Ahamad and Pathan
Complex Adapt Syst Model (2019) 7:3
https://doi.org/10.1186/s40294-019-0064-z

Complex Adaptive Systems Modeling

RESEARCH Open Access

Trusted service manager (TSM) based privacy preserving and secure mobile commerce framework with formal verification

Shaik Shakeel Ahamad[1] and Al-Sakib Khan Pathan[2*]

*Correspondence:
spathan@ieee.org
[2] Department of Computer Science and Engineering, Southeast University, Dhaka, Bangladesh
Full list of author information is available at the end of the article

Abstract

Mobile contactless payment (MCP) is the future technology that is used for mobile payments, mobile wallet, transportation, and for mobile coupons. Existing solutions in this realm do not ensure end-to-end communication, information privacy, and the client's anonymity. In order to overcome these flaws, we propose a secure and privacy preserving mobile commerce (SPPMC) framework for near-field communication (NFC) based proximity payments. SPPMC framework achieves both communication and information privacy. It ensures the client's anonymity by making use of traceable anonymous certificates (TAC). Grid of secure elements (GSE) is used at the banking servers. The cost of computation and communication is very less. SPPMC ensures end-to-end security and withstands any type of known attack including multi-protocol attack. SPPMC is successfully verified using Burrows–Abadi–Needham (BAN) logic and Scyther tool. It ensures all the security properties.

Keywords: Mobile contactless payment (MCP), Near-field communication (NFC), Traceable anonymous certificate (TAC), Grid of secure elements (GSE), Burrows–Abadi–Needham (BAN) logic, Scyther

Introduction

Nowadays, we see that the consumers are adopting cashless payments very rapidly and most of these payments are made using credit or debit cards. With the increasing popularity of near-field communication (NFC) enabled smartphones, consumers, merchants and mobile network operators (MNO) are predicting that NFC-enabled mobile contactless payment (MCP) will be the future as this technology can be used for mobile payments, mobile wallet, transportation, and for mobile coupons (de Luna et al. 2019; Liébana-Cabanillas et al. 2019). There are various types of works in the relevant areas like a delay-tolerant payment scheme based on Ethereum Blockchain is proposed in (Hu et al. 2019). This work focuses on micro-banking or branchless banking scenarios where network connectivity is unreliable. The key ideas of some other works are described later. In fact, this field is still emerging and we could expect more works in the near future.

According to Berg Insight, NFC-enabled point of sale (POS) terminal shipments will increase to 4.1 million by 2022 (https://www.electran.org/publication/transactiontrends/nfc-ready-pos-terminals-to-hit-8-in-10-globally-by-2022/). There is a lot of demand

for Secure Elements (SE) and it is evident from the SIMalliance report (https://simalliance.org/media/press-releases/simalliance-reports-continued-strength-of-global-sim-market-in-2018-with-estimated-5-6-billion-shipments-and-gives-first-view-of-esim-volumes/). In fact, SIMalliance confirms that Subscriber Identity Module (SIM) unit shipments remained at unsurpassed volumes in 2018, with an estimated 5.6 billion units shipped worldwide (https://simalliance.org/media/press-releases/simalliance-reports-continued-strength-of-global-sim-market-in-2018-with-estimated-5-6-billion-shipments-and-gives-first-view-of-esim-volumes/). In addition to this, the developments in hardware and software security techniques made secure mobile banking possible with mobile phones. Before adopting this technology, there are some issues that need to be solved by the governments and the industries. These issues are related to end-to-end security, communication and information privacy, and Consumer's/Client's anonymity.

Existing solutions in this realm do not ensure end-to-end security, communication and information privacy and consumer's anonymity. In order to solve these issues, the role of trusted service manager (TSM) should be very clear as its role is very vital in the ecosystem, TSM should be managed by the government with clear policies. In traditional proximity based mobile payment system, POS is the reader which reads sensitive information of C such as order information (OI), payment information (credit card details), Client's certificate, and consumers have no idea or control over the transmitted data over the POS. Existing proximity based mobile solutions (Eun et al. 2013; Ashrafi and Ng 2009; https://www.securetechalliance.org/publications-host-card-emulation-101/; https://www.mobilepaymentstoday.com/companies/media/isis/, https://www.gosoftcard.com/) are not suitable. In fact, all those schemes have the following common or overall drawbacks.

a. Client's credentials are stored on the device (i.e., memory of mobile phones).
b. Non-repudiation property is not achieved as the Client's credentials are not generated in tamper-resistant device and on top of that, the Client shares the credentials with the cloud.
c. The solution fails to achieve communication and information privacy.
d. The real identity of the C is revealed to the merchant.

In order to overcome these drawbacks, here we propose a secure and privacy preserving mobile commerce (SPPMC) Framework for NFC based proximity payments. SPPMC framework achieves both communication and information privacy. It ensures Client's anonymity by making use of TAC. All the required security properties are ensured in the proposed SPPMC.

Background

The work by Ashrafi and Ng (2009) proposes a Privacy-Preserving electronic payments scheme using one-time payment details but this scheme stores client's/credentials in the memory of the device and on the cloud and it is not shared with the merchants. However, there are a few limitations of this solution like, the memory of the mobile phone is used to save/store Client's/User's credentials, non-repudiation property is not achieved in this solution, this solution fails to achieve communication

and information privacy, and the anonymity of the Client/User. Likewise, the mechanism proposed in https://www.securetechalliance.org/publications-host-card-emulation-101/ cannot ensure non-repudiation and it also fails to achieve communication and information privacy. On top of that, the complexity of the approach is very high.

A soft card's payment system (based on NFC) is proposed in https://www.mobilepaymentstoday.com/companies/media/isis/, https://www.gosoftcard.com/. While the idea apparently reads well, following are the limitations of this solution. Once again, for this one also, non-repudiation property is not achieved as the data are not digitally signed, there is no clarify where the payment credentials are stored, and how payment information is actually protected in the device and during transit. Moreover, anonymity of the Client/User is not ensured.

Eun et al. (2013) propose a conditional privacy preserving security protocol for NFC applications which apparently looks efficient however, the drawback is that there is no clarity where the payment credentials are stored and how payment information is protected in the device and during transit. Without clarity in this matter, the practicality of the approach can be questioned.

Şengel et al. (2018) in their work, highlight the important points to be considered in mobile payment services and systems. One of the points is to provide enough space on the handset to store data securely; however, keeping user's credentials (cryptographic keys and PIN—personal identification number) and data in the memory of a handset is very risky as these credentials can be compromised easily. Handset could be lost sometimes, or out of reach, and it could be in any other's hand. Also, going through the flow of the discussion, this work basically failed to address/discuss the existing White Box Cryptography (WBC) based mobile payment solutions.

In Li et al. (2019) propose an offline transaction e-commerce system model based on mobile payment which includes the offline POS terminal, mobile device, and payment center. But, the paper's technical description is deficient. While the system is discussed, it still remains unclear how it really works and what its efficiency is. Moreover, the authors did not discuss the existing offline transaction models in the mobile payment systems. It does not clarify either which entity in the ecosystem plays the role of an adjudicator. In fact, it is not clear how the offline POS terminal even validates/verifies the payment confirmation sent by the payment center.

Contributions made

Through our investigation, we have found a limited number of publications in this specific area of research. Among those works, the number of publications in reliable venues is even less. Given the state of the art and recent trends, we have come up with a framework that is named SPPMC (as mentioned before). The contributions in this work could be summarized as:

a. We propose SPPMC framework based on TSM.
b. The framework achieves both communication and information privacy.
c. The framework ensures client's anonymity by making use of TAC.

d. SPPMC is designed in such a manner that merchants cannot make use of user data. Sensitive data of the user will not sit on unsafe merchant's server on which users have no control.
e. Non-repudiation property is ensured.
f. SPPMC consumes relatively fewer resources.
g. End-to-end security is ensured and it overcomes the known attacks.
h. Scyther and BAN logic are used to verify SPPMC.

The rest of the paper is organized as follows: "Methods" section presents our SPPMC framework, simulation results and analysis alongside security analysis and comparative studies are presented in "Results", "Discussion" sections present a discussion on some recent works and possible future scope of research, and finally, Conclusion" section concludes the paper.

Methods

In this section, we describe our SPPMC framework which has the following stakeholders.

Participants

- Client (C)/User (U): Client (C)/User (U) possesses Universal Integrated Circuit Card (UICC) in a mobile phone.
- UICC: It acts as a reader in our proposed framework.
- Banking community (BC): BC is a community cloud catering the needs of Banking Community containing issuing bank (IB) (Client's bank), acquiring bank (AB) (merchant's bank) and payment gateway (PG). PG acts as an adjudicator.
- Mobile network operator (MNO): MNO provides mobile network connectivity.
- Traceable anonymous certificate (TAC): TAC is used in this framework for ensuring anonymity of client.
- Trusted service manager (TSM): certification authority (CA) plays the role of TSM in addition to its normal functions. TSM acts as a neutral middle man and aggregator in our proposed framework. Roles of TSM in our proposed framework include: MNO management, Over The Air (OTA) provisioning and personalization, application testing and certification, and OTA provisioning.

Personalization of secure element (i.e. UICC) by TSM and client

SPPMC framework uses UICC as it hosts many applications which are independent of each other, each defining and controlling its own application.

TSM issued certificates

Following are the certificates that are issued by TSM:

a. Chip certificate: This certificate is issued to chip of the secure element, CA issues EAL4+ (evaluation assurance level 4+) certification for integrated circuit (IC) chip which is the responsibility of chip manufacturer.

b. OS certificate: This certificate is issued to operating system (OS) which excludes applications.
c. Application certificate: Applications which are installed by the client of the UICC falls in this category. Every application will have its owner and it is the owner's responsibility to get certificate from TSM for this application.
d. Client certificate: CA issues TAC to the client after the client personalizes UICC.

UICC personalization

Our proposed framework adopts the procedure proposed in Ahamad et al. (2014) for the personalization; so there are four certificates at the client side which are issued by TSM (which is also a CA). Before describing the full authentication and transaction protocol, Table 1 shows all the major mathematical notations used in this paper along with their meanings.

Authentication and transaction protocol

IB, AB and PG contain a grid of secure elements (GSE). GSE is considered as trusted execution environment (TEE) which is used to generate own credentials and to generate shared symmetric keys with their clients.

$$\textbf{\textit{Step}}\ \mathbf{1}: C \rightarrow POS: \{Cert_C\}_{pubkey_{POS}}$$

Client (here, referred to as C) visits a supermarket and selects items and then moves to the POS for billing of the selected items. C validates $Cert_{POS}$ and sends his $Cert_C$ to the POS for mutual authentication.

$$\textbf{\textit{Step}}\ \mathbf{2}: POS \rightarrow C: \left\{MS1, DS_{POS_C}(MS1)\right\}_{pubkey_C}$$

$$\textbf{\textit{MS}}\mathbf{1}: \{OI, TID, Amt, POS_{ID}, Cert_{POS}, T_{POS}, N_{POS}\}$$

OI here is the "*Order Information*". In this step, POS plays the role of a Tag and mobile phone plays the role of a reader. POS sends $\{OI, TID, Amt, POS_{ID}, Cert_{POS}, T_{POS}, N_{POS}\}$.

$$\textbf{\textit{Step}}\ \mathbf{3}: C \rightarrow IB: \left\{MS2, DS_{C_{IB}}\right\}_{K_{CIB}}$$

Table 1 Mathematical notations and their meanings

Notation	Meaning	Notation	Meaning
C	Client	TID	Transaction identifier
IB	Issuing bank	Item no	Item number of the goods
AB	Acquirer/acquiring bank	Success	Success
MNO	Mobile network operator	PI	Payment information
TSM	Trusted service manager	DS_{XY}	Digital signature generated by 'X' for 'Y'
CA	Certifying authority	MS	Message
Amt	Amount	N_X	Nonce generated by entity 'X'
$Cert_X$	Certificate of the participant 'X'	T_X	Timestamp generated by 'X'
OI	Order information	POS	Point of sale
K_{XY}	Symmetric key shared between 'X' and 'Y' participants	HOI	Hashed order information

$$\boldsymbol{MS2} = \{PI, HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_C, N_C\}$$

C hashes the OI which it has received from POS, adds PI, TID, Amt, $Cert_{POS}$, POS_{ID}, T_C, N_C and sends MS1 to Issuer Bank (IB).

$$\textbf{Step 4}: IB \rightarrow PG: \{HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_{IB}, N_{IB}, Success\}$$

IB validates the digital signature generated by the Client on MS1, checks the timestamps and nonce generated by C. IB sends $\{HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_{IB}, N_{IB}, Success\}$ to PG.

$$\textbf{Step 5}: IB \rightarrow C: \left\{MS3, DS_{IB_C}(MS3)\right\}_{K_{CIB}}$$

$$\boldsymbol{MS3} = \{HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_{IB}, N_{IB}, Success\}$$

IB validates the digital signature generated by the C on MS2, checks the timestamps and nonce generated by the C. IB sends $\{MS3, DS_{IB_C}(MS3)\}_{K_{CIB}}$ to C.

$$\textbf{Step 6}: PG \rightarrow AB: \{HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_{IB}, N_{IB}, Success\}$$

PG receives $\{HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_{IB}, N_{IB}, Success\}$ from IB through secure private banking network. PG checks the timestamps and nonce generated by IB. After successful verifications, PG keeps a copy of the message sent by IB in Step 4 as evidences for future use in case of disputes among the participants (to ensure non-repudiation). It then forwards the received message to AB through private banking network.

$$\textbf{Step 7}: AB \rightarrow POS: \left\{MS4, DS_{AB_{POS}}(MS4)\right\}_{K_{ABPOS}}$$

$$\boldsymbol{MS4}: \{Success, TID, Amt, T_{AB}, N_{AB}, POS_{ID}\}$$

AB receives $\{HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_{IB}, N_{IB}, Success\}$ from IB through secure private banking network which is very secure. AB checks the timestamps and nonce generated by IB. If all checks are successful, it then sends this message: $\{Success, TID, Amt, T_{AB}, N_{AB}, POS_{ID}\}$ to POS.

The entire mechanism is depicted in Fig. 1.

Authentication proof of SPPMC protocol based on BAN logic

In order to ensure security properties, a security protocol exchanges encrypted messages (Muhammad et al. 2006; Mall 2017). To prove that our proposed protocol is secure, we have use BAN logic (Abadi et al. 1993; Burrows et al. 1990).

Assumptions

a. Secrets and keys:

CA contains all the certificates (valid) of all the participants (**AS1**, **AS2)**.

AS1. CA **believes** $\left(\forall S \in \left\{C, \text{IB, AB, PG, POS/M and CA}\right\} \overset{K_s}{\mapsto} S\right)$. All the entities/participants know their own certificates.

AS2. $S \in \left\{C, \text{IB, AB, PG, POS/M and CA}\right\}$ S **believes** $\overset{K_{ca}}{\mapsto} CA$). CA's certificate is with all the participants.

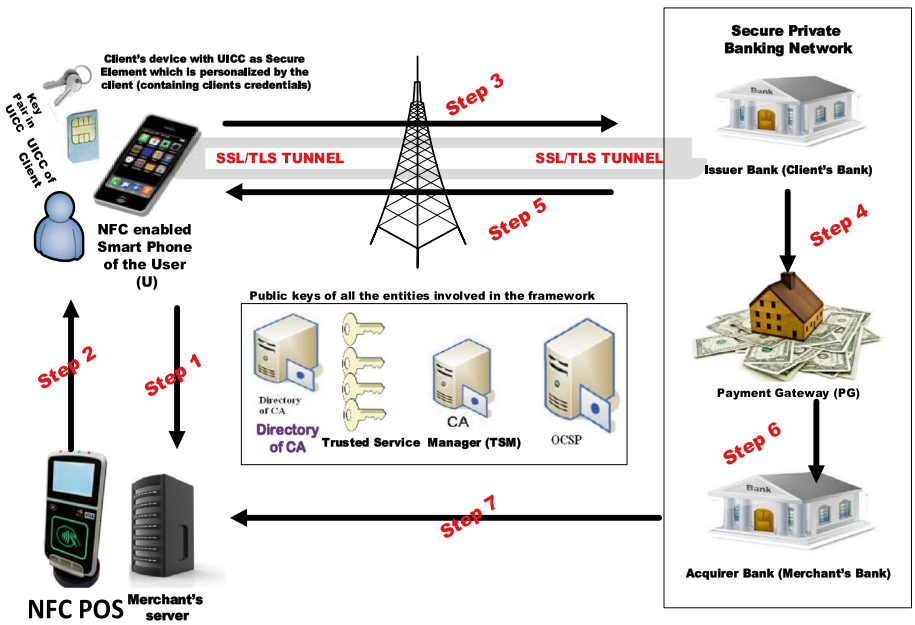

Fig. 1 Authentication and Transaction protocol of SPPMC

AS3. Client and IB share a symmetric shared key.

AS4. POS and AB share a symmetric shared key.

b. Freshness:

AS5 signifies freshness.

AS5. C believes freshness (N_c), **IB believes freshness** (N_{ib}), **AB believes freshness** (N_{ab}), and **POS believes freshness** (N_{pos})

AS6 signifies validity period of X.509 certificates.

AS6. TS_x and TS_y are the validity periods of participant's certificates.

c. Trust:

AS7. CA is trusted by all the participants.

AS8. Certification authority (CA) believes that U/C/UICC relays Client's beliefs.

AS9. ($S \in \{\text{C, IB, AB, PG, POS/M and CA}\}$, S **believes** QES

AS10. ($S \in \{\text{C, IB, AB, PG, POS/M and CA}\}$, S **believes** messages are encrypted using Symmetric Encryption algorithm from the personalized (personalized by IB) mobile payment application (MPA) of UICC in the mobile phone of C.

AS11. ($S \in \{\text{C, IB, AB, PG, POS/M and CA}\}$, S **believes** (every stakeholder) messages are encrypted using Symmetric Encryption algorithm from the personalized (personalized by AB) MPA of POS at the Merchant.

AS12. ($L \in \{\text{IB, AB and PG}\}$ L **believes** messages exchanged among **the banking entities** (IB, AB and PG) are through dedicated private banking network without encrypting their messages as this network is very secure.

AS13. ($S \in \{\text{C, IB, AB, PG, POS/M and CA}\}$, S **believes** CA ensures the anonymity of C by adopting TAC (Park et al. 2009).

Formal verification of SPPMC protocol using BAN logic

As discussed in Step 2 of our proposed protocol in "Authentication and transaction protocol" section,

$$\textbf{\textit{Step 2}}: POS \rightarrow C: \left\{MS1, DS_{POS_C}(MS1)\right\}_{pubkey_C}$$

$$\textbf{\textit{MS1}}: \{OI, TID, Amt, POS_{ID}, Cert_{POS}, T_{POS}, N_{POS}\}$$

C receives $\{MS1, DS_{POS_C}(MS1)\}_{pubkey_C}$ from the POS of merchant (M) and decrypts so from the assumptions: AS1, AS2, AS7, AS8, AS9 and AS10.

$$\text{C } \textbf{believes } \left\{MS1, DS_{POS_C}(MS1)\right\} \tag{1}$$

C validates the certificate (AS9) received from Client C as listed in (Ahamad et al. 2014). If the verification is successful then,

$$\text{C } \textbf{believes POS said } \left\{MS1, DS_{POS_C}(MS1)\right\} \tag{2}$$

$$\text{C } \textbf{believes fresh } N_{pos} \& \ T_{pos} \text{ from AS4 \&AS3} \tag{3}$$

$$\text{C } \textbf{believes QES from AS9} \tag{4}$$

Hence, from (1) to (4),

$$C \ \textbf{\textit{believes}} \ \{MS1, DS_{POS_C}(MS1)\}_{pubkey_C}$$

Then, Step 3 was:

$$\textbf{\textit{Step3}}: C \rightarrow IB: \left\{MS2, DS_{C_{IB}}\right\}_{K_{CIB}}$$

$$\textbf{\textit{MS2}} = \{PI, HOI, TID, Amt, POS_{ID}, Cert_{POS}, T_C, N_C\}$$

C hashes the OI which it has received from POS, adds PI, TID, Amt, $Cert_{POS}$, POS_{ID}, T_C, N_C and sends MS1 to Issuer Bank (IB).

IB receives $\left\{\textbf{\textit{MS2}}, \textbf{\textit{DS}}_{\textbf{\textit{C}}_{\textbf{\textit{IB}}}}\right\}_{\textbf{\textit{K}}_{\textbf{\textit{CIB}}}}$ from the C and decrypts from the assumption, **AS3**.

$$\text{IB } \textbf{believes} \left\{\textbf{\textit{MS2}}, \textbf{\textit{DS}}_{\textbf{\textit{C}}_{\textbf{\textit{IB}}}}\right\} \tag{5}$$

IB validates the certificate (**AS9**) received from Client/User from (Stinson 2005):
After successful verification,

$$\text{IB } \textbf{believes } \textbf{\textit{DS}}_{\textbf{\textit{C}}_{\textbf{\textit{IB}}}} \tag{6}$$

$$\text{C } \textbf{believes fresh } T_c \& N_c \text{ from } \textbf{AS3\&AS4} \tag{7}$$

$$\text{IB } \textbf{believes QES, thereby ensuring integrity,}$$
$$\text{authentication \& non repudiation properties from } \textbf{AS9} \tag{8}$$

Hence, from (5) to (8),

$$\text{IB receives } \left\{\textbf{\textit{MS2}}, \textbf{\textit{DS}}_{\textbf{\textit{C}}_{\textbf{\textit{IB}}}}\right\}_{\textbf{\textit{K}}_{\textbf{\textit{CIB}}}}$$

So, IB believes that the received message (MS2) ensures confidentiality, integrity and non-repudiation properties.

Then,

$$\textbf{\textit{Step4}}: \textbf{\textit{IB}} \rightarrow \textbf{\textit{PG}}: \{\textbf{\textit{HOI}}, \textbf{\textit{TID}}, \textbf{\textit{Amt}}, \textbf{\textit{POS}}_{\textbf{\textit{ID}}}, \textbf{\textit{Cert}}_{\textbf{\textit{POS}}}, \textbf{\textit{T}}_{\textbf{\textit{IB}}}, \textbf{\textit{N}}_{\textbf{\textit{IB}}}, \textbf{\textit{Success}}\}$$

From the **AS12**,

$$\text{PG } \textbf{believes}\{\textbf{\textit{HOI}}, \textbf{\textit{TID}}, \textbf{\textit{Amt}}, \textbf{\textit{POS}}_{\textbf{\textit{ID}}}, \textbf{\textit{Cert}}_{\textbf{\textit{POS}}}, \textbf{\textit{T}}_{\textbf{\textit{IB}}}, \textbf{\textit{N}}_{\textbf{\textit{IB}}}, \textbf{\textit{Success}}\} \tag{9}$$

In this step IB sends message without encrypting because messages are exchanged among PG, IB (Issuer) and AB (acquirer) using private banking network which is very secure.

For,

$$\textbf{\textit{Step 5}}: \textbf{\textit{IB}} \rightarrow \textbf{\textit{C}}: \left\{\textbf{\textit{MS}}3, \textbf{\textit{DS}}_{\textbf{\textit{IB}}_{\textbf{\textit{C}}}}(\textbf{\textit{MS}}3)\right\}_{K_{CIB}}$$

$$\textbf{\textit{MS3}} = \{\textbf{\textit{HOI}}, \textbf{\textit{TID}}, \textbf{\textit{Amt}}, \textbf{\textit{POS}}_{\textbf{\textit{ID}}}, \textbf{\textit{Cert}}_{\textbf{\textit{POS}}}, \textbf{\textit{T}}_{\textbf{\textit{IB}}}, \textbf{\textit{N}}_{\textbf{\textit{IB}}}, \textbf{\textit{Success}}\}$$

C receives $\left\{\textbf{\textit{MS}}3, \textbf{\textit{DS}}_{\textbf{\textit{IB}}_{\textbf{\textit{C}}}}(\textbf{\textit{MS}}3)\right\}_{K_{CIB}}$ from the IB and decrypts from the assumption, **AS3**

$$\text{C } \textbf{believes } \left\{\textbf{\textit{MS}}3, \textbf{\textit{DS}}_{\textbf{\textit{IB}}_{\textbf{\textit{C}}}}(\textbf{\textit{MS}}3)\right\} \tag{10}$$

C validates the certificate (**AS9**) received from IB as listed in (Stinson 2005).

If the verification is successful, then:

$$\text{C } \textbf{believes } \textbf{\textit{DS}}_{\textbf{\textit{IB}}_{\textbf{\textit{C}}}} \tag{11}$$

$$\text{C } \textbf{believes fresh } T_{ib}\&N_{ib}, \text{ from } \textbf{AS3}\&\textbf{AS4} \tag{12}$$

$$\text{C } \textbf{believes Qualified Electronic Signature(QES)from } \textbf{AS9} \tag{13}$$

So from (10) to (13),

$$\text{C } \textbf{believes}\left\{\textbf{\textit{MS}}3, \textbf{\textit{DS}}_{\textbf{\textit{IB}}_{\textbf{\textit{C}}}}(\textbf{\textit{MS}}3)\right\}_{K_{CIB}}$$

Hence, C believes that the received message (MS3) ensures confidentiality, integrity and non-repudiation properties.

Taking,

$$\textbf{\textit{Step 6}}: \textbf{\textit{PG}} \rightarrow \textbf{\textit{AB}}: \{\textbf{\textit{HOI}}, \textbf{\textit{TID}}, \textbf{\textit{Amt}}, \textbf{\textit{POS}}_{\textbf{\textit{ID}}}, \textbf{\textit{Cert}}_{\textbf{\textit{POS}}}, \textbf{\textit{T}}_{\textbf{\textit{IB}}}, \textbf{\textit{N}}_{\textbf{\textit{IB}}}, \textbf{\textit{Success}}\}$$

In this step PG sends message without encrypting because messages are exchanged among PG, I (Issuer) and AB (acquirer) using private banking network which is very secure.

From the **AS12**,

$$\text{AB } \textbf{believes } \{\textbf{\textit{HOI}}, \textbf{\textit{TID}}, \textbf{\textit{Amt}}, \textbf{\textit{POS}}_{\textbf{\textit{ID}}}, \textbf{\textit{Cert}}_{\textbf{\textit{POS}}}, \textbf{\textit{T}}_{\textbf{\textit{IB}}}, \textbf{\textit{N}}_{\textbf{\textit{IB}}}, \textbf{\textit{Success}}\} \tag{14}$$

Likewise,

$$\textbf{\textit{Step 7}}: \textbf{\textit{AB}} \rightarrow \textbf{\textit{POS}}: \left\{\textbf{\textit{MS}}4, \textbf{\textit{DS}}_{\textbf{\textit{AB}}_{\textbf{\textit{POS}}}}(\textbf{\textit{MS}}4)\right\}_{K_{ABPOS}}$$

$$\textbf{\textit{MS4}}: \{\textbf{\textit{Success}}, \textbf{\textit{TID}}, \textbf{\textit{Amt}}, \textbf{\textit{T}}_{\textbf{\textit{AB}}}, \textbf{\textit{N}}_{\textbf{\textit{AB}}}, \textbf{\textit{POS}}_{\textbf{\textit{ID}}}\}$$

POS receives $\left\{\left\{\textbf{\textit{MS}}4, \textbf{\textit{DS}}_{\textbf{\textit{AB}}_{\textbf{\textit{POS}}}}(\textbf{\textit{MS}}4)\right\}_{K_{ABPOS}}\right.$ from the AB and decrypts using **AS4** assumptions

$$\text{POS } \textbf{believes } \left\{\left\{\textbf{\textit{MS}}4, \textbf{\textit{DS}}_{\textbf{\textit{AB}}_{\textbf{\textit{POS}}}}(\textbf{\textit{MS}}4)\right\}_{K_{ABPOS}}\right. \tag{15}$$

POS validates the certificate (**AS9**) received from AB using (Stinson 2005).
If the verification is successful,

$$\text{POS } \textbf{believes } \boldsymbol{DS_{AB_{POS}}} \tag{16}$$

$$\text{POS } \textbf{believes fresh } T_{ab}\&N_{ab} \text{ from } \textbf{AS} \tag{17}$$

$$\text{POS } \textbf{believes QES from } \textbf{AS9} \tag{18}$$

So, from (14) to (18),

$$\text{POS } \textbf{believes } \left\{\boldsymbol{MS}4, \boldsymbol{DS_{AB_{POS}}}(\boldsymbol{MS}4)\right\}_{\boldsymbol{K_{ABPOS}}}$$

Hence, POS believes that the received message (MS4) ensures confidentiality, integrity and non-repudiation properties.

Results

We used Scyther (Cremers 2006; Cremers et al. 2009) tool for verifying the proposed protocol. Scyther provides reliable simulation environment. Security protocol description language (SPDL) is used to write code in Scyther tool. Following are the motivations in selecting Scyther tool compared to AVISPA tool (Armando 2005).

a. This tool assumes that each and every protocol runs with other protocols in the same network.
b. It uses SPDL language.
c. Good in verifying multi-protocol attacks.
d. When attacks are found in the protocol, attack graphs are generated.
e. Verification of protocols in Scyther tool is done by bounded/unbounded number of sessions.
f. Unbounded or bounded number of sessions are supported in Scyther tool.

Table 2 shows a comparative chart for the two available tools and our choice here was Scyther.

Scyther (Cremers 2006; Cremers et al. 2009) verifies, falsifies and analyzes security protocols. We define the role of C, POS, IB, AB, and PG. In our proposed framework, all the stakeholders make use of Trusted Modules such as UICC (SE) and Trusted Platform Module (TPM), for the key generation and storing of keys. It should be mentioned that TPM (https://www.iso.org/standard/50970.html) is an international standard for a secure crypto-processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. All the stakeholders use trusted modules. $DS_{X_Y}\&K_{XY}$ are stored within the trusted module, i.e., UICC of the mobile phone and TEE at the Bank side.

Security analysis

This section provides security analysis of SPPMC protocol to prove that SPPMC is safe against any other known attack.

Table 2 Differences between AVISPA and Scyther tool

AVISPA tool (Armando 2005)	Scyther tool (Cremers 2006; Cremers et al. 2009)
High level protocol specification language (HLPSL) is used	Security protocol description language (SPDL) is used
Multi-protocol attacks are not verified	Multi-protocol attacks are verified
Attack graphs are not generated	When attacks are found, attack graphs are generated
Verification of protocols is done using only bounded number of sessions	Verification of protocols is done by bounded/unbounded number of sessions
Assumes that every protocol runs in isolation	Assumes that each protocol runs with other protocols in the same network

Assumptions

Following are the assumptions that are made in the security analysis.

Assumption 1 CA plays the role of TSM in addition to its normal functions. TSM acts as a neutral middle man and aggregator in our proposed framework. It is trusted by all the entities involved in the ecosystem. MNO management, Over The Air (OTA) provisioning and personalization, Application testing and certification are the main functions of TSM.

Assumption 2 Client personalizes his/her UICC and cannot be tampered.

Assumption 3 Banking entities involved in SPPMC exchange their messages through dedicated private banking network without encrypting their messages.

Assumption 4 Intruders cannot decrypt the encrypted messages nor digitally sign the messages as they do not possess private keys and symmetric keys.

Assumption 5 SPPMC digitally signs the messages using private key stored in the UICC.

Assumption 6 TAC is used to ensure anonymity to the User's/Client's identity. Anonymity is given in RFC 5636 (Park et al. 2009).

Assumption 7 MPA of the client is personalized by IB and Payment Application (PA) of the POS is personalized by the acquirer bank (AB).

Threat model

Let us consider that the possible attacks on SPPMC are:

Attack on authentication: An intruder can intercept, intercept, monitor and introduce new participants on behalf of original participants.

Attack on confidentiality: An intruder accesses/views the unauthorized messages.

Attack on integrity: An intruder monitors the messages and modifies the messages.

Attack on non-repudiation: An intruder generates qualified electronic signatures (QESs) of the other stakeholders of the SPPMC framework.

Attack on anonymity of the client: Intruder/POS/AB knows the real identity of C or U.

Attack on communication privacy: Intruder captures/gets access to the messages in the transit.

Security proof

Following are the security proofs:

Theorem 1 *MPA of C is personalized by the IB Server.*

Proof MPA of the C is personalized by the IB Server using the procedure proposed in (Ahamad et al. 2014).

Theorem 2 *Intruder (In) fails in tampering messages exchanged by the participants during the transit.*

Proof SPPMC encrypts and digitally signs the messages using Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm.

Theorem 3 *Merchant (or) POS and AB fail in knowing the original identity of the client.*

Proof TAC is used to ensure anonymity to the User's/Client's identity. Anonymity is given in RFC 5636 (Park et al. 2009).

Theorem 4 *No other stakeholder (except IB) in the framework will be able to read payment information of the client.*

Proof Client encrypts the payment information (PI), thereby ensuring payment secrecy.

Theorem 5 *IB and AB will not know the spending habits of the client.*

Proof Secrecy of OI is ensured by hashing OI. C only sends HOI to the IB, thereby achieving OI secrecy. IB fails in retrieving OI from HOI as hash function is one way function.

Theorem 6 *SPPMC consumes very low resources from the client's perspective.*

Proof SPPMC consumes very low resources as it uses ECDSA based digital signatures. C is involved in the transaction only twice.

Theorem 7 *SPPMC overcomes over spending and double spending.*

Proof Over spending and double spending can be avoided from timestamps and nonce. In our proposed protocol, POS will not get PI of C; so, there is no threat from POS of double spending and over spending.

Theorem 8 *SPPMC framework ensures communication security.*

Proof Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol *is used for* ensuring communication security.

Theorem 9 *SPPMC overcomes all the well-known attacks.*

Proof Timestamps, nonce, encryption, and digital signatures are used to overcome all the well-known attacks.

Comparison of SPPMC with related works

Table 3 compares SPPMC protocol with the other relevant mobile payment protocols for the security and threat requirements. It is evident that SPPMC satisfies all security requirements and protects the operations from various known threats and attacks. We mentioned that the work by Eun et al. (2013) does not clarify anything about the location of storing payment credentials. Also, there is no clear mechanism that addresses how to protect the payment information either on the device or during transit. SPPMC overcomes these issues. Again, the work by Ashrafi and Ng (2009) does not ensure non-repudiation, secrecy of payment information and order information. These issues are also well taken care of by SPPMC. Unlike the mechanism presented in https://www.securetechalliance.org/publications-host-card-emulation-101/, our mechanism reduces the complexity alongside ensuring non-repudiation and communication privacy. Our mechanism is better than the mechanism presented in https://www.mobilepaymentstoday.com/companies/media/isis/, https://www.gosoftcard.com/ because of the same issues of ensuring non-repudiation, clear policy of storing payment information or protecting the same in transit. On top of all these positive features of SPPMC, it ensures anonymity of the client. The comparative strengths are summarized in the table.

Discussion

While in this work we proposed a technical solution for the issue and presented formal verification, in practice, mobile payment transactions are still less compared to regular type of cash-based and other digital transactions. Park et al. (2019) did a study to examine the effects of perceived risk, perceived benefits, and trust on consumers' intention to use mobile payment, or m-payment. Though the work is not directly related to this technical solution of ours, it raises important concern that trust would be a critical factor for the customers to embrace the technology fully. The work also gives some interesting perspective on the issue as they analyze its adoption based on demographics; gender, age, education, income of the people. Their study used the sample that came from a single demographic area of the United States, mainly the Midwest. Indeed, technological divide between different parts of the globe would have direct impact on the spread of such technology. Hence, solutions like ours would be mainly and primarily be applicable for the technologically developed parts of the globe which would be relatively smaller than the rest. Again, there may be country specific laws and regulations that can impede mobile payment's (or, mobile

Table 3 Comparison of SPPMC with related works

Features	Protocols				
	Eun et al. (2013)	Ashrafi and Ng (2009)	Google's host card emulation (HCE) (https://www.securetechalliance.org/publications-host-card-emulation-101/)	Soft card's NFC payment (https://www.mobilepaymentstoday.com/companies/media/isis/, https://www.gosoftcard.com/)	SPPMC (our proposal)
Authentication	Y	Y	Y	Y	Y
Confidentiality	Y	Y	Y	Y	Y
Integrity	Y	Y	Y	Y	Y
Non-repudiation	N	N	N	N	Y
Credentials are generated and stored in tamper-resistant hardware	N	N	N	N	Y
QES (qualified electronic signature)	N	N	N	N	Y
Does the framework ensure secrecy of payment information	Y	N	N	N	Y
Does the framework ensure secrecy of order information	Y	N	N	N	Y
Does the framework ensure anonymity of client (C/U) from POS, AB and eavesdropper	Y	N	N	N	Y
communication privacy	Y	N	N	N	Y
Does the framework ensure information privacy	Y	N	N	N	Y
Avoids double spending and over spending	Y	N	N	N	Y
Does the framework withstand replay attack	Y	Y	Y	Y	Y
Does the framework withstand impersonation attack	Y	Y	Y	Y	Y
Does the framework withstand MITM (man-in-the-middle attack) attack	Y	Y	Y	Y	Y
Does the framework withstand multi-protocol attack	N	N	N	N	Y
Is the framework/protocol verified with formal logic or formal tool	N	N	N	N	Y

contactless payment's) growth. Knowing this issue would be good for the researchers as in the coming future, they would need to take into consideration the country's economic strength and demography while proposing efficient solutions for various issues related to this area.

As Internet of Things (IoT) is getting warm welcome in many parts of the globe even in places with limited technological setting or facilities, there are some works that are recently done focusing on IoT setting. One such example is the work in (Sethia et al. 2018) in which the authors propose a framework for the NFC secure element (SE)-based mutual authentication and attestation for IoT access with a user device such as a mobile device using NFC-based Host Card Emulation (HCE) mode. This could be a future direction to expand our work considering IoT scenario. In this work, we basically tried to present the technical idea and it is possible to work on it further and explore different settings for practical use and acceptance of such mechanism.

Conclusions

Mobile contactless payments (MCP) is the future technology for mobile payments but the existing solutions are not yet efficient enough. There are critical weaknesses about preserving privacy and anonymity. That is why, we were motivated to propose the secure and privacy preserving mobile commerce (SPPMC) Framework for NFC based proximity payments. Through formal verification, we have shown that this one achieves the intended objectives. Moreover, computational and communication cost of SPPMC is very less due to using efficient and lightweight techniques. We have successfully verified SPPMC protocol using BAN logic and Scyther tool. As a future work, we would like to work on community cloud based mobile payments and also, the applicability of our mechanism in IoT environment.

Abbreviations

AB: acquirer/acquiring bank; BAN: Burrows–Abadi–Needham; CA: certification authority; EAL: evaluation assurance level; ECDSA: Elliptic Curve Digital Signature Algorithm; GSE: grid of secure elements; HLPSL: high level protocol specification language; HOI: hashed order information; IB: issuing bank; IC: integrated circuit; MCP: mobile contactless payment; MNO: mobile network operator; MPA: mobile payment application; NFC: near-field communication; OI: order information; OS: operating system; OTA: Over The Air; PI: payment information; PIN: personal identification number; POS: point of sale; QES: qualified electronic signatures; SIM: Subscriber Identity Module; SPDL: security protocol description language; SPPMC: secure and privacy preserving mobile commerce; TAC: traceable anonymous certificates; TEE: trusted execution environment; TID: transaction identifier; TPM: Trusted Platform Module; TSM: Trusted service manager; UICC: Universal Integrated Circuit Card.

Acknowledgements

We sincerely thank the editorial office for providing us with valuable instructions to prepare the paper with the appropriate format.

Authors' contributions

Each author has contributed to this work. Both authors read and approved the final manuscript.

Funding

No funding was available for this work.

Availability of data and materials

All data and materials are our own.

Competing interests

All authors declare that they have no competing interests.

Author details

[1] Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majmaah, Kingdom of Saudi Arabia. [2] Department of Computer Science and Engineering, Southeast University, Dhaka, Bangladesh.

Appendix: (SPDL Code of SPPMC)

```
/* SPPMC framework. This framework is based on UICC & TSM Centric NFC Eco-
system*/
/*Secure and Privacy Preserving Mobile Payment */
/* Wireless PKI*/
/*Steps 6 & 7 of the protocol are also included in SPDL code encrypted by symmetric
key but these messages are exchanged in Secure Private Banking Network in the pro-
tocol proposed */
const pk: Function;
secret sk: Function;
inversekeys (pk,sk);
clienttype Timestamp;
clienttype Success;
clienttype PI,Amt,Certc,Tc,Tpos,Tpg,Npos,Nc,Tib,Tab,HOI,TID,POSid,Certpos,OI;
//Protocol description
protocol SPPMC(C,POS,IB,AB,PG)
{
role C
{
const Nc: Nonce;
var Nib,Npos: Nonce;
const Kcib:SessionKey;
send_1(C,POS,{Certc}pk(POS));
read_2 (POS,C, {OI,TID,Amt,POSid,Certpos,Tpos,Npos}pk(C));
send_3 (C,IB, {PI,HOI,TID,Amt,POSid,Certpos,Tc,Nc}Kcib);
send_4 (C,POS, {{PI}Kcib,HOI,TID,Amt,POSid,Tc,Nc}pk(POS));
read_5 (IB,C, {Success,TID,Amt,POSid,Tib,Nib,Nc}Kcib);
claim_C1 (C, Secret, Kcib);
claim_C2 (C, Secret, Nc);
claim_C3 (C, Secret, PI);
claim_C4 (C, Secret, Nib);
claim_C5 (C, Niagree);
claim_C6 (C, Nisynch);
}
role POS
{
const Npos: Nonce;
var Nc,Nab: Nonce;
const Kcib:SessionKey;
const Kposab:SessionKey;
read_1 (C,POS,{Certc}pk(POS));
send_2 (POS,C, {OI,TID,Amt,POSid,Certpos,Tpos,Npos}pk(C));
read_4 (C,POS, {{PI}Kcib,HOI,TID,Amt,POSid,Tc,Nc}pk(POS));
read_8 (AB,POS, {Success,TID,Amt,POSid,Tab,Nab}Kposab);
```

```
claim_POS1 (POS, Secret, Kposab);
claim_POS2 (POS, Secret, Nc);
claim_POS3 (POS, Secret, Npos);
claim_POS4 (POS, Niagree);
claim_POS5 (POS, Nisynch);
}
role IB
{
const Nib: Nonce;
var Nc: Nonce;
const Kcib:SessionKey;
const Kibpg:SessionKey;
read_3 (C,IB, {PI,HOI,TID,Amt,POSid,Certpos,Tc,Nc}Kcib);
send_5 (IB,C, {Success,TID,Amt,POSid,Tib,Nib,Nc}Kcib);
send_6 (IB,PG, {Success,TID,Amt,POSid,Tib,Nib,Nc}Kibpg);
claim_IB1 (IB, Secret, Nib);
claim_IB2 (IB, Secret, Kcib);
claim_IB3 (IB, Niagree);
claim_IB4 (IB, Nisynch);
}
role AB
{
const Nab: Nonce;
var Npg: Nonce;
const Kcab:SessionKey;
const Kposab:SessionKey;
const Kabpg:SessionKey;
read_7(PG, AB,{Success,TID,Amt,POSid,Tpg,Npg}Kabpg);
send_8 (AB,POS, {Success,TID,Amt,POSid,Tab,Nab}Kposab);
claim_AB1 (AB, Secret, Nab);
claim_AB2 (AB, Secret, Kcab);
claim_AB3 (AB, Niagree);
claim_AB4 (AB, Nisynch);
}
role PG
{
const Npg: Nonce;
var Nc,Nib: Nonce;
const Kabpg:SessionKey;
const Kibpg:SessionKey;
read_6 (IB,PG, {Success,TID,Amt,POSid,Tib,Nib,Nc}Kibpg);
send_7(PG, AB,{Success,TID,Amt,POSid,Tpg,Npg}Kabpg);
claim_PG1 (PG, Secret, Nib);
claim_PG2 (PG, Secret, Kibpg);
claim_PG3 (PG, Secret, Kabpg);
claim_PG4 (PG, Niagree);
```

```
claim_PG5 (PG, Nisynch);
}
}
//An untrusted agent, with compromised key
const e: Agent;
untrusted e;
compromised sk(e);
```

Received: 29 June 2019 Accepted: 2 August 2019
Published online: 08 August 2019

References

Abadi M, Burrows M, Kaufman C, Lampson B (1993) Authentication and delegation with smart-cards. Sci Comput Program 21(2):93–113
Ahamad SS, Sastry VN, Udgata SK (2014) Secure mobile payment framework based on UICC with formal verification. Int J Comput Sci Eng 9(4):355–370
Armando A et al (2005) The AVISPA tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification, CAV 2005, pp 281–285
Ashrafi MZ, Ng SK (2009) Privacy-preserving e-payments using one-time payment details. Comput Stand Interfaces 31(2):321–328
Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst (TOCS) 8(1):18–36
Cremers CJF (2006) Scyther-semantics and verification of security protocols. Ph.D. Thesis, Eindhoven University of Technology
Cremers CJF, Lafourcade P, Nadeau P (2009) Comparing state spaces in automatic security protocol analysis. LNCS 5458:70–94
de Luna IR, Liébana-Cabanillas F, Sánchez-Fernández J, Muñoz-Leiva F (2019) Mobile payment is not all the same: the adoption of mobile payment systems depending on the technology applied. Technol Forecast Soc Change 146:931–944
Eun H, Lee H, Oh H (2013) Conditional privacy preserving security protocol for NFC applications. IEEE Trans Consum Electron 59(1):153–160
Host Card Emulation 101. White paper, secure technology alliance, August 2014. https://www.securetechalliance.org/publications-host-card-emulation-101/. Accessed 23 June 2019
Hu Y, Manzoor A, Ekparinya P, Liyanage M, Thilakarathna K, Jourjon G, Seneviratne A (2019) A delay-tolerant payment scheme based on the Ethereum Blockchain. IEEE Access 7:33159–33172
ISO/IEC 11889-1:2009—Information technology—trusted platform module—Part 1: Overview. ISO.org. International Organization for Standardization. May 2009. https://www.iso.org/standard/50970.html. Accessed June 23 2019
Li S, Hu X, Fengling, Zhang Y, Dong W, Ye J, Sun H (2019) Research on offline transaction model in mobile payment system. In: International Conference on Frontier Computing 2018, LNEE, vol 542. pp 1815–1820
Liébana-Cabanillas F, Molinillo S, Ruiz-Montañez M (2019) To use or not to use, that is the question: analysis of the determining factors for using NFC mobile payment systems in public transportation. Technol Forecast Soc Change 139:266–276
Mall D, Konaté K, Pathan A-SK (2017) ECL-EKM: an enhanced certificateless effective key management protocol for dynamic WSN. In: International conference on networking, systems and security (NSysS 2017), January 5–8, Dhaka, Bangladesh, pp 150–155
Muhammad S, Furqan Z, Guha RK (2006) Understanding the intruder through attacks on cryptographic protocols. In: Proceedings of the 44th annual Southeast regional conference, pp 667–672
NFC-Ready POS Terminals to Hit 8 in 10 Globally by 2022. https://www.electran.org/publication/transactiontrends/nfc-ready-pos-terminals-to-hit-8-in-10-globally-by-2022/. Accessed 12 Apr 2019
Park S, Park H, Won Y, Lee J (2009) Traceable anonymous certificate. RFC 5636—IETF Tools. https://tools.ietf.org/html/rfc5636. Accessed 27 May 2019
Park J, Amendah E, Lee Y, Hyun H (2019) M-payment service: interplay of perceived risk, benefit, and trust in service adoption. Hum Factors Ergon Manuf Serv Ind 29(1):31–43
Şengel Ö, Aydin MA, Sertbaş A (2018) A survey on white box cryptography model for mobile payment systems. Lect Notes Electr Eng 504:215–225
Sethia D, Gupta D, Saran H (2018) NFC secure element-based mutual authentication and attestation for IoT access. IEEE Trans Consum Electron 64(4):470–479
SIMalliance reports continued strength of global SIM market in 2018 with estimated 5.6 billion shipments and gives first view of eSIM volumes. https://simalliance.org/media/press-releases/simalliance-reports-continued-strength-of-global-sim-market-in-2018-with-estimated-5-6-billion-shipments-and-gives-first-view-of-esim-volumes/. Accessed 27 May 2019
Softcard. https://www.mobilepaymentstoday.com/companies/media/isis/, https://www.gosoftcard.com/. Accessed 27 May 2019
Stinson DR (2005) Cryptography-theory and practice. Chapman & Hall/CRC, Boca Raton. ISBN 978-1-58-488508-5

Publisher's Note