{\{Yes/No, ID_M, h(OI)\}_{Pri\text{-}A}\}_{Pub\text{-}PG}$ ถอดรหัสลับด้วยกุญแจส่วนตัวของ PG แล้วถอดรหัสลับอีกครั้งด้วยกุญแจสาธารณะของ A และนำข้อความ $Yes/No, ID_M, h(OI)$ มาเข้ารหัสลับด้วยกุญแจสาธารณะของ M และเข้ารหัสลับอีกครั้งด้วยกุญแจส่วนตัวของ PG ส่งให้กับ M ซึ่งข้อความนี้เป็นการพิสูจน์ทราบตัวตนระหว่าง M และ PG ต่อจากนั้น PG ส่งใบเสร็จรับเงินให้กับ C โดยส่งข้อความ $Yes/No, h(h(Yes/No, h(OI), SK_{C\text{-}Ij+1}), SK_{C\text{-}PGj+1})$ สิ้นสุดการทำงานของโพโทคอล



*รูปที่ 2. แสดง*โพรโทคอลการชำระเงิน

4. การวิเคราะห์และอภิปราย

ในส่วนนี้จะวิเคราะห์และอธิปรายเกี่ยวกับโพรโทคอลที่นำเสนอซึ่งประกอบด้วยการวิเคราะห์ความมั่นคงปลอดภัย การวิเคราะห์การพิสูจน์ทราบตัวตนสองทาง และวิเคราะห์การห้ามปฏิเสธความรับผิดชอบ

4.1. การวิเคราะห์ความมั่นคงปลอดภัย

4.1.1 การรักษาความลับของข้อมูล (Data Confidentiality)

การเข้ารหัสลับด้วยเซสชันคีย์แต่ละครั้งผู้ที่มีเซสชันคีย์ที่ตรงกันเท่านั้นที่จะสามารถถอดรหัสลับข้อมูลได้และการสร้างเซสชันคีย์มีลักษณะเป็นแบบออฟไลน์ โดยไม่มีการส่งเซสชันคีย์ผ่านทางเครือข่าย จะทำให้การดักจับคีย์ไปทำการวิเคราะห์เป็นไปได้ยาก ส่งผลทำให้ระบบมีความมั่นคงปลอดภัยเพิ่มยิ่งขึ้น นอกจากนี้การเข้ารหัสลับด้วยกุญแจสาธารณะของผู้รับยังสามารถรักษาความลับของข้อมูลได้ เนื่องจากผู้ที่มีกุญแจส่วนตัวของผู้รับเท่านั้น จึงจะสามารถถอดรหัสลับได้

4.1.2 การพิสูจน์ทราบตัวตนของผู้ส่งข้อความ (Party Authentication)

คุณสมบัตินี้เป็นการพิสูจน์ทราบตัวตนของผู้ส่งข้อความ โดยการนำเอา Message Authentication Code (MAC) มาประยุกต์ใช้งาน ทำให้ผู้รับมั่นใจได้ว่าผู้ส่งเป็นผู้ส่งข้อความมาจริงและผู้รับเป็นผู้รับข้อความจริง นอกจากนี้การเข้ารหัสลับด้วยกุญแจส่วนตัวของผู้ส่งยังสามารถพิสูจน์ทราบตัวตนของผู้ส่งข้อความได้ เพราะว่าผู้รับข้อความสามารถใช้กุญแจสาธารณะของผู้ส่งถอดรหัสลับข้อความได้จึงรู้ว่าใครเป็นผู้ส่งข้อความ

4.1.3 การต้านทานการโจมตีแบบ Replay Attack

การโจมตีแบบ Replay Attack โดยการปลอมตัวเป็นไคลเอนท์ (Client) แล้วส่งข้อมูลที่ดักจับได้อีกครั้ง จะประสบความสำเร็จได้น้อย เนื่องจากการเปลี่ยนเซสชันคีย์ทุกครั้งที่มีการติดต่อสื่อสารอย่างสมบูรณ์ นอกจากนี้โพรโทคอลที่นำเสนอยังใช้วันที่และเวลาของแต่ละธุรกรรมไม่ซ้ำกัน สามารถตรวจสอบได้ว่ามีการส่งข้อความซ้ำหรือไม่

4.1.4 การคงสภาพของข้อความ

การใช้ฟังก์ชันแฮชทำให้สามารถตรวจสอบได้ว่าข้อมูลที่ส่งมานั้นระหว่างทางถูกเปลี่ยนแปลงข้อมูลจากบุคคลอื่นมาก่อนหรือไม่และการพิสูจน์ทราบตัวตนของผู้ส่งข้อความ โดยนำเอา Message Authentication Code ยังมีคุณสมบัติตรวจสอบความถูกต้องของข้อความอีกด้วย

4.1.5 การต้านทานการโจมตีแบบ Brute Force Attack

การโจมตีชนิด Brute Force Attack เพื่อค้นหาคีย์ที่ถูกต้องนั้นในโพรโทคอลที่นำเสนอนั้นทำได้ยาก เนื่องจากมีการเปลี่ยนแปลงค่าของเซสชันคีย์ในทุกๆ ครั้งที่มีการติดต่อสมบูรณ์ นอกจากนี้การนำเอาเทคนิคการสร้างและการกระจายคีย์แบบออฟไลน์มาใช้งาน ทำให้การค้นหาคีย์ตั้งต้นในการสร้างชุดของเซสชันคีย์ทั้งหมดสามารถทำได้ยาก จึงส่งผลต่อการโจมตีแบบ Brute Force Attack ประสบความสำเร็จน้อยลง และการนำการเข้ารหัสลับแบบอสมมาตรมาใช้งานยังสามารถทนทานการโจมตีแบบ Brute Force Attack อีกด้วย

4.1.6 การโจมตีชนิด Man in The Middle Attack

ผู้โจมตีไม่สามารถปลอมตัวเป็นผู้ที่มีความเกี่ยวข้องหรือดักฟังข้อความของผู้ส่งได้ เนื่องจากมีการสร้างและกระจายเซสชันคีย์

โดยที่ไม่ต้องมีการส่งคีย์ดังกล่าวผ่านเครือข่าย นอกจากนี้ยังมีการเปลี่ยนคีย์ทุกครั้งในการสื่อสารอย่างสมบูรณ์ พร้อมทั้งใช้การเข้ารหัสลับที่เหมาะสม

4.2. การวิเคราะห์การพิสูจน์ทราบตัวตนสองทาง

การนำการสร้างและกระจายเซสชันคีย์แบบออฟไลน์มาใช้งาน ทำให้สามารถยืนยันได้ว่า ผู้ที่มีคีย์ที่ตรงกันเท่านั้นที่สามารถเข้ารหัสลับและถอดรหัสลับได้ หรือสามารถตรวจสอบข้อความที่รับมาได้ พร้อมทั้งโพรโทคอลที่นำเสนอได้นำเอา Message Authentication Code (MAC) มาประยุกต์ใช้ ทำให้สามารถยืนยันตัวผู้ส่งและตัวผู้รับได้เช่น ในข้อความที่หนึ่งของโพรโทคอลที่นำเสนอ

M1: C → M: ID_C, $\{ID_C, h(OI), Price, \{ID_C, h(OI), Price\}_{SKC\text{-}PGj}\}_{SKC\text{-}Mj}$, $h(ID_C, h(OI), Price, SK_{C\text{-}Ij})$

จากข้อความข้างบนการเข้ารหัสลับด้วยเซสชันคีย์ $SK_{C\text{-}PGj}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *PG* และเซสชันคีย์ $SK_{C\text{-}Mj}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *M* ดังนั้นข้อความนี้ *C* เท่านั้นที่สามารถสร้างข้อความและข้อความนี้ยังสามารถยืนยันผู้รับข้อความ

นอกจากนี้วิทยาการการเข้ารหัสลับแบบอสมมาตรมาใช้งานยังสามารถยืนยันผู้ส่งและผู้รับได้ เนื่องจากการเข้ารหัสลับด้วยกุญแจสาธารณะของผู้รับซึ่งผู้รับเท่านั้นจะสามารถถอดรหัสลับได้ จึงสามารถยืนยันตัวผู้รับได้และการเข้ารหัสลับด้วยกุญแจ ส่วนตัวผู้ส่งที่มีกุญแจสาธารณะของผู้ส่งจะสามารถถอดรหัสลับได้ จึงสามารถยืนยันตัวผู้ส่งได้เช่น ในข้อข้อความที่สามของโพรโทคอลที่นำเสนอ

M3: PG → I: ID_C, $h(ID_C, h(OI), Price, SK_{C\text{-}Ij})$, $\{ID_C, h(OI), Price\}_{Pri\text{-}PG}\}_{Pub\text{-}I}$

จากข้อความข้างบนการเข้ารหัสลับด้วยกุญแจส่วนตัวของ *PG* ผู้ที่มีกุญแจสาธารณะของ *PG* เท่านั้นที่จะสามารถถอดรหัสลับได้ จึงสามารถยืนยันผู้ส่งและการเข้ารหัสลับด้วยกุญแจสาธารณะของ *I* จึงสามารถยืนยันผู้รับเพราะ *I* มีกุญแจส่วนตัวจึงสามารถถอดรหัสลับได้

4.3. วิเคราะห์การห้ามปฏิเสธความรับผิดชอบ

การห้ามปฏิเสธความรับผิดชอบเป็นคุณสมบัติอย่างหนึ่งของความมั่นคงปลอดภัยโดยใช้การเข้ารหัสลับแบบอสมมาตร แต่อย่างไรก็ตาม งานวิจัยที่นำเสนอสามารถใช้การเข้ารหัสลับแบบสมมาตรเพื่อให้มีคุณสมบัติการไม่สามารถปฏิเสธความรับผิดชอบเช่น ข้อความที่หนึ่ง

M1: C → M: ID_C, $\{ID_C, h(OI), Price, \{ID_C, h(OI), Price\}_{SKC\text{-}PGj}\}_{SKC\text{-}Mj}$, $h(ID_C, h(OI), Price, SK_{C\text{-}Ij})$

จากข้อความข้างบนเซสชันคีย์ $SK_{C\text{-}PG}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *PG* และ $SK_{C\text{-}M}$ เป็นเซสชันคีย์ที่ใช้งานร่วมกันระหว่าง *C* และ *M* ซึ่งเป็นเซสชันคีย์ที่ *C* มี ดังนั้นข้อความ $\{ID_C, h(OI), Price\}_{SKC\text{-}PGj}\}_{SKC\text{-}Mj}$, *C* ไม่สามารถปฏิเสธความรับผิดชอบว่าไม่ได้เป็นผู้สร้างข้อความนี้

5. การวิเคราะห์ประสิทธิภาพของโพรโทคอล

หัวข้อนี้จะเป็นการวิเคราะห์ประสิทธิภาพของโพรโทคอลที่ได้มีการนำเสนอในข้างต้น จากตาราง 2 แสดงรายละเอียดขนาดและรูปแบบของข้อความที่ใช้กับโพรโทคอลที่นำเสนอ

ตาราง 2. รูปแบบข้อความและความยาวแต่ละสัญลักษณ์

Symbol	Size (Bits)	Example
T	160	01/01/2015 08:00:00
OD	80	P0001 9999
Price	32	9999
ID	80	00000001
Yes/No	24	Yes/No

จากตารางที่ 2 แสดงรูปแบบข้อความและความยาวแต่ละสัญลักษณ์โพรโทคอลที่นำเสนอ

ตาราง 3. วิทยาการเข้ารหัสลับ

Cryptography	Size (Bits)
Advanced Encryption Standard (AES)	128
Rivest-Shamir-Adleman (RSA)	1,024
Secure Hash Algorithm (SHA1)	160
Keyed-hash Message Authentication Code (HMAC)	160

จากตารางที่ 3 แสดงรายละเอียดวิทยาการเข้ารหัสลับที่ใช้กับโพรโทคอลที่นำเสนอ

ตารางที่ 4. ขนาดความยาวของโพรโทคอลที่นำเสนอ

Message	Size (Bits)
M1	1,008
M2	1,344
M3	1,264
M4	1,208
M5	1,024
M6	1,048
M7	1,048
M8	184
Total (Byte)	**8,128**

จากตารางที่ 4 แสดงรายละเอียดขนาดความยาวของโพรโทคอลที่นำเสนอมีขนาดความยาวของข้อความน้อยกว่าความยาวสูงสุด 1G (2048 bps) ดังนั้นโพรโทคอลที่นำเสนอจึงเหมาะสมกับเครือข่ายตั้งแต่ 1G ขึ้นไป

ตาราง 5. การเปรียบเทียบวิทยาการเข้ารหัสลับ

	[7]	[8]	[9]	Our Protocol
Symmetric Cryptography	9	9	5	2
Asymmetric Cryptography	3	3	1	11
Hash Function	7	7	3	2
Message Authentication Code	-	-	-	4
Number of Messages	11	11	17	8
Number of Parties	5	5	5	5

จากตารางที่ 5 แสดงรายการเปรียบเทียบวิทยาการเข้ารหัสลับโพรโทคอล [7] [8] [9] กับโพรโทคอลที่นำเสนอ โดยที่โพรโทคอลที่นำเสนอจะใช้การเข้ารหัสลับแบบอสมมาตรมากกว่า [7] [8] [9] เนื่องจากต้องการแก้ไขข้อจำกัดของ [7] [8] [9] การพิสูจน์ทราบตัวตนสองทาง แต่อย่างไรก็ตามจำนวนข้อความสิ้นสุดการทำงานของโพรโทคอลที่นำเสนอน้อยกว่า [7] [8] [9] จึงทำให้โพรโทคอลที่นำเสนอมีประสิทธิภาพมากกว่า [7] [8] [9]

ตาราง 6. การเปรียบเทียบความมั่นคงปลอดภัย

	[7]	[8]	9]	Our Protocol
การรักษาความลับของข้อมูล	Y	Y	Y	Y
ความคงสภาพของข้อมูล	Y	Y	Y	Y
การห้ามปฏิเสธความรับผิดชอบ	Y	Y	Y	Y
การพิสูจน์ทราบตัวตนสองทาง	N	N	N	Y

ตารางที่ 6 แสดงรายการเปรียบเทียบความมั่นคงปลอดภัยโพรโทคอล [7] [8] [9] กับโพรโทคอลที่นำเสนอ โดยที่งานที่

นำเสนอมีคุณสมบัติความมั่นคงปลอดภัยเช่น การรักษาความลับของข้อมูล ความคงสภาพของข้อมูล การห้ามปฏิเสธความรับผิดชอบและการพิสูจน์ทราบตัวตนสองทาง ขณะที่โพรโทคอล [7] [8] [9] ขาดคุณสมบัติความมั่นคงปลอดภัยเช่น การพิสูจน์ทราบตัวตนสองทาง ดังนั้นโพรโทคอลที่นำเสนอจึงมีคุณสมบัติความมั่นคงปลอดภัยดีกว่า [7] [8] [9] โดยที่ Y หมายถึงมีคุณสมบัติความมั่นคงปลอดภัยและ N หมายถึงไม่มีคุณสมบัติความมั่นคงปลอดภัย

ตารางที่ 7 การวิเคราะห์พื้นที่ที่สูญเสียให้แก่โพรโทคอล

Protocol Overhead		%	2048-Bit (1G)
M1	1,008	49.12	1,040
M2	1,344	65.62	704
M3	1,264	61.71	784
M4	1,208	58.98	840
M5	1,024	50.00	1,024
M6	1,048	51.17	1,000
M7	1,048	51.17	1,000
M8	184	8.98	1,864

จากตารางที่ 7 แสดงพื้นที่ที่สูญเสียให้แก่โพรโทคอลเปรียบเทียบกับการสื่อสารแบบ 1G (2048 bps) กับงานวิจัยที่นำเสนอ โดยส่วนใหญ่พื้นที่ที่สูญเสียให้แก่โพรโทคอลน้อยกว่าข้อมูลสูงสุดในการสื่อสารคือ 2048 bps เพราะการออกแบบโพรโทคอลจะเน้นการใช้ฟังก์ชันแฮชและการเข้ารหัสลับแบบอสมมาตรและสมมาตรเท่าที่จำเป็นแต่ยังคงมีความมั่นคงปลอดภัยที่เพียงพอ

6. สรุปผลการวิจัย

งานวิจัยที่ได้นำเสนอได้โพรโทคอลเพื่อแก้ข้อจำกัดของงานวิจัยที่มีอยู่เช่น ความมั่นคงปลอดภัยที่จำเป็นเช่น การรักษาความลับของข้อมูล ความคงสภาพของข้อมูล การห้ามปฏิเสธความรับผิดชอบและการพิสูจน์ทราบตัวตนสองทาง โพรโทคอลที่นำเสนอข้อความที่มีจำนวนน้อยในการจบการทำงานของโพรโทคอลส่งผลทำให้มีประสิทธิภาพและใช้เวลาน้อยกว่าโพรโทคอลที่มีอยู่ นอกจากนี้งานวิจัยที่นำเสนอใช้การเข้ารหัสลับแบบอสมมาตรและสมมาตรพร้อมทั้งฟังก์ชันแฮชเพื่อเพิ่มความมั่นคงปลอดภัยเพิ่มขึ้นและยังเข้ากับโครงสร้างระบบเครือข่ายไร้สายในปัจจุบันโดยไม่ต้องเพิ่มโครงสร้างระบบเครือข่ายไร้สาย

เอกสารอ้างอิง

[1] S. Kungpisdan, and S. Metheekul, "A Secure Offline Key Generation With Protection Against Key Compromise," Proceedings of the 13th World Multi-conference on Systemics, Cybernetics, and Informatics 2009, Orlando, USA, 2009.

[2] O. Dandash , Y. Wang , P. Dung, and L.B. Srinivasan , "Fraudulent Internet Banking Payments Prevention using Dynamic Key, Journal of Networks," Vol. 3, No. 1, Academy Publisher, pp. 25-34, 2008.

[3] S. Kungpisdan, P.D. Le, and B. Srinivasan, "A Limited-Used Key Generation Scheme for Internet Transactions," Lecture Notes in Computer Science, Vol. 3325, 2005.

[4] H.H. Ngo, X. Wu, P. D. Le, C. Wilson, and B. Srinivasan, "Dynamic Key Cryptography and Applications," International Journal of Network Security, Vol. 10, No. 3, pp. 161-174, 2010.

[5] S. Kungpisdan, B. Srinivasan, and P.D. Le, "Lightweight Mobile Credit-card Payment Protocol," Lecture Notes in Computer Science, Vol. 2904, pp. 295-308, 2003.

[6] A. D. Rubin, and R.N. Wright, "Off-line Generation of Limited-Use Credit Card Numbers," Lecture Notes in Computer Science, Vol. 2339, pp. 196-209, 2002.

[7] M. Vahidalizadehdizaj and T Lixin, "A new mobile payment protocol (GMPCP) by using a new key agreement protocol (GC)," Intelligence and Security Informatics (ISI), 2015 IEEE International Conference, pp. 169-172, 2015.

[8] M. Vahidalizadehdizaj, T. Lixin, and J. Jigar, "A new mobile payment protocol (GMPCP) by using a new group key agreement protocol (VTGKA)," In 2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-7), 2015.

[9] J. Yang, and L. Pei-Yu, "A mobile payment mechanism with anonymity for cloud computing," Journal of Systems and Software 116, pp. 69-74, 2016.

[10] S. Kungpisdan, B. Srinivasan, and P.D. Le, "A secure account-based mobile payment protocol," Information Technology: Coding and Computing, Proceedings, ITCC 2004, International Conference on. Vol. 1. IEEE, pp. 35-39, 2004.