การวิเคราะห์และออกแบบโพรโตคอลสำหรับชำระค่าสินค้าและบริการบนโทรศัพท์มือถือผ่านตัวแทนที่มีความมั่นคงปลอดภัย
The Analysis and Design of Agent-based Secure Mobile Payment Protocol

เพ็ญศรี ปักกะสีนัง
สาขาวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏราชนครินทร์

Abstract

The payment for goods and services on mobile devices via an agent-based mobile payment protocol is gaining in popularity amidst today's fast paced lifestyles. The protocol's features provide for the needs of this new era by offering service that is fast, easy, secure and global. However, existing mobile payment systems still have problems with performance and security. One of the main problems is computation time, in which the result of the calculation for data packages transmission is long and complex. This paper proposed a new, secure and lightweight mobile payment protocol for making payments on mobile devices. This protocol not only provides necessary security properties, but also supports multiple payments.

Keywords : Protocol, Mobile Payment, Secure, Agent-based

บทคัดย่อ

การชำระเงินค่าสินค้าและบริการผ่านตัวแทนบนโทรศัพท์มือถือกำลังได้รับความนิยมสูง เนื่องจากสภาวะการดำรงชีวิตในปัจจุบันที่มีความเร่งรีบ โดยคุณสมบัติของโพรโตคอลที่ชำระเงินผ่านโทรศัพท์มือถือที่ใช้งานในยุคปัจจุบันจำเป็นต้องมีความรวดเร็ว ความมั่นคงปลอดภัย และสามารถเข้าถึงได้ง่ายไม่จำกัดสถานที่ทั่วโลก อย่างไรก็ตามในการใช้งานจริงยังพบว่ามีประเด็นปัญหาด้านความมั่นคงปลอดภัยของข้อมูลและด้านประสิทธิภาพของการชำระเงินผ่านโทรศัพท์มือถือ ประเด็นปัญหาหลักคือระยะเวลาการคำนวณและส่งผ่านข้อมูลจะใช้เวลานานและมีความซับซ้อน ในงานวิจัยนี้นำเสนอโพรโตคอลใหม่สำหรับการชำระค่าสินค้าและบริการบนโทรศัพท์มือถือที่มีน้ำหนักเบาและมีความมั่นคงปลอดภัยสูง โพรโตคอลนี้นอกจากจะให้ความมั่นคงปลอดภัยแล้ว ยังรองรับการชำระเงินได้หลายรายการพร้อมๆ กันได้

คำสำคัญ : โพรโตคอล, การชำระเงินผ่านโทรศัพท์มือถือ, ความมั่นคงปลอดภัย, ตัวแทน

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการทำธุรกรรมทางการเงินผ่านระบบโทรศัพท์มือถือได้รับความนิยมอย่างแพร่หลายจากผู้คนทั่วโลก และยังคงมีแนวโน้มในการขยายตัวเพิ่มมากขึ้นอย่างต่อเนื่อง รายงานข้อมูลจากสถิติมูลค่าการใช้บริการชำระเงินผ่านโทรศัพท์มือถือทั่วโลกของ www.statista.com จากปี 2011 ถึง 2013 มีมูลค่าจากปี 2011 คือ 105.9 ล้านล้านเหรียญสหรัฐ เพิ่มเป็น 253.4 ล้านล้านเหรียญสหรัฐในปี 2013 และคาดการณ์ว่ามูลค่าจะเพิ่มขึ้นถึง 721 ล้านล้านเหรียญสหรัฐในปี 2017 ส่วน Gartner Group ได้ประเมินว่าในปี 2017 จะมีมูลค่าของการจ่ายเงินผ่านโทรศัพท์มือถือถึง 600,000 ล้านเหรียญสหรัฐ และ Juniper Research ได้ประเมินมูลค่าการจ่ายเงินผ่านโทรศัพท์มือถือด้วยเทคโนโลยี NFC สูงถึง 180,000 ล้านเหรียญสหรัฐ เพิ่มจากปี 2012 ถึง 7 เท่าตัว (Juniper, 2016)

อย่างไรก็ตามปัจจุบันพบว่ายังมีข้อจำกัดเกี่ยวกับความปลอดภัย และประสิทธิภาพโทรศัพท์มือถือสำหรับการชำระเงินผ่านโทรศัพท์มือถือ ซึ่งมีรายงานจากศูนย์วิจัย SAN institute ได้วิจัยเกี่ยวกับเรื่อง Security of Mobile Banking and Payments พบว่าร้อยละ 48 ของผู้ตอบแบบสอบถามไม่ใช้ mobile banking เนื่องจากยังมีความกังวลเกี่ยวกับความปลอดภัยในการใช้บริการ mobile banking ร้อยละ32 ไม่มั่นใจในข้อมูลส่วนบุคคล และร้อยละ 34 ไม่แน่ใจในความปลอดภัยของระบบ ซึ่งสอดคล้องกับผลการวิจัยของสถาบันบริการทางการเงินและลูกค้าของรัฐบาลอเมริกัน (Matthew B. Gross, Jeanne M. Hogarth, and Maximilian D. Schmeiser, 2012) จากผู้ตอบแบบสอบถาม 1,973 คน พบว่าร้อยละ 38 ไม่ใช้บริการชำระเงินผ่านระบบโทรศัพท์มือถือ โดยมีเหตุผลคือไม่มั่นใจในเรื่องความปลอดภัย และในรายงานการวิจัยของ ศูนย์วิจัย SAN institute ได้สรุปปัจจัยเสี่ยงในการใช้บริการบนโทรศัพท์มือถือประกอบด้วย ภัยคุกคามจากมัลแวร์ โปรแกรมประสงค์ร้าย ช่องโหว่บนระบบ SMS ช่องโหว่ของฮาร์ดแวร์และซอฟท์แวร์ โครงสร้างของระบบเครือข่ายไร้สาย โครงสร้างพื้นฐานของระบบชำระเงิน โปรแกรมเกี่ยวกับความเป็นส่วนตัวของข้อมูล การขาดเครื่องมือสำหรับควบคุมการปลอมแปลงหลอกลวงข้อมูล นอกจากนี้ยังพบว่าการใช้อุปกรณ์ไร้สายสำหรับชำระเงินยังมีข้อจำกัดอยู่คือโทรศัพท์ไร้สายมีข้อจำกัดด้านพลังงานต่ำ มีความสามารถในการคำนวณและมีพื้นที่ในการจัดเก็บข้อมูลต่ำ นอกจากนั้นยังมีข้อจำกัดของเครือข่ายแบบไร้สาย คือ มีแบนวิดท์ต่ำ ความน่าเชื่อถือต่ำกว่าเครือข่ายแบบใช้สาย และค่าใช้จ่ายในการเชื่อมต่อผ่านเครือข่ายไร้สายสูงกว่าเครือข่ายแบบใช้สาย (T. S. Fun, L. Y. Beng, and M. N. Razali, 2013)

จากประเด็นปัญหาและข้อจำกัดที่กล่าวมาแล้ว มีนักวิจัยจำนวนมากพยายามจะลดข้อจำกัดโดยทำการวิจัย ในหลากหลายรูปแบบ เช่น การสร้างความเชื่อมั่นให้กับผู้ใช้โดยออกแบบและพัฒนาโพรโตคอลสำหรับการรับส่งข้อมูลการชำระเงินผ่านระบบโทรศัพท์มือถือที่มีความปลอดภัยและมีประสิทธิภาพ โดยใช้เทคนิคทางด้านวิทยาการรหัสลับสำหรับเข้ารหัสลับข้อมูลและถอดรหัสลับเพื่อปกป้องข้อมูลให้มีความลับสูงสุด มีความเป็นส่วนตัว และมีความถูกต้อง นอกจากนี้ยังมีการออกแบบสถาปัตยกรรมสำหรับการรับส่งข้อมูลผ่านระบบโทรศัพท์มือถือ ให้สามารถส่งผ่านได้อย่างรวดเร็วและมีความปลอดภัยภายใต้ข้อจำกัดของทรัพยากรบนโทรศัพท์มือถือ อย่างไรก็ตามความพยายามในการค้นหาเทคนิควิธีการที่ดีที่สุดเหมาะสมที่สุดสำหรับการชำระเงินผ่านระบบโทรศัพท์มือถือคงมีการวิจัยอย่างต่อเนื่อง ด้วยเหตุนี้ผู้วิจัยจึงมุ่งหวังที่จะทำการค้นคว้าและทดลองเพื่อให้ค้นพบวิธีการที่เหมาะสมสำหรับการชำระเงินผ่านระบบโทรศัพท์มือภายใต้ข้อจำกัดของเวลาและพลังงาน

วัตถุประสงค์การวิจัย

การวิจัยครั้งนี้ มีวัตถุประสงค์ดังนี้

1. เพื่อศึกษาโพรโตคอลชำระเงินผ่านโทรศัพท์มือถือที่มีในปัจจุบัน
2. เพื่อออกแบบโพรโตคอลสำหรับชำระเงินผ่านโทรศัพท์มือถือ ที่เน้นความมั่นคงปลอดภัยและมีน้ำหนักเบา

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโพรโตคอลสำหรับการชำระเงินทางโทรศัพท์มือถือ แบ่งออกได้เป็น 2 ลักษณะ คือ แบบลูกค้าหนึ่งคนทำรายการ 1 ครั้งเพื่อชำระค่าสินค้าต่อหนึ่งร้านค้า หรือหนึ่งบิล (Bill) เรียกว่าเป็น (1 : 1 Merchant) และแบบ ลูกค้าทำรายการเพียงหนึ่งครั้ง (1 Transaction) เพื่อชำระค่าสินค้ากับหลายร้านค้าหรือหลาย Merchant (1 Merchants) มีรายละเอียดดังนี้

1. การทำรายการชำระเงินแบบ 1 : 1 (one to one)

งานวิจัยที่มุ่งพัฒนาโพรโตคอลให้มีน้ำหนักเบา และมีความมั่นคงปลอดภัยสูงมีดังนี้

1.1 SET Protocol (Secure Electronic Transfer Protocol) เป็นโพรโตคอลที่เป็นมาตรฐาน De facto standard สำหรับชำระเงินผ่านบัตรเครดิต โดยใช้เทคนิคการเข้ารหัสลับแบบอสมมาตร (public key cryptography) และลายเซ็นดิจิทัล เพื่อทำให้ข้อมูล มีคุณสมบัติความมั่นคงปลอดภัย การทำงานมี 3 ขั้นตอน คือ Purchase request, Payment authorization,

Payment Capture การแลกเปลี่ยนข้อมูลจะมี CA (Certificate Authorization) เป็นผู้อนุญาตการทำรายการข้อมูล สนับสนุนคุณสมบัติความปลอดภัยของข้อมูล 3 ด้าน คือ C : Confidentiality, I : Integrity และ A : Authorization (Y. Li and Y. Wang, 2014)

1.2 iKP Protocol (i-Key-Protocol) ใช้เทคนิคการเข้ารหัสลับแบบเดียวกับ SET โพรโตคอลนี้สนับสนุนคุณสมบัติความปลอดภัยของข้อมูล 3 ด้าน คือ CIA (M. Bellare and J. A. Garay, 2000)

1.3 KSL Protocol (Kungpisdan Logic) เป็นโพรโตคอลนี้เน้นการออกแบบเพื่อลดการทำงานที่ Client ให้มีการคำนวณต่ำ ให้เหมาะสำหรับอุปกรณ์ไร้สาย โดยใช้เพียงการเข้ารหัสลับแบบสมมาตรที่ Client สนับสนุนคุณสมบัติด้านความปลอดภัยได้มากกว่าคือ สามารถรองรับคุณสมบัติ Non-repudiation ได้ (S. Kungpisdan and B. Srinivasan, 2003)

1.4 Kungpisdan Protocol (account-based Mobile Payment) พัฒนาต่อเนื่องมาจากโพรโตรคอล KSL โดยใช้วิธีการเข้ารหัสลับแบบสมมาตรทั้งหมด และมีการแชร์คีย์ระหว่างผู้รับกับผู้ส่ง เน้นการชำระเงินผ่านบัตรเครดิต credit card และเปรียบเทียบประสิทธิภาพการทำงานของระบบโดยพิจารณาจากจำนวน Operation ในการเข้ารหัสลับ เทียบกับโพรโตคอล Protocol SET และ iKP พบว่า KSL มีประสิทธิภาพเหนือกว่า และมีคุณสมบัติด้านความปลอดภัยมากกว่าคือ สามารถรองรับคุณสมบัติ Non-repudiation ได้ ทั้งที่ไม่มี Trusted Party (S.Kungpisdan, B. Srinivasan, Le. Phu Dung Le., 2004)

1.5 LMPP Protocol (Lightweight Mobile Payment Protocol) เป็นโพรโตคอลที่ออกแบบการทำงานให้มีประสิทธิภาพเหนือกว่า SET, iKP และ Kungpisdan คือ SET และ iKP ใช้วิธีการเข้ารหัสลับแบบอสมมาตร และลายเซ็นดิจิทัล Kungpisdan ใช้การเข้ารหัสลับแบบสมมาตรและไม่ใช้ Key-has-Function (T. S. Fun, L. Y. Beng, Likoh, J. , Roslan, R., 2008)

1.6 MSET Protocol (Modified SET Protocol) เป็นการปรับปรุงการทำงานของ โพรโตคอล SET ลดจำนวน Operation ในการคำนวณ คือจากการเข้ารหัสลับโดยใช้พลับลิคคีย์จำนวน 11 ครั้ง และ ใช้ไพรเวทคีย์จำนวน 5 ครั้ง ลดเหลือใช้แชร์คีย์ เพียง 10 ครั้ง (Operation) และไม่ใช้ฟังก์ชันแฮช (S. M. Shedid., 2010)

1.7 MPCP2 Protocol (Mobile Pay Center Protocol 2) เป้าหมายของโพรโตคอลนี้คือ การลดจำนวน Operation ในการคำนวณ และการส่งข้อมูลระหว่าง Engaging Parties เน้นการทำงานแบบใช้ Client เป็นศูนย์กลาง (Client Centric Model) การทำงานของโพรโตคอลมีการเข้ารหัสลับแบบสมมาตรที่ทุกๆ Parties โดยใช้การแลกเปลี่ยนคีย์แบบ offline ตามหลักการของ Diffie-Hellman ที่คำนวณค่าคีย์โดยใช้คณิตศาสตร์ Algebra exponential และ modulus และปรับปรุงเป็น Algebra logarithm และ modulus arithmetic และเปรียบเทียบประสิทธิภาพการทำงานกับโพรโตคอล SET, iKP, KSL, Kungpisdan พบว่า มีการคำนวณที่ Client น้อยกว่าทั้ง 3 โพรโตคอล (M. V. Alizadeh Dizaj, R.A. Moghaddam, Samad Momenebellah., 2011)

1.8 PCMS Protocol (Payment Centric Model Using Symmetric Cryptography) เป็นโพรโตคอลที่เน้นการประมวลผลผ่านตัวกลาง วิธีการเข้ารหัสลับแบบสมมาตร (J. T. Isaac, S. Zeadally, 2012)

1.9 SLMPP Protocol Secure Lightweight Mobile Payment Protocol) เป็นโพรโตคอลที่เน้นการออกแบบที่เน้นความปลอดภัยที่อุปกรณ์ปลายทาง หรือ end-to-end ลดการคำนวณที่ Client ซึ่งเปรียบเทียบกับโพรโตคอล SET, iKP, Kungpisdan พบว่าวิธีการนี้มีการคำนวณที่ Client น้อยกว่า จึงเหมาะกับการใช้งานบนอุปกรณ์ไร้สาย ที่มีข้อจำกัดเรื่องความเร็ว ในการประมวลผลและหน่วยความจำ (C. Sekhar, M. Sarvabhatla, 2012)

1.10 LPMP Protocol (Lightweight Protocol For Mobile Payment) เป็นโพรโตคอลที่ลดจำนวน Operation ในการคำนวณลง เพื่อให้เหมาะกับอุปกรณ์ไร้สาย หรือเครือข่ายไร้สาย มีการทำงาน 14 step โดยเทียบประสิทธิภาพกับโพรโตคอล SET, iKP และ KSL พบว่าวิธีการ LPMP มีประสิทธิภาพเหนือกว่าทั้ง 3 วิธีการ โดยไม่มีการใช้ Key-hash-function (D. M. Tripathi, Ojha, A., 2012)

1.11 SAMPP Protocol (Secure Account-based Mobile Payment Protocol) เป็นโพรโตคอลที่ใช้เทคนิคการเข้ารหัสลับแบบอสมมาตร รวมกับ Digital Signature ที่มีการเข้ารหัสลับโดยใช้ Biometric เป็นคีย์ร่วมเพื่อเพิ่มระดับความปลอดภัยของข้อมูล (Multifactor factor authentication) คือเข้ารหัสลับโดยใช้ไพรเวทคีย์ ร่วมกับ Biometric เพื่อยืนยันตัวตน (P. S. Auala and H. Arora, 2013)

2. การทำรายการชำระเงินแบบ 1 : m (one to many) หรือผ่านตัวกลาง

ผู้วิจัยได้ทำการศึกษาโพรโตคอลของ (P. Limpittaya, 2012) และคณะ และโพรโตคอลของ (M. Carbonell, 2008) และคณะ มีรายละเอียดของแต่ละโพรโตคอลดังนี้

2.1 P. Limpittaya และคณะ ได้นำเสนอโพรโตคอลชำระค่าสินค้าแบบเคลื่อนที่ผ่านตัวแทนที่มีความมั่นคงปลอดภัยสูง โดยใช้เทคนิคการเข้ารหัสลับแบบสมมาตร (Symmetric Cryptography) และฟังก์ชันแฮช รูปแบบของโพรโตคอล ดังรูปที่ (a) โดยการประมวลผลมีผู้ที่เกี่ยวข้อง 5 ฝ่าย ได้แก่ ลูกค้า (C : Customer) ตัวแทนของลูกค้า (AC : Customer agent) พ่อค้า (M : Merchant) ตัวแทนของพ่อค้า (AM: Merchant agent) และแม่ข่ายกลาง ที่เรียกว่า BPAC (Bill Payment Accountability) การติดต่อระหว่างเอนทิตีแต่ละตัว จะใช้คีย์กลาง (Intermediate Key) ที่สร้างขึ้นและใช้ร่วมกันระหว่างผู้ส่งกับผู้รับ (b) ซึ่งใช้เป็นเซสชันคีย์ในการทำรายการแต่ละครั้ง และมีการเปลี่ยนแปลงคีย์ไปเรื่อยๆ เพื่อป้องกันการทำรายการซ้ำ ซึ่งโพรโตคอลนี้เน้นการออกแบบให้มีขนาดของข้อความสั้นลงและมีน้ำหนักเบา เพื่อเพิ่มประสิทธิภาพสำหรับการประมวลผลและการเข้ารหัสลับได้อย่างรวดเร็ว และสนับสนุนคุณสมบัติด้านความมั่นคงปลอดภัยที่จำเป็น คือ การรักษาความลับ ความคงสภาพของข้อมูล การพิสูจน์ตัวจริงข้อความ และการส่งต่อความลับ โดยโพรโตคอลที่นำเสนอ มีขั้นตอนการทำงาน 3 กระบวนการคือ การลงทะเบียน การวางใบแจ้งหนี้ และการขอชำระค่าสินค้าของลูกค้า

2.2 M.Carbonell และคณะ (M. Carbonell, J. Torres, D. Suarez, 2008) นำเสนอโพรโตคอลสำหรับชำระเงินอิเล็กทรอนิกส์ (e-payment) ผ่านตัวแทนกลาง (Intermediary) โดยใช้เทคนิคการเข้ารหัสลับแบบอสมมาตร (Asymmetric Cryptography) และการทำลายเซ็นดิจิทัล เพื่อปกป้องข้อมูลให้มีคุณสมบัติด้านความมั่นคงปลอดภัยครบทั้ง 4 ด้านคือ Confidentiality, Integrity, Authentication, Non-repudiation การทำงานของโพรโตคอลเป็นการประยุกต์ใช้ SET protocol โดยในประมวลผลลูกค้า 1 คน สามารถทำรายการเพียงครั้งเดียว สำหรับติดต่อชำระเงินกับพ่อค้าได้หลาย ๆ คน ซึ่งโพรโตคอลนี้เน้นการเข้ารหัสลับข้อมูลสำหรับปกป้องข้อมูลการทำรายการชำระเงินในส่วนต้นทางและปลายทางคือ end-to-end ซึ่งการชำระเงินจะติดต่อผ่านตัวกลาง เพื่อติดต่อชำระเงินกับสถาบันทางการเงินหรือธนาคาร สำหรับการทำรายการชำระเงิน ในโพรโตคอลประกอบด้วยผู้ที่เกี่ยวข้อง หรือเอนทิตี จำนวน 5 เอนทิตี ได้แก่ ลูกค้าหรือ Client Side (C) พ่อค้า (M) ซึ่งเป็น Virtual Merchant ตัวกลาง (Intermediary หรือ Agents) ผู้ให้บริการชำระเงิน (PSP : Payment Service Provider) อาจเป็นสถาบันการเงินหรือไม่ใช่สถาบันการเงินก็ได้ ส่วนของลูกค้าคือ Issuer bank และพ่อค้าส่วนของพ่อค้า คือ Acquirer bank ถือว่าเป็น Trusted Third Parties

ในครั้งนี้ผู้วิจัยได้ทำการศึกษาวิเคราะห์โพรโตคอลสำหรับการชำระเงินผ่านโทรศัพท์มือถือ โดยพิจารณาใน 3 ประเด็นดังนี้

1. ประเด็นเทคนิคที่ใช้ในการเข้ารหัสลับ

ในกระบวนการทำงานของการรับส่งข้อมูลระหว่าง Customer, Merchant และ Payment Gateway

โดยทั่วไปกระทำเพื่อให้มีคุณสมบัติของความปลอดภัย โดยมีการตรวจสอบสิทธิ์การเข้าถึงข้อมูล Authorization และการพิสูจน์ตัวตนของผู้ใช้ ในงานวิจัย ที่กล่าวมามีการตรวจสอบสิทธิ์โดยใช้ รหัสผ่าน และพิสูจน์ตัวจริงโดยใช้ลายนิ้วมือ และมีการปกป้องข้อมูลให้มีความเป็นส่วนตัว มีความถูกต้องรวมทั้งผู้ซื้อขายไม่สามารถปฏิเสธความรับผิดชอบได้ โดยมีเทคนิคที่ใช้ในโพรโตคอลต่างๆ สรุปได้ดังนี้

1) เทคนิคการเข้ารหัสแบบสมมาตร ได้แก่ โพรโตคอล Kungpisdan, LMPP, MSET, MPCP2, PCMS, SLMPP และ LPMP โดยมี Operations คือ Symmetric Key Encryption/Decryption, Hash Function และ Key Generations

2) เทคนิคการเข้ารหัสแบบอสมมาตรได้แก่ โพรโตคอล SET, iKP และ SAMPP โดยมี Operations คือ Public Encryption, Public Decryption, Signature Generations, Signature Verifications, Symmetric Key Encryption/Decryption, Hash Function และ Key Generations

ทั้งนี้ จากเทคนิคการเข้ารหัสทั้งสองประเภท จะเห็นว่าการเข้ารหัสแบบสมมาตรโดยส่วนใหญ่ใช้ Operation น้อยกว่าการเข้ารหัสแบบอสมมาตร จึงทำให้ประสิทธิภาพดีกว่าการเข้ารหัสแบบอสมมาตร ซึ่งเหมาะสำหรับการประมวลผลบนเครือข่ายแบบไร้สาย อย่างไรก็ตามประสิทธิภาพเหมือนจะสวนทางกับความปลอดภัย นั่นหมายถึง การเข้ารหัสแบบอสมมาตรมีกระบวนการที่ซับซ้อนใช้ Operation มากกว่า เวลาในการประมวลผลย่อมมากกว่า ทั้งนี้ ความซับซ้อนของการเข้ารหัสข้อมูล หมายถึงความปลอดภัยที่เพิ่มขึ้นตามไปด้วย ซึ่งเหมาะสำหรับการประมวลผลบนเครือข่ายแบบมีสายที่สามารถรองรับการใช้ทรัพยากรต่างๆ ในปริมาณสูง

2. ประเด็นด้านความปลอดภัย

จากการศึกษาและวิเคราะห์ความปลอดภัยของโพรโตคอลทั้ง 11 โพรโตคอลพบว่า ส่วนใหญ่มีคุณสมบัติสนับสนุนความปลอดภัยใน 4 ด้านหลัก ได้แก่ Confidentiality, Integrity, Authentication และ Non-repudiation พบเพียง 3 โพรโตคอลแบบเดิม คือ SET, iKP และ KSL ที่ไม่รองรับคุณสมบัติ Non-repudiation ส่วนคุณสมบัติด้าน Privacy มีเพียงโพรโตคอล LMPP, MSET, MPCP2, SLMPP, LPMP และ SAMPP ที่รองรับครบทั้ง 4 ด้าน โดยเทคนิคที่สนับสนุนคุณสมบัติความปลอดภัยมีดังนี้

1) Encryption สนับสนุนคุณสมบัติ Confidentiality และ Privacy คือเข้ารหัสข้อมูลทำให้ข้อมูลมีความลับและเป็นส่วนตัว

2) Hash Function สนับสนุนคุณสมบัติ Integrity คือข้อมูลที่ได้รับกับข้อมูลที่ส่งถูกต้องตรงกัน

3) HMAC, Digital Signature, Dual Signature สนับสนุนคุณสมบัติ Authentication เป็นการพิสูจน์ตัวจริงของผู้ใช้งานจากลายเซ็นดิจิทัล โดยใช้คีย์เพื่อตรวจสอบว่ามีคุณสมบัติตรงกันหรือเป็นตัวจริง รวมทั้งสนับสนุนคุณสมบัติ Non-repudiation

4) Key Generation สนับสนุนคุณสมบัติ Non-repudiation เป็นการยืนยันข้อมูลที่ตรงกัน ก่อนการเริ่มทำรายการเพื่อป้องกันไม่ให้ปฏิเสธความรับผิดชอบ

3. การวิเคราะห์ประสิทธิภาพ

การวิเคราะห์ประสิทธิภาพของโพรโตคอลทั้งหมดใช้หลักการนับจำนวน Operations ในการทำเข้ารหัสและถอดรหัส รวมทั้ง Operations อื่นๆ ที่เกี่ยวข้องในการส่งผ่านข้อมูลระหว่าง 3 ส่วน คือ Customer Merchant และ Payment Gateway ซึ่งพบว่า จำนวน Operations ในโพรโตคอลทั้งหมดเรียงจากน้อยไปหามากได้แก่ Protocol LPMP, LMPP, MSET, SAMPP, MPCP2 PCMS, SLMPP, iKP, Kungpisdan, SET และ KSL

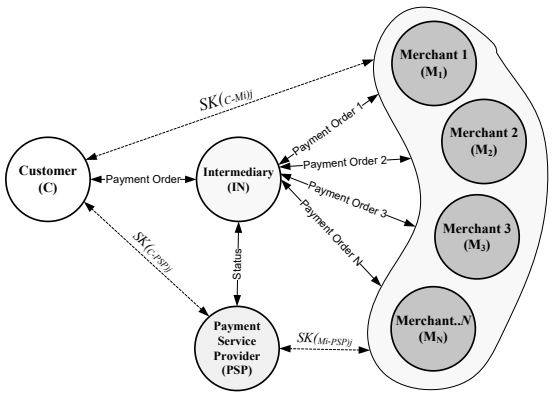
อุปกรณ์และวิธีดำเนินการวิจัย

การชำระค่าสินค้าและบริการ โดยทั่วไปผู้ซื้อ 1 คนสามารถซื้อสินค้าจากพ่อค้าได้หลายคนๆ ละหลายๆ รายการ กล่าวคือผู้ซื้อจะจ่ายเงินค่าสินค้าและบริการตามใบสั่งซื้อหรือใบเรียกเก็บเงินโดยจะจ่ายเป็นรายๆ ไป เช่นถ้าซื้อสินค้าจากร้านค้า 5 ร้าน ผู้ซื้อต้องทำรายการจ่ายจำนวน 5 ครั้ง หรือเรียกว่าเป็นการจ่ายแบบขนาน (parallel payment) ซึ่งวิธีการนี้ทำให้ลูกค้าเสียเวลา จึงมีการพัฒนาการชำระเงินค่าสินค้าและบริการเป็นแบบผ่านตัวแทน หรือคนกลาง เป็นลักษณะห่วงโซ่การชำระเงิน (Chained Payment) คือจะมีตัวแทนกลางทำหน้าที่จ่ายเงินให้กับพ่อค้า โดยจะมีการเก็บค่าธรรมเนียมการจ่ายเงินในแต่ละครั้ง รายละเอียดเกี่ยวกับโพรโตคอลการชำระเงินค่าสินค้าและบริการผ่านตัวแทน ที่นำเสนอมีดังนี้

1. แนวคิดการชำระเงินค่าสินค้าและบริการผ่านตัวแทนที่มีความปลอดภัยสูง

การชำระเงินค่าสินค้าและบริการที่ผ่านตัวแทนที่มีความมั่นคงปลอดภัยสูงตามรูปที่ 1 ประกอบด้วย ผู้ที่เกี่ยวข้อง 4 ฝ่าย ได้แก่ ลูกค้า (Customer หรือ Client แทนด้วยอักษรตัว C) ตัวแทนกลางที่ทำหน้าที่ติดต่อระหว่าง ลูกค้ากับร้านค้า (Intermediary แทนด้วยอักษรตัว IN) ซึ่งจะเป็นผู้รวบรวมรายการสั่งซื้อหรือรายการขอชำระเงิน (PO=POi) พ่อค้าหรือร้านค้า (Merchant แทนด้วยอักษร M) ซึ่งเป็นผู้จำหน่ายสินค้าหรือบริการ ในที่นี้สมมติให้มีพ่อค้าหลายๆ คน โดยกำหนดให้ i แทนจำนวนพ่อค้า ซึ่งมีค่าตั้งแต่ 1 ถึง N แทนด้วยสัญลักษณ์ (Mi, i = 1.. n) และผู้ใช้บริการเกี่ยวกับการชำระค่าสินค้าและบริการ (Payment Service Provider : PSP) จะติดต่อกับสถาบันการเงินของลูกค้าและพ่อค้าอาจเป็นสถาบันการเงินที่เป็นธนาคารพาณิชย์ เช่น ธนาคารของลูกค้า (Issuer) ธนาคารของพ่อค้า (Acquirer) หรือตัวแทนที่ไม่ใช่สถาบันการเงิน โดยมีลูกค้าเท่านั้นที่สามารถติดต่อกับ PSPได้แนวคิดจากรูปคือกลุ่มผู้ประกอบการค้า จะนำเสนอสินค้าและบริการผ่านทางตัวกลาง และลูกค้าเข้าใช้บริการโดยผ่านการอนุญาตจาก IN จึงจะสามารถทำการสั่งซื้อหรือชำระค่าสินค้าและบริการได้ โดย IN เป็นผู้กระจายรายการ ไปยังพ่อค้าหรือร้านค้าต่างๆ และ IN จะเก็บค่าธรรมเนียมการให้บริการจากกลุ่มพ่อค้าที่ใช้บริการผ่านตัวแทนกลาง

จากรูปแบบโพรโตคอลในรูปที่ 1 จะเห็นว่า ลูกค้าไม่สามารถติดต่อธนาคารหรือระบบผู้ให้บริการชำระค่าสินค้าและบริการโดยตรง จะกระทำได้ต่อเมื่อผ่าน IN ดังนั้นรายการจ่ายชำระเงินทั้งหลายจะต้องส่งผ่านมายัง IN และไปตรวจสอบรายการจ่ายที่ Mi เช่น รายการในบิล เลขที่บัญชีของพ่อค้าที่แจ้งไว้กับผู้ซื้อว่าให้ชำระที่หมายเลขบัญชีใด ก่อน และส่งกลับที่ IN เพื่อแจ้งธนาคารให้ทำรายการหักบัญชีของลูกค้าตามที่แจ้งมาในที่นี้ PSP เป็นบุคคลที่สามที่เชื่อถือได้ (Trusted Third Party) ทั้งนี้ในการติดต่อระหว่างเอนทิตีทั้งหมดจะมีการใช้คีย์ร่วมกันเพื่อยืนยันตัวตนของผู้ใช้งาน การแลกเปลี่ยนคีย์และกระจายคีย์ประยุกต์ใช้วิธีการของ Kungpisdan et al.'s approach



รูปที่ 1 จำลองการทำงานของโพรโตคอล

2. การไหลของข้อความในระบบ

ในงานวิจัยนี้การทำงานของโมเดลอยู่ในรูปแบบของ e-payment ซึ่งผู้ซื้อผู้ขายจะมีการติดต่อกันผ่านทางอิเล็กทรอนิกส์ โดยมีโปรแกรมประยุกต์ใช้งาน และอุปกรณ์สื่อสารต่างๆ เช่น โทรศัพท์มือถือ หรือคอมพิวเตอร์ ในการชำระค่าสินค้าและบริการ มีเส้นทางการไหลของข้อมูลเกิดขึ้นในระบบดังนี้ (ดูรูปที่ 2 ประกอบ)

1) ลูกค้า ส่งข้อมูลการขอชำระค่าสินค้าหรือบริการ (Payment Order: PO) ไปยังพ่อค้า โดยผ่านตัวแทนกลาง คือ IN ซึ่งรายละเอียดการขอชำระค่าสินค้าและบริการจะรวมหลายๆ ข้อความสำหรับพ่อค้าหลายคนแทนด้วย

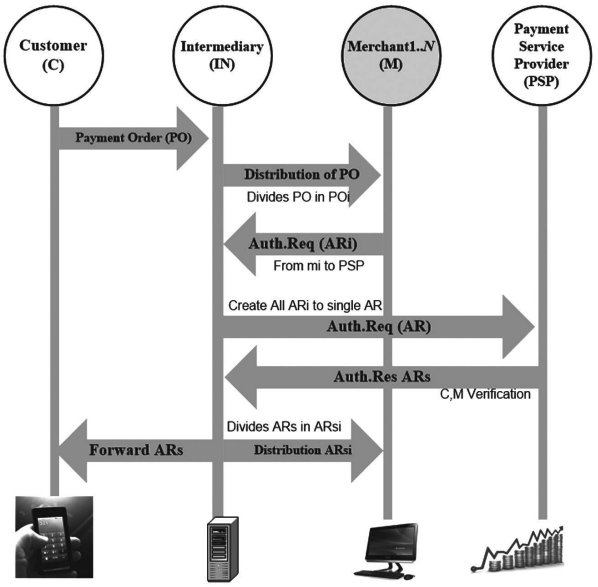
2) ตัวแทนรับรายละเอียดการขอชำระค่าสินค้าและบริการจากลูกค้าในแต่ละครั้งแล้วทำการแยก หรือกระจาย (Multi-Payment Order : Distribution) ใบคำขอชำระค่าสินค้าและบริการ เพื่อส่งไปยังร้านค้าต่างๆ ในที่นี้แทนด้วย

3) พ่อค้าแต่ละคนเมื่อได้รับข้อมูลของลูกค้า ที่ส่งผ่านมาทางตัวแทน และทำการตรวจสอบรายละเอียดต่างๆ เช่น เลขที่ใบสั่งซื้อ จำนวนเงิน ลูกค้า และเลขบัญชีของพ่อค้าที่กำหนดให้ลูกค้าโอนเงินเข้าบัญชีเป็นต้น จากนั้นส่งคำร้องขอทำรายการชำระเงินของลูกค้าไปยังตัวแทนเพื่อให้ดำเนินการหักเงินจากบัญชีลูกค้า เข้าบัญชีของพ่อค้าตามจำนวนเงินที่ลูกค้าสั่งซื้อ ซึ่งในขั้นตอนนี้พ่อค้าแต่ละรายจะตรวจสอบรายละเอียดตามใบ PO และเลขบัญชีที่ให้ลูกค้าโอนเงินเข้าว่าเป็นไปตามที่แจ้งไว้แก่ลูกค้า (Auth.req = ARi)

4) ตัวแทนส่งคำขอทำรายการ (Authorization Request : AR) ไปยัง PSP ซึ่งมีข้อมูลสำคัญ คือ ข้อมูลของลูกค้าและพ่อค้า เช่นเลขบัญชีของลูกค้าและพ่อค้า ซึ่งในส่วนนี้ข้อมูลจะถูกเข้ารหัสโดยเซสชันคีย์ทั้งสองฝ่ายมีเพียง PSP เท่านั้นที่สามารถถอดรหัสลับได้

5) ผู้ให้บริการรับชำระค่าสินค้าและบริการ หรือ PSP ทำการตรวจสอบข้อมูลที่ส่งมาจากตัวแทน ว่าข้อมูลของลูกค้าที่ขอชำระค่าบริการ กับข้อมูลของพ่อค้าตรงกันหรือไม่ แล้วทำรายการหักเงินจากบัญชีลูกค้าไปยังบัญชีพ่อค้า และส่งคำตอบกลับการทำรายการ (Authorization Response : ARs) กลับไปยังตัวแทนกลาง IN (ARs)

6) ตัวแทนเมื่อรับคำตอบกลับการทำรายการ ARs แล้ว Forward ต่อไปให้ลูกค้า และกระจายเป็น ARsi ส่งต่อไปยังพ่อค้าแต่ละคน (IDMi)



รูปที่ 2 เส้นทางการไหลของข้อมูล

3. รายละเอียดโพรโตคอลที่นำเสนอ

โพรโตคอลการชำระเงินบนโทรศัพท์มือถือแบบผ่านตัวแทนที่มีความมั่นคงปลอดภัยสูง สนับสนุนการทำงานแบบ 1 Transaction ของร้านค้า ต่อหลายร้านค้า ซึ่งอำนวยความสะดวกให้ผู้ใช้งาน กรณีที่มีค่าสินค้าและบริการต่างๆ ที่ต้องชำระหลายร้านค้า (bills) ทั้งนี้ มีผู้ที่เกี่ยวข้อง 5 กลุ่ม ได้แก่ ลูกค้า (C) พ่อค้า (M) ตัวแทน (IN) กลุ่มผู้ให้บริการชำระเงิน (PSP) อาจเป็นธนาคารหรือสถาบันการเงินของลูกค้า และพ่อค้า ในการทำงานของระบบจะถือว่า IN เป็น Virtual Machine รายละเอียดของโพรโตคอลที่นำเสนอมีดังนี้

1) นิยามและสมมติฐาน

ตัวแปรที่มีในระบบมีดังนี้

TID : (Transaction ID) หมายถึง รหัสการทำรายการ

IDx : (Unique Identifier of entity x) หมายถึง รหัสของเอนทิตี x เช่น IDC หมายถึง รหัสลูกค้า

PO : (Payment Order) หมายถึง ใบรายการขอชำระเงิน หรือใบเรียกเก็บเงิน (Bill) และยอดรวมจำนวนเงินของใบ PO คำนวณจาก PO.PA = (A : amount)

POi : หมายถึง ใบรายการขอชำระเงินของร้านค้าแต่ละร้าน ซึ่งมีรายการสินค้า และจำนวนที่ต้องจ่ายให้กับ Mi

Mi : หมายถึง พ่อค้า หรือใช้แทนด้วย IDMi

Tp : Timestamp หมายถึง วันที่และเวลาทำธุรกรรม

SK(x-y)j โดย (x-y) คือ คีย์ที่ใช้ร่วมกันระหว่าง เอนทิตี x กับ เอนทิตี y; j = 1..n

h (m,k) : หมายถึง การใช้ฟังก์ชันแฮชเข้ารหัสข้อความ m ที่ต่อกับ คีย์ k เพื่อใช้พิสูจน์ตัวตน

ARi : Authorization Request หมายถึงรายการร้องขอทำรายการแต่ละร้านค้า

ARi = (TID, IDC, IDMi ,TP, POi.PA, IDPSP-ACC-Mi) and (TID, IDC, IDMi, TP, POi.PA, IDPSP-ACC-C)

AR : Authorization Request หมายถึงรายการคำร้องขอทำรายการรวมทุกรายการ

ARSi Authorization Response หมายถึงคำตอบกลับของพ่อค้าแต่ละร้าน Mi

ARSi = (Status, TID, IDC, IDMi, POi.PA, TP, IDPSP-ACC-Mi) and (Status, TID, IDC, IDMi, POi.PA, TP, IDPSP-ACC-C)

ARS : Authorization Response หมายถึงคำตอบกลับรวมของทุกร้านค้า M'

IDPSP-ACC-x หมายถึง เลขบัญชีหรือบัตรเครดิตของสถาบันการเงินของเอนทิตี x เฉพาะ C กับ M' เท่านั้น Confirm Payment แจ้งยืนยันการทำรายการ

Status =(Y/N)หมายถึงสถานการณ์ทำรายการชำระเงิน

2) สมมติฐานของโพรโตคอลที่นำเสนอ

ก่อนเริ่มทำรายการใดๆ จะมีการแลกเปลี่ยนคีย์ที่ใช้ร่วมกันหรือเป็นคีย์คู่ โดยแต่ละคู่ต้องเก็บไว้เป็นความลับถือว่าเป็นคีย์ส่วนตัว มีคีย์คู่ดังนี้

C ⟶ M ได้แก่ SK(C-Mi)j

C ⟶ PSP ได้แก่ SK(C-PSP)j

M ⟶ PSP ได้แก่ SK(Mi-PSP)j

C ⟶ IN ได้แก่ SK(C-IN)j

IN ⟶ PSP ได้แก่ SK(IN-PSP)j

IN ⟶ M ได้แก่ SK(IN-Mi)j

นอกจากนี้ ยังมีการยืนยันตัวตนก่อนเริ่มทำรายการ คือ IN ⟶ C : {IDC, IDIN, h(IDC, IDIN,SK(C-IN)j)} Sk(C-IN) j

ตัวแทน ส่งข้อมูลการระบุรหัสลูกค้า รหัสของตัวแทนไปที่ C เพื่อยืนยันตัวตนโดยใช้ฟังก์ชันแฮช และเข้ารหัสลับด้วยเซสชันคีย์ที่ใช้ร่วมกันระหว่าง C กับ IN ในที่นี้หมายถึง SK(C-IN) j ทั้งนี้เพื่อเป็นการยืนยันตัวตนของผู้ส่งข้อมูลโดยเซสชันคีย์ และเพื่อการยืนยันว่าข้อมูลไม่ถูกแก้ไขโดยใคร โดยดูจากค่าของฟังก์ชันแฮชจากผู้ส่งเทียบกับฟังก์ชันแฮชในส่วนของผู้รับ คือ h(IDC, IDIN, SK(C-IN)j) ของผู้ส่งมีค่าเท่ากับ h(IDC, IDIN, SK(C-IN)j) ของผู้รับ

3) รายละเอียดของโพรโตคอล

การทำงานของโพรโตคอลมี 4 subprotocols ได้แก่ Payment Order, Payment Distribution Process, Authorization request, Authorization response, และ AR Distribution Process มีรายละเอียด ดังนี้

Payment Order PO:

1. C ⟶ IN: {(IDC, IDIN, TID, PO, IDMi , h(IDC, IDIN,TID, PO, IDM', SK(C-IN) j)), {IDC, TID, PO, IDMi, IDPSP-ACC-C , h(IDC, TID,

PO, IDMi, IDPSP-ACC-C , SK(C-PSP) j) }SK (C-PSP) j , {TID, PO, IDMi, IDPSP-ACC-Mi , h(IDC, TID, PO, IDMi, IDPSP-ACC-Mi , SK(C-Mi) j)}SK(C-Mi) j } SK(C-IN) j

อธิบายการทำงานขั้นตอนที่ 1

เมื่อลูกค้าได้รับใบแจ้งหนี้จากหนึ่งร้านค้าหรือหลายๆ ร้านค้าเพื่อชำระค่าสินค้าหรือบริการ ลูกค้าจะทำการส่งข้อมูลที่เกี่ยวกับการชำระเงินไปยังพ่อค้าและธนาคารเพื่อหักเงิน โดยส่งข้อความผ่านตัวแทน ข้อความที่ส่งมีทั้งหมด 3 ชุด คือ

1.1 (IDC, IDIN,TID, PO, IDMi , h(IDC, IDIN, TID, PO, IDMi, SK(C-IN) j) เป็นข้อมูลลูกค้าที่ส่งไปให้ตัวแทน ประกอบด้วย IDC, IDIN, TID, PO ,IDMi เป็นข้อมูลยืนยันรหัสลูกค้า รหัสร้านค้า และรายละเอียดในใบขอชำระเงิน โดยใช้ฟังก์แฮชและการเข้ารหัสลับข้อมูลด้วยคีย์ที่ใช้ร่วมกันระหว่าง C กับ IN

1.2 {IDC, TID, PO, IDMi, IDPSP-ACC-C, h(IDC,TID, PO, IDMi, IDPSP-ACC-C, SK(C-PSP)j) เป็นข้อมูลลูกค้าที่จะส่งให้PSP เช่น เลขบัตรเครดิต หรือเลขบัญชีสำหรับให้ PSP หักเงินชำระค่าสินค้าและบริการของร้านต่างๆ ตาม IDMi ที่ส่งมาในส่วนนี้ข้อมูลจะเป็นความลับ ผู้ไม่มีสิทธิ์ไม่สามารถถอดรหัสลับได้ ผู้ที่สามารถถอดได้มีเพียงผู้ที่รู้เซสชันคีย์ที่ใช้ร่วมกันเท่านั้น ในที่นี้ คือ PSP

1.3 {TID, PO, IDMi, IDPSP-ACC-Mi, h(IDC,TID, PO, IDMi, IDPSP-ACC-Mi , SK(C-Mi)j)} SK(C-Mi) j ส่วนนี้ลูกค้าส่งเลขบัญชีของร้านค้า และรายละเอียดการชำระเงินไปให้ร้านค้ายืนยัน ว่าถูกต้องหรือไม่ วิธีการนี้ โดยนำข้อความรายละเอียดการชำระเงิน ผ่านฟังก์แฮช และเข้ารหัสด้วยเซสชันคีย์ระหว่าง C และ Mi ผู้ที่สามารถถอดรหัสนี้ได้มีเพียง C กับ M เท่านั้น

Payment distribution Process:

2.IN ⟶ M:{((IDC, IDIN, TID, POi, IDMi , h(IDC, IDIN,TID, POi, IDM', SK(C-IN) j)), {IDC, TID, POi, IDMi, IDPSP-ACC-C, h(IDC,TID,

POi, IDMi, IDPSP-Acc-C , SK(C-PSP) j) }SK(C-PSP)j,
{IDC, TID, POi, IDMi, IDPSP-Acc-Mi,
h(IDC,TID, POi, IDMi, IDPSP-ACC-Mi , SK(C-Mi)j) }
SK(C-Mi) j,
h(((IDC, IDIN,TID, POi, IDMi, h(IDC,IDIN,TID,
POi, IDMi, SK(C-IN) j)),
{IDC,TID, POi, IDMi, IDPSP-ACC-C, h(IDC,TID,
POi, IDMi, IDPSP-ACC-C , SK(C-PSP) j) }SK(C-PSP) j,
{IDC, TID, POi, IDMi, IDPSP-ACC-Mi, h(IDC,TID,
POi, IDMi, IDPSP-Acc-Mi, SK(C-Mi)j)}SK(C-Mi)j,
SK(IN-Mi)j)} SK(IN-Mi) j

อธิบายการทำงานขั้นตอนที่ 2

IN รับข้อมูลจาก C และทำการส่งต่อไปให้ M โดยนำข้อมูลทั้งหมดที่รับมาผ่านฟังก์ชันแฮช และเข้ารหัสลับด้วยคีย์ที่ใช้ร่วมกันระหว่าง IN กับ Mi ข้อมูลที่ส่งมาเป็นรายละเอียดของรายการชำระเงิน ได้แก่ IDC,TID, POi, IDMi IDPSP-Acc-Mi เป็นข้อมูลที่พ่อค้าเรียกเก็บกับลูกค้า ซึ่งลูกค้าได้แจ้งความจำนงเพื่อชำระหนี้พร้อมแจ้งเลขบัญชีธนาคารของพ่อค้าที่จะโอนเงินให้พ่อค้าตรวจสอบ รายการที่ส่งมาว่าเป็นรายการของร้านตัวเองจริง โดยดูจากข้อมูลที่ส่งมาถูกเข้ารหัสโดยรหัสที่แชร์กันระหว่าง C-Mi ซึ่งยืนยันได้ว่าเป็นข้อมูลที่ถูกต้อง และส่งมาโดยผู้มีสิทธิ์จริง รวมทั้งพิจารณาจากข้อมูลในใบ PO

Authorization request from M to PSP

3.M ⟶ IN: {{ConfirmPayment}SK(Mi-PSP)j}, TID, IDC, I

DMi, ARi }SK(Mi-IN) j+1

ARi = { (TID, IDC, IDMi, TP, POi.PA, IDPSP-ACC-Mi),

h((TID, IDC, IDMi, TP, POi.PA, IDPSP-ACC-Mi),SK (Mi-PSP)j)}SK(Mi-PSP)j and

{(TID, IDC, IDMi, TP, POi.PA, IDPSP-ACC-C),
h((TID, IDC, IDMi ,TP, POi.PA, IDPSP-ACC-C),
SK(C-PSP)j)}SK(C-PSP)j

อธิบายการทำงานขั้นตอนที่ 3

เมื่อพ่อค้าตรวจสอบข้อมูลการขอชำระเงินของลูกค้าแล้วว่าเป็นข้อมูลจริง ตรงกับข้อมูลของร้านค้า จึงยืนยันการทำรายการโดยส่งคำร้องขอไปยัง PSP เพื่อให้หักเงินจากร้านค้า โดยส่งข้อความผ่าน IN โดยกำหนดให้รายละเอียดการชำระเงินใน ARi ประกอบด้วยส่วนที่ส่งมาจาก M คือ TID, IDC, IDMi, TP, POi.PA, IDPSP-ACC-Mi และส่วนที่ C ส่งฝากมากับ M ได้แก่ TID, IDC, IDMi , TP, POi.PA, IDPSP-ACC-C ในที่นี้ M ไม่สามารถรู้เลขบัญชีของลูกค้า เพราะทำการเข้ารหัสด้วยคีย์ที่ใช้ร่วมกันระหว่าง C กับ PSP เพราะฉะนั้น มีเพียง C กับ PSP เท่านั้นที่ถอดได้

4.IN ⟶ PSP: {{ConfirmPayment}SK(Mi-PSP) j, TID, IDC,

IDMi, AR, h(({ConfirmPayment}SK(Mi-PSP) j,
TID, IDC, IDMi, AR), SK(IN-PSP) j)} SK(IN-PSP) j
AR = {ARi}

อธิบายการทำงานขั้นตอนที่ 4

IN ส่งต่อข้อมูลจาก Mi ไปยัง PSP เพื่อยืนยันการทำรายการหักบัญชีจากบัญชีลูกค้าไปยังบัญชีของพ่อค้า ซึ่งข้อมูลที่ส่งมาจาก IN ทั้งหมดเข้ารหัสลับด้วยคีย์ที่ใช้ร่วมกันระหว่าง IN และ PSP เมื่อถอดรหัสลับแล้ว PSP สามารถถอดรหัสข้อมูลที่บรรจุใน ARi ได้ ซึ่งเป็นรายละเอียดการขอชำระเงินที่ส่งมาจากลูกค้า และร้านค้าซึ่งมีการยืนยันข้อมูลตรงกันแล้ว จากนั้น PSP ทำการหักเงินตามรายการในใบ PO

Authorization Response from PSP to C and Mi

5.PSP⟶IN: {(Status, TID, Tp, PO.PA, ARS) , h((Status,
TID, Tp, PO.PA, ARS), SK(IN-PSP) j+1)} SK(IN-PSP)j+1
ARS= {(ARSi), h((ARSi), SK(IN-PSP) j+1 }SK(IN-PSP) j+1

ARSi = {(Status, TID, IDC, IDMi, POi.PA, Tp,
IDPSP-ACC-Mi), h((Status, TID, IDC,
IDMi, POi.PA, Tp, IDPSP-ACC-Mi), SK(Mi-PSP)
j+1)} SK(Mi-PSP) j+1
and {(Status, TID, IDC, IDMi, POi.PA, Tp,
IDPSP-ACC-C) , h((Status, TID, IDC, IDMi,
POi.PA, TP, IDPSP-ACC-C), SK(C-PSP) j+1)}
SK(C-PSP) j+1

อธิบายการทำงานขั้นตอนที่ 5

เมื่อ PSP ทำรายการหักเงินตามที่ C ร้องขอแล้ว จึงทำการส่งรายการข้อมูลยืนยันการหักเงินจากบัญชีของ C ไป M และแจ้งไปยัง C และ M โดยส่งผ่าน IN

Authorization Response Distribution Process From IN to C and IN to M:

6. IN ⟶ C: {ARS, h(ARS, SK(IN-C) j+1) } SK(IN-C) j+1
IN ⟶ M: {ARSi, h(ARSi, SK(IN-Mi) j+1) }SK(IN-Mi) j+1

อธิบายการทำงานขั้นตอนที่ 6

IN รับข้อมูลจาก PSP และส่งรายละเอียดการชำระเงินกลับไปให้ C และ M ซึ่งแต่จะเอนทิตีจะสามารถถอดรหัสลับข้อมูลได้ในส่วนที่มีคีย์ที่ใช้ร่วมกันกับ IN เท่านั้น

จากการเปรียบเทียบโพรโตคอลที่นำเสนอและโพรโตคอลในลักษณะเดียวกัน ได้ผลลัพธ์ตารางที่ 1

ตารางที่ 1 เปรียบเทียบคุณลักษณะของโพรโตคอล

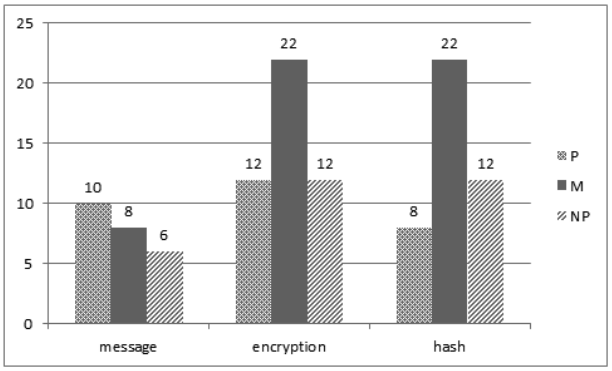
โพรโตคอล	วิธีการ	จำนวนข้อความ	อัตราส่วนเทียบกับ NP	ความสัมพันธ์ c:m	จำนวนเข้ารหัส	จำนวนแฮช
M. Carbonell	Asym	8	1.33	1:m	22	22
P. Limpittaya	Sym	10	1.66	1:1	12	8
NP. Propose	Sym	6	1.00	1:m	12	12

Asym : Asymmetric key, Sym : Symmetric key

ในตารางที่ 1 โพรโตคอลของ P. Limpittaya และคณะ (P. Limpittaya, M. Warasat, S. Kungpisdan, 2012) เป็นโพรโตคอลสำหรับชำระค่าสินค้าแบบผ่านตัวแทน แบบทำรายการระหว่างลูกค้ากับพ่อค้าได้ครั้งละ 1 รายการ (1 : 1) โดยมีจำนวนข้อความในส่วนชำระเงิน (bill payment) จำนวน 1 ข้อความ ส่วนโพรโตคอลของ M. Carbonell et al. (M. Carbonell, J. Torres, D. Suarez., 2008) เป็นโพรโตคอลชำระค่าสินค้าและบริการผ่านตัวแทน แบบ (1 : m) มีจำนวนข้อมูลในการส่งต่อ 1 รายการ 8 ข้อความ ส่วนโพรโตคอลที่นำเสนอ มีข้อความสั้นกว่าคือ 6 ข้อความ ถ้าคิดเป็นสัดส่วนน้ำหนักของข้อความระหว่าง 3 โพรโตคอล คือ โพรโตคอล ที่นำเสนอ (NP) โพรโตคอลของ M. และ P. เป็น 1 : 1.33 : 1.66 ซึ่งแสดงว่าโพรโตคอลที่นำเสนอมีน้ำหนักเบากว่าทั้งสองโพรโตคอล ส่วนประเด็นอื่นคือ Operator สำหรับการเข้ารหัส และจำนวนฟังก์ชันแฮชที่ใช้มีสัดส่วน NP : M : P คือ 12 : 22 : 12 และ 12 : 22 : 8 ตามลำดับ กราฟเปรียบเทียบจำนวนข้อความ จำนวนการเข้ารหัสและฟังก์ชันแฮช ดังรูปที่ 3

บทสรุป

ปัญหาด้านความมั่นคงปลอดภัยของระบบการชำระเงินผ่านโทรศัพท์มือถือ เป็นปัญหาหนึ่งที่นักวิจัยให้ความสนใจ และหาแนวทางแก้ไขอย่างต่อเนื่อง ซึ่งผู้วิจัยได้ทำการศึกษาโพรโตคอลที่เกี่ยวข้อง และวิเคราะห์เทคนิควิธีการที่ทำให้ข้อมูลมีความมั่นคงปลอดภัยสูง รวมทั้งแนวทางในการนำไปประยุกต์ใช้เป็นแนวทางนำสู่การพัฒนาโพรโตคอลใหม่ในรายงานนี้ ในรายงานวิจัยที่นำเสนอนี้ เป็นการออกแบบโพรโตคอลสำหรับชำระเงินผ่านโทรศัพท์มือถือ โดยใช้วิธีการเข้ารหัสลับแบบสมมาตร ร่วมกับฟังก์ชันแฮช โดยเน้นออกแบบให้โพรโตคอลมีจำนวนข้อมูลที่วิ่งในระบบน้อยมีน้ำหนักเบาเพื่อให้เหมาะกับการประยุกต์ใช้บนโทรศัพท์มือถือ



รูปที่ 3 เปรียบเทียบจำนวนข้อความของสามโพรโตคอล

หรือเครือข่ายไร้สาย โพรโตคอลที่ออกแบบสามารถลดจำนวนข้อมูลในระบบลงได้เมื่อเทียบกับโพรโตคอลอื่นที่ทำงานในลักษณะเดียวกันคือโพรโตคอลของ P. Limpittaya และคณะ มีจำนวนข้อมูลวิ่งในระบบจำนวน 10 Message ส่วนโพรโตคอลของ M. Carbonell และคณะ มีจำนวนข้อมูลวิ่งในระบบ 8 Message ซึ่งวิธีการที่นำเสนอนี้จะลดจำนวนโพรโตคอลลงเหลือเพียง 6 Message ซึ่งน่าจะมีความเร็ว หรือใช้ทรัพยากรน้อยกว่าทั้งสองโพรโตคอล อย่างไรก็ตามวิธีการวัดประสิทธิภาพของโพรโตคอลยังไม่มีมาตรฐานที่ชัดเจน ซึ่งต้องมีการวิจัยและพัฒนาต่อไป ทั้งนี้ผู้วิจัยมีเป้าหมายมุ่งพัฒนาวิธีการทดสอบประสิทธิภาพของโพรโตคอลใน scenario ที่แตกต่างกัน โดยศึกษาวิเคราะห์และออกแบบวิธีการวัดประสิทธิภาพความปลอดภัยของโพรโตรคอลสำหรับการทำธุรกรรมอิเล็กทรอนิกส์ และเปรียบเทียบประสิทธิภาพโพรโตคอลที่นำเสนอกับโพรโตคอลอื่นๆ รวมทั้งศึกษาโมเดลสำหรับการทำธุรกรรมอิเล็กทรอนิกส์ที่มีการประยุกต์ใช้งานร่วมกับระบบพิกัดรองรับความต้องการในอนาคต

เอกสารอ้างอิง

C. Sekhar, Sarvabhatla. **Secure Lightweight mobile payment protocol using symmetric key techniques**, International Conference on Computer Communication and Informatics (ICCCI), 2012.

D. M. Tripathi , Ojha, A. **LPMP: An Efficient Lightweight Protocol For Mobile Payment**, National Conference on Emerging Trends and Applications in Computer Science (NCETACS) 3rd, 2012. Juniper, http://juniperresearch.com/viewpresselease.php?pr=327, july 11, 2016.

J. T. Isaac, S. Zeadally, **An Anonymous Secure Payment Protocol in a Payment Gateway Centric Model**, The 9th International Conference on Mobile Web Information System (MobiWIS), Published by Elsevier Ltd. 2012.

Matthew B. Gross, Jeanne M. Hogarth, and Maximilian D. Schmeiser (2012), **Consumers and Mobile Financial Services**, Report (Washington: Board of Governors of the Federal Reserve System, March), www,fedralreserve.gov/econresdata/mobile-devices/files/mobile-device-report-201203.pdf, july 10, 2016.

M. Bellare and J. A.Garay, **Design Implementation, and Deployment of the iKPSecure electronic Payment System**, IEEE Journal on SELECTED AREAS IN COMMUNICATIOINs, VOL. 18, NO. 4, APRIL 2000.

M. Carbonell, J. Torres, D. Suarez**, Secure E-Payment Protocol With New Involved Entity**, IEEE, 2008.

M. V. Alizadeh Dizaj, R.A. Moghaddam, Samad Momenebellah. **New mobile payment protocol: Mobile Pay Center Protocol 2 (MPCP2) By using new Key agreement protocol: VAM**, International Conference on Electronics Computer Technology (ICECT), 2011 3rd.

P. Limpittaya, M. Warasat, S. Kungpisdan, **Design and Analysis of A Secure Agent-based Mobile Bill Payment Protocol for Bulk Transactions**, 2012 Ninth International Joint Conference on Computer Science and Software Engineering (JCSSE).

P. S. Auala, H. Arora. **A Secure Account based Mobile Payment Protocol with Public Key Cryptography and Biometic Characteristics**, International Journal of Science and Research (IJSR), India online ISSN: 2319-7064, Volume 2 Issue3, March 2013.

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

S. Kungpisdan, B. Srinivasan, Le. Phu Dung Le. **A secure Account-based Mobile Payment protocol**, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004)

S. M. Shedid. **Modified SET Protocol for Mobile Payment**, Proceeding of the international Conference Journal of Computer Science And Network Security, Vol.10 no.7, pp.289-295 July 2010.

T. S. Fun , L. Y. Beng , Likoh, J. , Roslan, R. **A lightweight and private mobile payment protocol by using mobile network operator**, Proceedings of the International Conference on Computer and Communication Engineering 2008 May 13-15, 2008 Kuala Lumpur, Malaysia.

T. S. Fun, L. Y. Beng, and M. N. Razali, **Review of Mobile Macro-Payments Schemes**, Journal of Advances in Computer Networks, Vol. 1. No. 4, December 2013.

Y. Li and Y. Wang, **Secure Electronic Transaction (SETProtocol)**, http://people.dsv.su.se/~matei/courses/IK2001_SJE/ li-wang_SET.pdf, July 10, 2014.