JIST Journal of Information Science and Technology
Volume 10, NO 2 | JUL – DEC 2020 | 10-18
ISSN: 2651-1053 (Online)
ISSN: 1906-9553 (Print)

# Mobile Payment: A Review

*Surakarn Duangphasuk[1], Chalee Thammarat[1*] and Supakorn Kungpisdan[2]*

*[1]Faculty of Information Science and Technology, Mahanakorn University of Technology*

*[2]RV Connex Co.,Ltd.*

**Received**: June 14, 2020; **Revised**: September 30, 2020; **Accepted**: October 4, 2020; **Published**: December 22, 2020

**ABSTRACT – Currently, online business, especially e-commerce where buying and selling of goods and/or services are via the Internet, is being used widespread. It allows people to buy goods and/or services from anywhere at any time and get delivery to any location. Mobile commerce is one of the most popular types of electronic commerce. In this paper, we propose a literature review of current research results obtained by specialists and researchers area of the mobile payment.**

**KEYWORDS:** Mobile Payment, Review, Literature Review, Mobile Payment Security

## 1. Introduction

During the past years, individuals can buy goods and/or services from home, at anytime from anywhere. They can operate to buy goods and/or services via wireless technologies through mobile devices. Wireless technologies and mobile device technologies raise electronic commerce (e-commerce) [1]. Presently, mobile devices have the ability and speed to support mobile applications. According to [2], mobile devices are shipped annually than personal computers (PCs). Moreover, mobile devices now can serve to pay for goods and/or services employing the transmission of information of the transaction [3]. One major factor that drives the success of mobile commerce (m-commerce) is mobile payments (m-payment). According to [4] users of m-payment will increase 448 million of the worldwide.

## 2. Characteristics of Mobile Payment

According to [5, 6], the conditions of the mode of payment in the electronic commerce for a mobile payment service can become acceptable following lists:

- Simplicity and Usability: The mobile payment applications should be a user friendly interface. The learning curve of the mobile payment applications must be closed to zero.
- Universality: Mobile payment systems should support universal payment services including person-to-person (P2P), government-to-person (G2P), business-to-consumer (B2C), and business-to-business (B2B).
- Interoperability: Universal standards and open technologies allow one to implement a system to interact with other systems.
- Security, Privacy and Trust: Mobile payment applications should be resistant to attacks from hackers and terrorists.
- Cost and Speed: Mobile payment systems should be cost-effective and less expensive compared with existing payment mechanisms.
- Cross-Border Payments: Mobile payment systems should be widely acceptable and globally accessible.

## 3. Summary of Existing Mobile Payment Methods

The detail of these methods can be described as below:

*Corresponding Author: chalee23@gmail.com

## 3.1 Payment Amount

- The payment amount for goods and/or services can be classified mobile payment methods as follows [7]: Pico-payments are transactions amount, is less than US$0.10.
- Micro-payments are transactions amounts between US$0.11 and US$10.
- Macro-payments are transactions amounts exceeding US$10.

## 3.2 Basis of Payment

- Account-based: Customers are associated with a specific account maintained by an Internet Payment Provider (IPP). IPP helps debits and credits that are exchanged during a transaction and that are periodically billed and pays for the balance of the account to it. Genially, this account is not suitable for pico-payments and micro-payments [8, 9]. This account-based payment has been proposed protocols in [10, 11].
- Token-based: In this account, before beginning making a transaction, the customers are necessary to transform his/her actual currency from his/her account into electronic format, i.e., tokens that are usually issued by a bank. A merchant will send to his/her acquire all the tokens collected to redeem the actual currency, which will be transferred to the account of the merchant [12]. Token-based is proposed in [13, 14].

## 3.3 Timing of Payment

To make payment goods and/or services via mobile payment can be performed at different times.

- Real-time (cash): In this payment timing is called real-time or cash-like payment that uses an electronic currency that is exchanged during a transaction like eCash and beenz [15]. Real-time is proposed protocols in [16, 17].
- Pre-paid (debit): In this payment timing is used by mobile network operators and can only be used by consumers capable of paying abruptly. Consumers must advance before they receive the product wanted [18]. This timing is suggested in mobile payment protocols [19, 20].
- Post-paid (credit): In this payment timing, consumers will receive the goods them before paying, for example, electronic checks and credit cards. At this time, the most common payment method is used in electronic commerce transactions [21]. This timing is recommended in mobile payment protocols [22, 23].

## 3.4 Location of Payment

Location for supporting payment can be categorized as following [24]:

- Remote transactions: A customer can perform transactions for paying goods independently of the users' location, such as tickets, digital cash, and peer-to-peer payments.
- Proximity/local transactions: A customer can perform transactions for paying goods with smartphone by using short-range communication messaging protocols like Bluetooth, infrared, RFID, and contactless chips.

## 3.5 Technologies Used for Mobile Payments

Many technologies to support mobile payment are proposed by several existing types of research that can group these technologies as described below:

- Short Message Service (SMS): It is a technology that enables the mobile device to exchange short text messages [25, 26] with other network-connected devices that is less than 160 alphanumeric characters. SMS is now available on a wide range of networks. In mobile payment, SMS can be used mobile payments, mobile banking, voting or even for sharing opinions on some activities. [25, 26] proposed security issues including eavesdropping and modifying, stealing mobile stations, spoofing, man-in-middle attack, replay attack, message disclosure, and denial of service (DoS) attacks.
- Biometric Technology: It is a technology that uses to identify, and verification people like, such as the face, finger, hand, iris, and voice recognition. Moreover, this technology uses a biometric payment system that is very safe, secure, and easy to use and the user does not even need to remember any password or secret codes [27, 28].
- 2-D Barcode Technology: It is a technology that is linear barcodes to encode numbers and letters in a sequence of varying width bars and spaces. A computer can read, retrieve, process, and validate. The advantages of barcode are fast and precise. Moreover, it enters the data without keyboard data entry [29].

- Near Field Communication (NFC): It is a wireless communications technology based on radio frequency at 13.56 MHz [30, 31]. It can transmit data within a range of 10 cm. The maximum transmission speed is 424 kbps as defined by ISO 14443. NFC devices can perform fast pairing with other devices and consume low energy. NFC is currently used for transmitting a small amount of data within a short range. There are two communication modes passive mode and active mode [32]. There are three operating modes including card emulation mode, reader/writer mode and peer-to-peer (P2P) mode [33]. Some researches discussed flaws of NFC, especially the fact that NFC was implemented by focusing mainly on the speed of communications, instead of security properties. Furthermore, NFC does not provide encryption of data transmitted at the hardware level. The results in several security threats like eavesdropping, data manipulation, relay attack, man-in-the-middle attack, and denial of service. Several techniques were proposed to provide secure mobile payments of transactions over NFC [34-36].
- Radio Frequency Identification (RFID): It is a technology that is developed during the 80's for non-contact reading. There are three components of RFID chip, including an antenna, a transceiver, and a transponder. This technology uses radio frequency (RF) signals to exchange data between a reader and an electronic tag. Some applications have been used, containing animal tracking, automatic toll collection, access control systems, mobile payment, and supply-chain management [37].
- Session Initiation Protocol (SIP): It is a technology that is application-layer control protocol. SIP can establish, modify, and terminate sessions for voice and video calls over the Internet Protocol (IP) [38]. SIP can implement and deploy to support mobile payment by the mobile phone network.

# 4. Mobile Payment Systems

A mobile payment system consists of engaging parties, primitive transactions, and payment transactions. The details these transactions can describe as below [39-41]:

## 4.1 Engaging Parties

1) Client (C): A client is a party that would like to purchase goods and/or services from the merchant. This party uses a mobile device to purchase goods and/or services from the merchant.

2) Merchant (M): A merchant is a party that has goods and/or services to sell.

3) Acquirer (A): An acquirer is a party that has the merchant's account (the merchant's financial institution). It manages the merchant's account and affords the electronic payment instruments.

4) Issuer (I): An issuer is a party that has the client's account (the client's financial institution). It manages the client's account and affords the electronic payment instruments.

5) Payment Gateway (PG): A payment gateway is a party that provides performing payment transactions on behalf of the issuer (the client's financial institution) the acquirer (the merchant's financial institution). The payment gateway, and the issuer operates on behalf of the issuer and the acquirer on the Internet side

## 4.2 Primitive Transactions

- Payment-order: This is the activity between the client and the merchant, in which the client asks the merchant to purchase goods and/or services.
- Debit: This is the activity between the client and the issuer (via the payment gateway). It is made by the client to request the issuer to deduct the amount from the account of the client.
- Credit: This is the activity between the merchant and the acquirer (through the payment gateway). The merchant makes it in order to transfer the requested amount to the account of the merchant.
- Payment-clearing: This is the activity between the issuer and the acquirer in order to transfer the amount requested by the client and the merchant between their accounts (via the payment gateway).

## 4.3 Payment Transaction

A number of the payment protocols [39, 40] are depended on the details of payment transactions in the following step:

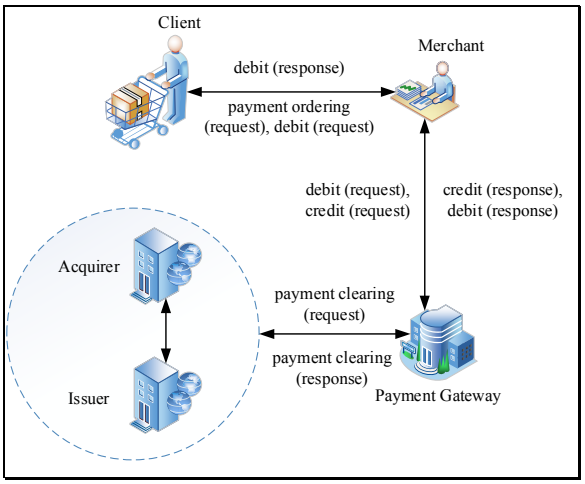


*Figure 1. Mobile Payment System.*

From Figure 1 shows transaction flow between parties of the mobile payment system.

**C → M:** *payment ordering (request), debit (request)*

**M → PG:** *debit (request), credit (request)*

**PG ↔ I, A:** *payment clearing (request), payment clearing (response)*

**PG → M:** *credit (response), debit (response)*

**M → C:** *debit (response)*

The above transaction shows the flowing of the payment transaction. Payment ordering will request from the client to the merchant together the request debit. Then, the merchant will request the payment gateway to debit and credit request. Next, the payment gateway will process from the issuer to the acquirer in payment clearing. Afterward, the payment gateway will send back credit response and debit response to the merchant, and then the merchant will forward the debit response to the client. Note that the payment gateway will act as an intermediary between the client and the merchant, and the issuer and the acquirer. So debit and credit will be performed through the payment gateway.

# 5. Classification of Mobile Devices

Mobile devices have potent functions. A user can use mobile devices to watching movies, listening to music, access to the Internet, gaming, payment, and so on. We can classify mobile devices shown below [42]:

## 5.1 Notebooks

It is equipment that small size and a portable computer that has powerful functions both computing and storage. This device can install operating systems, whereas other devices execute more lightweight operating systems.

## 5.2 Tablets

It is equipment that is a tiny notebook and works as a smartphone. This device has touch screens, digital pen, or fingertip instead of a keyboard or mouse. Moreover, some models are bigger than a smartphone.

## 5.3 Mobile Phones

It is equipment that is capable only receive telephone calls, send and receive text messages. This device is also known as a cellular phone, cell phone, or headphone.

## 5.4 Smartphones

It is equipment that is a small notebook and tablet. This device can install the application by running its complete operating system that is similar to the notebook and is equipped with cameras, accelerometers, and touch screens that need to be operated with a stylus, digital pen, and so on.

# 6. Existing Mobile Payment Protocols

In this section, we present a literature review of mobile payment protocols. The details of mobile payment protocols can explain as below.

[16] offered a payment protocol uses purchase an electronic commodity (software or a movie) from an on-line shop with electronic cash via a computing-capable device (a PC, notebook, or smartphone, connected to the Internet). This protocol includes five sub protocols: withdrawal protocol, payment protocol, change protocol, deposit protocol, and revocation protocol. There are three parties, including customers, shops and banks. The main security properties of this protocol like customer anonymity and unforgeability.

[17] proposed a novel electronic cash protocol. It is building electronic cash data as chain of transaction (or blockchain). The proposed protocol can work without proper network infrastructure. This protocol

applies identity based signcryption to provide its security of the protocol such as against forgery and double spending. There are six sub protocols: setup protocol, extract protocol, withdraw protocol, transaction protocol, dispute protocol, and settlement protocol.

[19] presented a fairness protocol for mobile payment based on Short Message Service (SMS) infrastructure. Cryptographic algorithms are used this protocol, including symmetric key encryption, and hash function. The protocol is based on the secure session key generation technique to enhance transaction security (security properties include confidentiality, integrity, mutual authentication, and nonrepudiation) and lightweight property. The proposed protocol consists four parties: a client, a merchant, a mobile operator (or payment gateway), and a trusted third party. There are four phases: Registration Phase, Purchase Credit Request Phase, Making Payment Phase, and Dispute Resolution Phase.

[20] submitted fair exchange model and protocol for mobile payment. In this model includes a client, a merchant, an issuer, an acquirer, a payment gateway, and a trusted third party. The trusted third party keeps all transactions occurred between parties for later verification. The session key generation technique is utilized to ensure security and fairness. There two sub protocols: Purchase Credit, and Request Making Payment. The mobile payment system is composed of four engaging parties: a client, a merchant, a verifier (or the trusted third party), and a mobile operator. In the Purchase Credit, this sub protocol is activity between the client and the mobile operator to the client top-up cash card. In the Request Making Payment, this sub protocol is activity between the client, the merchant, and the mobile operator to perform payment ordering, credit, debit and payment clearing.

[22] suggested a private mobile payment protocol called New mobile payment protocol: Mobile Pay Center Protocol (MPCP). The client centric model is used for this protocol. Symmetric key encryption and hash function are used to secure transactions. The proposed protocol not only decreases the computational operations and communications between the parties, but also achieves security properties like transaction privacy for the payer, and replay attacks. There are five engaging parties, a payer, a payee, payer's mobile network operator, payee's mobile network operator. The sub protocol of this protocol consists of registration protocol and payment protocol. In the registration protocol, the objective of this protocol to share session key between the payer and payer's mobile network operator, and share session key between the payee and payee's mobile network operator. In the payment protocol, the objective of this protocol to pay goods or service between the payer and the payee via payer's mobile network operator, and payee's mobile network operator.

[23] proffered mobile payment protocol based on symmetric key algorithm which is a lightweight mobile payment protocol. The proposed protocol ensures anonymity and unlinkability of the merchant. In this protocol, engaging parties comprise of four entities: a payer, a payee, payer's MNO, payee's MNO, and Mobile Network Operator (MNO) stands for the financial institution of the issuer and the financial institution of the acquirer. There are two sub protocols, including registration protocol and payment protocol. There are seven phases the payment protocol: Payment Initialization, Payment Subtraction Request, Payment Authorization Request, Payment Confirmation Request, Payment Confirmation Response, Payment Authorization Response, and Payment Subtraction Response or Payment Receivable Updates. This protocol ensures security properties like confidentiality, authentication, integrity, non-repudiation, anonymity, privacy and unlinkability.

[34] recommended fairness near□field communication (NFC) mobile payment protocol. The protocol uses both symmetric key encryption and asymmetric key encryption including hash function. Moreover, the proposed protocol uses offline session key generation technique to enhance the security of transactions and the lightweight property. Not only Burrows, Abadi and Needham (BAN logic) but also the Scyther tool are utilized to verify security of in this protocol. This proposed protocol is designed to resist attacks like double□spending, man□in□the□middle attacks, and replay attacks and provide security properties such as confidentiality, integrity, and authentication. In addition, the main aim of this proposed protocol is strong fairness for all parties of the transactions.

[35] introduced Near Field Communications (NFC) mobile payment protocol. The protocol satisfies not only fair exchange, but also sale transaction security. Moreover, this protocol uses offline session key generation and distribution to secure the security of sale transactions, and lightweight property. Secure security of sale transactions includes security properties like confidentiality of transactions, mutual authentication of transactions, and non-repudiation of transactions, and resistance to attack such as brute force attacks, double-spending detection, replay attack prevention, and man-in-the-middle attacks.

[36] proposed mobile payment protocol named Untraceable and Anonymous Mobile Payment Scheme Based on Near Field Communication (NFC). There are six features in the proposed protocol. Firstly, user authentication uses password-based authentication using low-entropy password. Secondly, convenience is compatible with EuroPay, MasterCard and Visa (EMV-compatible) based on NFC-enabled devices. Thirdly, efficiency of protocol does not use the public key cryptography and the private key cryptography. But the protocol applies symmetric key cryptography to provide confidentiality of transactions to reduce computational cost of protocol. Fourthly, the anonymity of protocol utilizes virtual accounts in the online shopping processes to prevent to disclose user information. Fifthly, untraceablity of protocol cannot trace a transaction by using virtual accounts that are re-new each transaction. Finally, either encryption or signing of the sender can provide confidentiality and authenticity.

# 7. Security in Mobile Payment Systems

## 7.1 Authentication

This is a security property related to identification. This function applies to both entities and transactions itself. Two parties entering into a communication should identify each other. Transaction delivered over a channel should be authenticated as to origin, date of origin, data content, time sent.

## 7.2 Confidentiality

This is a security property used to keep the content of transaction from all but those authorized. Preserving authorized restrictions on transaction access and disclosure, including means for protecting personal privacy and proprietary transaction. A loss of confidentiality is the unauthorized disclosure of transaction.

## 7.3 Integrity

This is a security property which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties.

## 7.4 Authorization

This is a security property which provides allowing access to specific services and/or resources, and allows that the user can make the requested transactions.

## 7.5 Non-repudiation

This is a security property which prevents an entity from denying previous commitments or actions. The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, a message, or message originator.

## 7.6 Anonymity and Unlinkability

This is hide user's real identity in the payment procedure or is unable to know their transaction records.

## 7.7 Privacy

This is concerned without revealing payment information and goods description like credit card numbers or bank account in the transaction.

## 7.8 Background Concepts in Cryptography

Cryptography is the study of mathematical techniques related to aspects of transaction security. Cryptography is an effective way of protecting sensitive transaction as it is stored on media or transmitted through network communication paths [43].

- Symmetric Cryptography: Symmetric encryption, also referred to as conventional encryption or single-key encryption. The sender and the recipient using symmetric same algorithms. The sender and the recipient use the same key for encryption and decryption functions.
- Public Key Cryptography: Public key encryption, each entity has different keys or asymmetric keys. The two different asymmetric keys are mathematically related. If a message is encrypted by one key, the other key is required to decrypt the message. The pair of keys is made up of one public key and one private key. The public key can be known to everyone, and the private key must only be known to the owner. The public and the private keys are mathematically related, but cannot be derived from each other.
- Hash Function: A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called hash-values. One of the fundamental primitives in

modern cryptography is the cryptographic hash function, often informally called a one-way hash function. A one-way hash is a function that takes a variable-length string, a message, and compresses and transforms it into a fixed-length value referred to as a hash value. A hash value is also called a message digest.

## 8. Mobile Payment Comparison

In this section, we will compare mobile payments that are up to date in this research topic. The details shown as below:

*Table 1. Comparison of Mobile Payment.*

| Protocol | Payment Type | Timing | Location |
|---|---|---|---|
| [16] | Token-based | Real-time | Remote |
| [17] | Token-based | Real-time | Remote |
| [19] | Token-based | Pre-paid | Remote |
| [20] | Token-based | Pre-paid | Remote |
| [22] | Token-based | Pre-paid/Post-paid | Remote |
| [23] | Token-based | Pre-paid/Post-paid | Remote |
| [34] | Token-based | Post-paid | Proximity/local |
| [35] | Token-based | Post-paid | Proximity/local |
| [36] | Token-based | Post-paid | Proximity/local |

From table 1, it can be seen that token-based, post-paid and remote presently are used for mobile payment systems.

## 9. Conclusion and Discussion

In this paper, we discussed the overall of mobile payment systems including characteristics of mobile payment, summary of existing mobile payment methods, technologies used for mobile payments, mobile payment system, classification of mobile devices, and security in mobile payment systems. This paper summarizes from current research results obtained by specialists and researchers area of the mobile payment.

## References

[1] E. W. Ngai, and A. Gunasekaran, “A review for mobile commerce research and applications,” Decision support systems, vol. 43, no. 1, pp. 3-15, 2007.

[2] Z. S. Chen, R. Li, X. Chen, and H. Xu, “A survey study on consumer perception of mobile-commerce applications,” Procedia Environmental Sciences," vol. 11, pp. 118-124, 2011.

[3] F. Liébana-Cabanillas, I. Ramos de Luna, and F. Montoro-Ríos, “Intention to use new mobile payment systems: a comparative analysis of SMS and NFC payments,” Economic research-Ekonomska istraživanja, vol. 30, no. 1, pp. 892-910, 2017.

[4] T. Falk, W. H. Kunz, J. J. Schepers, and A. J. Mrozek, “How mobile payment influences the overall store price image,” Journal of Business Research, vol. 69, no. 7, pp. 2417-2423, 2016.

[5] S. Karnouskos, “Mobile payment: a journey through existing procedures and standardization initiatives,” IEEE Communications Surveys & Tutorials, vol. 6, no. 4, pp. 44–66, 2004.

[6] N. Iman, “Is mobile payment still relevant in the fintech era?,” Electronic Commerce Research and Applications, vol. 30, pp. 72-82, 2018.

[7] G. Me, M. A. Strangio, and A. Schuster, "Mobile local macropayments: Security and prototyping," IEEE Pervasive Computing, vol. 5, no. 4, pp. 94-100, 2006.

[8] J. Gao, J. Cai, K. Patel, and S. Shim, "A wireless payment system," The 2nd. Conf. Embedded Software and Systems, pp. 8, 2005.

[9] S. Nambiar, C.T. Lu, and L.R. Liang, "Analysis of payment transaction security in mobile commerce," Proc. Information Reuse and Integration, pp. 475-480, 2004.

[10] I. C. Lin, and C. C. Chang, “A practical electronic payment system for message delivery service in the mobile environment," Wireless Personal Communications, vol. 42, no.2, pp. 247-261, 2007.

[11] J. T. Isaac, and J. S. Camara, "An anonymous account-based mobile payment protocol for a restricted connectivity scenario," The 18th. Int. Conf. Database and Expert Systems Applications, pp. 688-692, 2007.

[12] W. Guo, "Design of architecture for mobile payments system," Int. Conf. Control and Decision Conference, pp. 1732-1735, 2008.

[13] N. C. Liebau, V. Darlagiannis, A. Mauthe, and R. Steinmetz, "Token-based accounting for p2p-systems," Int. Conf. Kommunikation in Verteilten Systemen, Berlin, Heidelberg, 2005.

[14] R. Borgohain, M. T. Singh, C. Sakharwade, and S. Sanyal, "TSET: Token based secure electronic transaction," 2012.

[15] J. T. Isaac, and Z. Sherali, "Secure mobile payment systems," IT Professional, vol. 16, no. 3, pp. 36-43, 2014.

[16] L. Batten, and X. Yi, "Off-line digital cash schemes providing untraceability, anonymity and change," Electronic Commerce Research, pp. 1-30, 2018.

[17] D. E. Saputra, S. Sutikno, and S. H. Supangkat, "Peer-to-peer electronic cash using identity based signcryption," International Journal on Electrical Engineering and Informatics, vol. 10, no. 2, pp. 384-394, 2018.

[18] D. Flood, T. West, and D. Wheadon, "Trends in mobile payments in developing and advanced economies," RBA Bulletin, pp. 71-80, 2013.

[19] C. Thammarat, and W. Kurutach, "A secure fair exchange for SMS-based mobile payment protocols based on symmetric encryption algorithms with formal verification," Wireless Communications and Mobile Computing, vol. 2018, pp. 1-21, 2018.

[20] C. Thammarat, R. Chokngamwong, C. Techapanupreeda, and S. Kungpisdan, "A secure SMS mobile payment protocol ensuring fair exchange," the 29th Int. Conf. Circuit/Systems Computers and Communications, pp. 163-166, 2014.

[21] P. Pukkasenung, and R. Chokngamwong, "Review and comparison of mobile payment protocol," Int. Conf. Advances in parallel and distributed computing and ubiquitous services, pp. 11-20, 2016.

[22] M. V. Alizade, R. A. Moghaddam, and S. Momenebellah, "New mobile payment protocol: Mobile pay center protocol (MPCP)," The 3rd Int. Conf. Electronics Computer Technology, pp. 74-78, 2011.

[23] F. Zamanian, H. and Mala, "A new anonymous unlinkable mobile payment protocol," Int. Conf. Computer and Knowledge Engineering, pp. 117-122, 2016.

[24] E. Ramezani, "Mobile payment," Lecture E-Business Technologies, BCM1, 2008.

[25] J. L. C. Lo, J. Bishop, and J. H. Eloff, "SMSSec: An end-to-end protocol for secure SMS," Computers & Security, vol. 27, no. 5-6, pp. 154-167, 2008.

[26] H. Rongyu, Z. Guolei, C. Chaowen, X. Hui, Q. Xi, and Q. Zheng, "A PK-SIM card based end-to-end security framework for SMS," Computer Standards & Interfaces, vol. 31, no. 4, pp. 629-641, 2009.

[27] S. S. Ahamad, I. Al-Shourbaji, and S. Al-Janabi, "A secure NFC mobile payment protocol based on biometrics with formal verification," International Journal of Internet Technology and Secured Transactions, vol. 6, no. 2, pp. 103-132, 2016.

[28] D. Pal, P. Khethavath, T. Chen, and Y. Zhang, "Mobile payments in global markets using biometrics and cloud," International Journal of Communication Systems, vol. 30, no. 14, pp. 1-10, 2017.

[29] J. Lee, C. H. Cho, and M. S. Jun, "Secure quick response-payment (QR-pay) system using mobile device," The 13th Int. Conf. Advanced Communication Technology, pp. 1424–1427, 2011.

[30] V. Coskun, B. Ozdenizci, and K. Ok, "The survey on near field communication," Sensors, vol. 15, no. 6, pp. 13348-13405, 2015.

[31] K. Fan, C. Zhang, K. Yang, H. Li, and Y. Yang, "Lightweight NFC protocol for privacy protection in pobile IoT," Applied Sciences, vol. 8, no. 12, pp. 2506, 2018.

[32] Y. H. Tung, and W. S. Juang, "Secure and efficient mutual authentication scheme for NFC mobile devices," Journal of electronic science and technology, vol. 15, no. 3, pp. 240-245, 2017.

[33] N. E. Tabet, and M. A. Ayu, "Analysing the security of NFC based payment systems," Int.

Conf. Informatics and Computing, pp. 169-174, 2016.

[34] C. Thammarat, and W. Kurutach, “A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification,” International Journal of Communication Systems, e3991, 2019.

[35] C. Thammarat, W. Kurutach, and S. Phoomvuthisarn, “A secure lightweight and fair exchange protocol for NFC mobile payment based on limited-use of session keys,” the 17th Int. Conf. Communications and Information Technologies, pp. 1-6, 2017.

[36] R. Tso, "Untraceable and anonymous mobile payment scheme based on near field communication," Symmetry, vol. 10, no. 12, pp. 685, 2018.

[37] E. O. Blass, A. Kurmus, R. Molva, and T. Strufe, "PSP: Private and secure payment with RFID," Computer Communications, vol. 36, no. 4, pp. 468-480, 2013.

[38] A. Ruiz-Martínez, J. A. Sánchez-Laguna, and A. F. Skarmeta, "Extending SIP to support payments in a generic way," Computer Standards & Interfaces, vol. 46, pp. 23-36, 2016.

[39] S. Kungpisdan, "Modelling, design, and analysis of secure mobile payment systems," PhD Thesis, School of Computer Science and Software Engineering, Monash University, 2005.

[40] R. Kailar. "Accountability in electronic commerce protocols," IEEE Trans Software Engineering, vol. 22, no. 5, 1996.

[41] S. Kungpisdan, "Accountability in centralized payment environments," In Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on, pp. 1022-1027, 2009.

[42] J. Téllez, and S. Zeadally, “Mobile payment systems: secure network architectures and protocols,” Springer, 2017.

[43] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, 2017.

[44] N. Janpitak and R. Montha, “The Blockchain-Based Cooperative Management System,” Journal of Information Science and Technology, Vol.9, No. 2, pp. 1-12, 2019.

[45] S. Duangphasuk and C. Thammarat, “A Secure SMS Authentication Based on Limited-Used Session Keys,” Journal of Information Science and Technology, Vol.6, No. 2, pp. 38-47, 2016.