Journal of Organizational and End User Computing
Volume 33 • Issue 2 • March-April 2021

A Key-Based Mutual Authentication Framework for Mobile Contactless Payment System Using Authentication Server

Brij B. Gupta, National Institute of Technology, Kurukshetra, India & Asia University, Taiwan & Macquarie University, Australia

Shaifali Narayan, National Institute of Technology, Kurukshetra, India

ABSTRACT

This paper presents a framework for mutual authentication between a user device and a point of sale (POS) machine using magnetic secure transmission (MST) to prevent the wormhole attack in Samsung pay. The primary attribute of this method is authenticating the POS terminals by an authentication server to bind the generated token to a single POS machine. To secure the system from eavesdropping attack, the data transmitted between the user device and the machine is encrypted by using the Elgamal encryption method. The keys used in the method are dynamic in nature. Furthermore, comparison and security analysis are presented with previously proposed systems.

KEYWORDS

Authentication, Contactless Payment, Magnetic Secure Transmission, Samsung Pay, Wormhole Attack

INTRODUCTION

The rapid growth in the technology has led to the development of many innovative services and applications in the field of payment systems. The transactions have turned from cashed to cashless. (Gupta & Quamara, 2018, 2019) discussed that to make the transactions cashless, smartcards were used as the credit/debit card, but they were prone to physical attacks, side channel attacks, and logical attacks. To make the cards more secure, different security algorithms that were combined with the smart cards and added biometric features for security and privacy (Nedjah et al., 2017, pp. 18-32). To reduce the time complexity and to provide ease to the user contactless smartcards were brought in use. Contactless smartcards were prone to sniffing attack and physical damage, and to overcome it mobile wallets and mobile contactless payment systems were used which are based on NFC (Near Field Communication) and MST (Magnetic Secure Transmission) (Andersson, 2016).

With the change in time, the methods to carry out the cashless transactions has also modified from smart cards to smart phones and internet banking. The current trends for e-cash payment includes the debit and credit cards, Samsung Pay, Google Pay, Apple Pay, Freecharge, Mobiwik, Jio money, SBI money, Paytm, Airtel money, pockets by ICICI, and many more mobile banking applications. These applications are provided by the bank, telecom industries and private industries. According to Wang et al. (2016), the key characteristics provided by the mobile wallets include the security, transferability, and anonymity. The mobile wallets are differentiated based on proximity payment technologies like NFC, MST, QR code, etc. There are certain threats to be considered against the basic mobile wallet components which are described in table 1.

DOI: 10.4018/JOEUC.20210301.oa1

NFC is a group of communication protocols which allows two electronic devices to establish communication by radio frequency, example- Apple Pay. NFC is a short-range half duplex communication protocol that creates communication between two devices at an operating frequency of 13.56 MHz. There are three modes of communication for NFC: reader/writer mode, peer to peer, and card emulation. MST is a technology for mobile payments which enables the smart phone to emit electromagnetic signals and mimic as the magnetic stripe on the credit/debit cards like Samsung Pay. MST sends the magnetic signals from user device to the card reader and emulates the swiping of a card. The transactions are made without upgrading the systems which is an advantage over the NFC. The NFC requires the card reader terminal to be upgraded in hardware and software aspect.

NXP semiconductors is a company that manufactures semiconductors and have splits the contactless possible application into four categories which depends upon the way the consumer will use the application:

1. **Touch and Go:** Application allows the consumer to tap the card on POS and no wait to confirm the transaction.
2. **Touch and Connect:** Link the two devices to exchange the data or money.
3. **Touch and Confirm:** User must confirm the transaction by entering password or fingerprint.
4. **Touch and Explore:** User is offered more than one features to make use.

Mobile contactless payment system stores the virtual debit and credit card information and allows the customer to use that information to securely pay for the purchases in store with those cards by tapping the smart phone in front of the radio frequency enabled readers (Andersson, 2016). The use of virtual card eliminates the threat to compromise of cardholder sensitive data. These systems working on the Near Field Technology (NFC) and Magnetic Secure Transmission (MST) technique provides notable advantages and is compliant to EMV standards. It provides multi-layer security and is convenient as it has eliminated the need to carry plastic cards. The popular applications which are in use nowadays are Apple Pay, Samsung Pay, Google Pay, and Pockets by ICICI bank (Bosamia, 2018). Other than the credit/debit cards loyalty cards can also be stored in these applications.

Depending on the amount of money transferred, the contactless payment can be divided into two groups - micro and macro. Micro payment is the one where the user makes a small contactless transaction. For this the user uses the contactless application 'touch and go', while the Macro payment is the one where the user transfers a big amount. For this the user will use the contactless application 'touch and confirm', where the transaction will be confirmed either by entering pin or by a physical signature.

To make the contactless transactions secure, the concept of tokenization is used. As these transactions are done without any physical connection with the terminal and the data is transmitted wirelessly, it is more prone to wormhole attack (Gupta & Narayan, 2020). Samsung Pay uses MST and (Korolov, 2016, para. 4) discussed that Salvador Mendoza detected eavesdrop on the MST transmission. (Vincent, 2016, para. 2, 3) discussed how this vulnerability enables the attacker to skim the cards and make fraud payments. (Kawamoto, 2017, para. 2,3) discussed how the leaked information can allow an attacker to learn much about the internal mechanism of Samsung pay, and the attacker can use the information for their own advantage.

In this paper we will propose a framework to secure Samsung Pay from wormhole attack with the help of an authentication server. The framework is different from the previously proposed schemes in multiple ways like complexity, data storage and key generation. The framework is designed to overcome the merchant threats, acquirer threat, payment application provider threat and threat to payment network provider. The rest of the paper is organized as follows- section 2 describes the background of the topic, section 3 describes the related schemes proposed to overcome the wormhole attack in contactless payment using MST, section 4 describes the proposed system, section 5 gives the details of implementation including the results and comparison and section 6 presents the conclusion.

Table 1. Threat model for mobile wallet

Mobile Wallet Component	Threats
User threat	Phishing, installation of malware applications, OS access permission, social engineering.
Device threat	Implementation issues, data interception, unauthorized access.
Application threat	Malware/rootkits installation, application tampering, reverse engineering, OS access permission.
Merchant threats	Relay attack on terminals, man-in-the-middle attack and malware on terminals.
Acquirer threat	Malware/rootkits installation, payment processing system compromise, data connectivity, mobile payment authorization repudiation.
Payment application provider threat	Compromise of cardholder sensitive data, DDoS attack, compromising token service data, privacy issue, transaction error.
Threat to payment network provider	Reliability of device and mobile network, data connectivity, token service compromise.

BACKGROUND

This section will give knowledge about some basic terms that are used in payment systems along with the current working model and threats identified in the current system.

EMV

EMV is an acronym given to Europay, Mastercard and Visa which is a global standard for the smart cards and the technology which is used for authenticating the transactions done by chip-based cards. EMV specifications are supported by banks, processors, merchants, and vendors and are not limited to terminal and card evaluation, managing interoperability issues and security evaluation (EMVCO). The EMV technologies are:

- Contact EMV – It refers to specifications related to contact chip cards and defines how the transactions should be conducted by the contact chip cards. In addition, it also supports the cryptographic functions to prevent card's counterfeiting and make them more secure.
- Contactless EMV – It refers to the transactions which are performed using NFC payment devices. These cards are supported by terminals which are EMV contactless enabled. It also supports functions to secure the card data and transactions.
- Mobile EMV – It refers to the specifications for mobile devices which have replaced the contactless cards. It also includes mobile payments and remote commerce by using the mobile.
- Payment tokenisation EMV – It provides a framework which describes the payment tokenisation system globally and works together with the existing payment system and provides digital support and new payment methods.
- QR code EMV – QR code is compliant to ISO 18004 for data encoding and visualising. EMV specification for QR code includes the use of QR code for making the payment. Merchant presented QR code and User presented QR code are the area to be focused.

Other than this 2nd generation EMV, secure remote commerce EMV and 3-D secure EMV are also the EMV technologies.

Payment Network

Card networks Mastercard, Visa, Discover and American express is in the centre of payment industry which provides users, merchants, consumers, banks and processors to communicate to perform the transaction. The processors are used to transfer money between the banks and to provide services to the merchants. In addition, the financial institutions are charged with fees for transactions that are based on total transaction volume (Chakravorti, 2003). The bank works with the user by issuing credit cards to them and works with merchants by issuing credits. Merchant works with financial institutions to accept the payments. In the payment system these institutions are referred as the merchant acquirers.

Tokenisation

To provide security to the contactless transactions, tokenization is used to eliminate the sniffing of original card details. (Tillman, 2019, para. 18) describes that tokenization is an operation were the important card details like card number, Card Verification Value (CVV), expiry date, etc are replaced by some substitute value which is known as the token Primary Account Number or Digitized (PAN). The original card details and its corresponding token value are securely stored on the Token Service Providers (TSP) (EMVCO). Tokenization service is provided by the global payment networks and is available for all card association members. Third-party TSP integration and TSPs are separately owned and operated by card issuers themselves. The guidelines are set by card issuers for the token service and perform the account verification and authorization of the cardholder during the token request period.

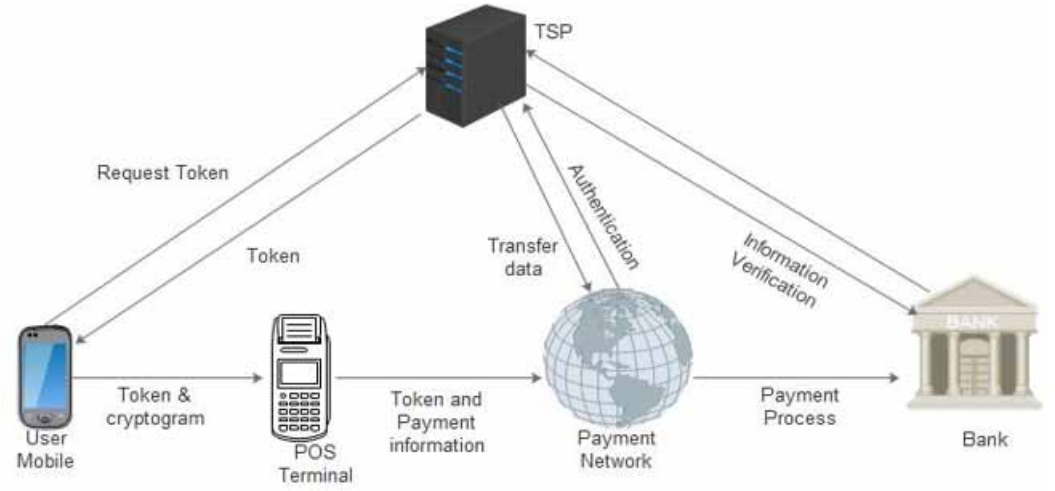
To ensure the integrity of the transaction, cryptogram is used which contains the encrypted information which is derived from the timestamp, DPAN, and Application Transaction counter (ATC) to prevent the transaction from replay attack. The cryptogram is created by using a cryptographic key which is based on the algorithm used by the card network. Depending on the card network, these keys can be static and dynamic and are stored securely in the trusted zone of the device. The tokens and keys are securely stored in encrypted form in the TEE (Trusted Execution environment) using a hardware-based device key which is unique for every device. During a transaction, the cryptogram is verified by the payment network on behalf of the issuer. On the failure of cryptogram match, the transaction is rolled back.

The current framework which is used by the Samsung Pay is described in Fig. 1. This framework is described to the best of my knowledge. (Acosta, 2019) describes that the user enrols his card in the application and the issuer performs the account verification during the stage of token request. On proper verification, tokens are generated by TSP and are stored in the trusted zone of the mobile device along with the keys used for generating the cryptogram. TSP provides token requester (TR) registration, security and control, token lifecycle management and process management. When a user performs any transaction, the token and cryptogram which is generated by the keys are binded together and forwarded to the payment terminal. The payment terminal forwards the received token along with the payment information to the payment network. The payment network on receiving the token verifies the cryptogram with the keys stored in payment network and on successful verification it fetches the account details corresponding to the token from the TSP. On receiving the account details, payment network forwards the payment details to the bank to complete the transaction.

To analyse the security of Samsung Pay, (Mendoza, 2016) analysed its Android Package (APK) and used Magspoof (Kamkar, 2015) to perform the wormhole attack. Wormhole attack allows the attacker to record network packets from one location tunnels it to another location and retransmits them there into the network. Magspoof is a device that can spoof/emulate any magnetic stripe or credit card. With the device the author captured the token and the cryptogram from a mobile device and performed the wormhole attack.

Another token capturing method was given by Choi & Lee (2018), where the author implemented an eavesdropping system that consists of magnetic signal collector, to transform the captured magnetic signals into electrical signals. A software module worked in a smart phone to decode electronic

Figure 1. Current payment scenario using MST



signals into payment information. These attacks identified poor authentication (Kaushik, S., 2019; DeviPriya, K. 2020) and authorization policy that leads to identity theft. To overcome the wormhole attack, schemes and protocols were proposed which are described in the next section.

RELATED WORK

To ensure system security (Tewari, A., 2020; Mirsadeghi, F., 2020), it is necessary to protect it from the wormhole attack. To prevent the attack certain schemes were proposed which are discussed below. The advantage and disadvantages of various scheme is presented in Table 2.

Cortier et al. (2017) proposed a protocol to secure the system from wormhole attack. The protocol is divided in two phases. In the first phase, the user provisions some of the tokens for the future transactions, when the user connects to the internet. The tokens are encrypted and are securely stored on the user mobile device. In the second phase, the user will initiate any transaction and the stored token will be used for it. It is decrypted by the key stored in the secure element of the mobile device, once the user authenticates on the device. The merchant id and the payment amount are attached to the token which cannot be changed. The token with lower count value will get invalidated on the successful use of the token with higher value. The security of the protocol was proven by Tamarin tool. The drawbacks for the defined protocols includes - it allows card holder to interact with both the honest and the rogue terminal and the token may be used until a new transaction is made by the user, which indicates that the system will have a limited impact on token stealing.

Ryu et al. (2017) proposed a system based on the location authentication by the wireless access point information (WI). The system used the media access control (MAC) address and the Received Signal Strength Indication (RSSI) which is retrieved by the Basic Service Set Identifier (BSSID). To identify the sections in the wireless local area network, BSSID is used. It can identify the routers and the access point by their unique address that creates the wireless network. The WI near the POS terminal collected by the user smart phone, compared with the wireless AP model (WM) built with the WI provided by the previous user. The comparison of received WI and the WM is performed on the Samsung pay servers. On failed comparison, relay attack is detected. The lack in the model is the creation of WM by the user provided information which can lead to the entry of rogue terminals on the server database by attacker. The system was developed under the assumptions that the servers, user smart phone and the POS are secure from active attacks.

POS authentication mechanism proposed by Bai et al. (2017) binds the token to a payment transaction and the POS terminal involved in the process, by fetching the terminal id through scanning the QR code. On getting the terminal id, the payer encodes the id into the payment token and to protect it from replacement during sniffing, adds one-way HMAC computation. Payment service provider compares the PID received by token and the terminal and a successful comparison leads to a successful payment. The keys used in hashing and encoding are the static keys and are stored on the user device which is the drawback of the scheme.

Rathee et al. (2018) proposed a hybrid genetic tabu search and optimization algorithm to secure the optimized test paths which was achieved by Samsung pay application activity diagram. The implementation of the proposed scheme was done in C++ on the case study of online airline reservation system and Samsung pay.

The proposed model in this paper overcomes the drawback in the different schemes and improves the current payment system security. The proposed model is discussed in the next section.

PROPOSED SYSTEM

In this section, the proposed system is discussed in detail, also elaborated the system entities and the threat and functional assumption.

Threat and Functional Assumption

While designing the proposed schemes following threat and functional assumptions were considered:

- **Communication Interception:** To collect the secret information, an ongoing communication may be intercepted by the attacker.
- **Second Authorization:** An attacker may try to participate in the system communication by rogue terminals without appropriate privileges.
- **Breach of Privacy:** The attacker may breach the user privacy by intercepting the communication and pretend to be an authorize user to the payment terminal.

System Entities

The system entities involved in the proposed system are discussed below:

- **Application Service Server (ASS):** The server that will provide the required payment application and services to the user. It is also used for the initial registration of the user. The user initial registration will provide the login credentials to the payment application.
- **Token Service Provider (TSP):** The server is used for the registration of the user's payment card. These servers are verified by the bank and on successful verification of the card details the token generated for the card is stored at the server and user account. Original card details are not stored on the server.
- **Terminal Authentication Server (TAS):** The server is used for the registration of the POS terminals. The server also authenticates the POS terminal during payment process, which eliminates the payment through rogue terminals. The TAS is authenticated by the application service provider and the channel between the user and TAS and between terminal and TAS is secure and encrypted.
- **Service Requester or User:** The person who request for the use of payment application. Before starting the payment, only once the user must register at ASS and the payment cards will be registered at TSP. The user on login to the application can use his cards to make payment.
- **Payment Server:** The server is used to process the payment request on successful cryptogram verification. In real world these servers are compliant to EMV standards.

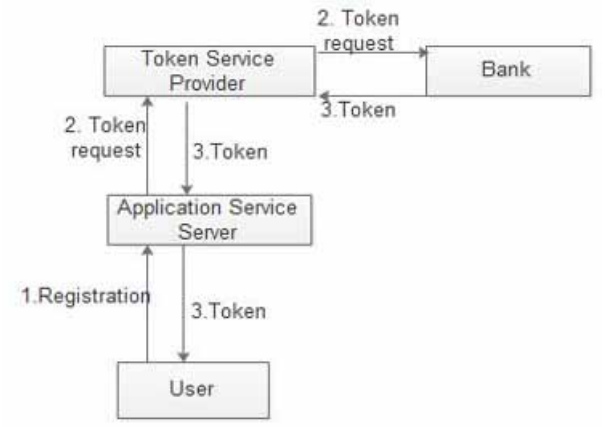
Table 2. Related Work

Year	Author	Description	Advantages	Disadvantages
2017	Cortier et al. (2017)	· Designed a protocol compatible with EMV static data authentication for payment, along with light use of secure element. · The security of the tool was proved by Tamarin.	· Prevents wormhole attack. · Secure from stolen key attack.	· Interaction with rogue terminal is possible. · Token can be used until new token with greater value is not generated.
2017	Ryu et al. (2017)	· A location authentication system whose main feature is to compare the WI provided by current user with the WM that was generated by the WI provided by previous user. · The system does not require any changes to the POS software or additional hardware.	· Prevents wormhole attack · Secure from key attack. · Model is identity based and not key based.	· Entry of rogue terminal on the server database.
2017	Bai et al. (2017)	· Demonstrated that an active attacker sniffs the token generated for payment and halts the ongoing transaction by different ways and performed the wormhole attack. · Proposed a solution POSAUTH that adds the terminal unique identity to the payment token. · POSAUTH binds the transaction to a particular terminal.	· Prevents wormhole attack. · Use one way hashing to prevent sniffing and replacement.	· Static keys used in hashing and encoding.
2018	Rathee et al. (2018)	· Testing of mobile pay solutions have several cases and optimization techniques are used to find the optimized test paths. · Proposed algorithm to secure the optimized test paths. · Implemented in C++.	· Experimentally, it is shown that proposed technique is more effective in automatic generation and optimization of test paths comparing to the simple genetic algorithm.	· Using the technique to overcome wormhole attack can be time consuming.

Proposed System and Working

Figure 2 shows the registration phase and Figure 3 shows the model of system proposed in this scheme. In this model, the user first registers to the ASS to use the application. After registration, add a card for payment and for every card a token is requested. On successful validation of user credentials, token is generated and stored in the TSP and user device. To perform any transaction, the user will first scan the QR code corresponding to the payment terminal and sends a key generation request to TAS which will provide user and the POS terminals the keys for the transaction. The TAS will generate keys only for the registered POS terminals. The user device will encrypt the token with the key and forward it through MST to the POS terminal. The POS terminal will decrypt the token

Figure 2. Registration phase



and send it to the payment server, which performs the token verification by TSP. As only the POS for which the transaction was initiated will have the decryption key, it will prevent system from the wormhole attack. On successful token verification, forwards the payment process request to the bank for payment. Mathematical representation of the scheme is described in the next sub section.

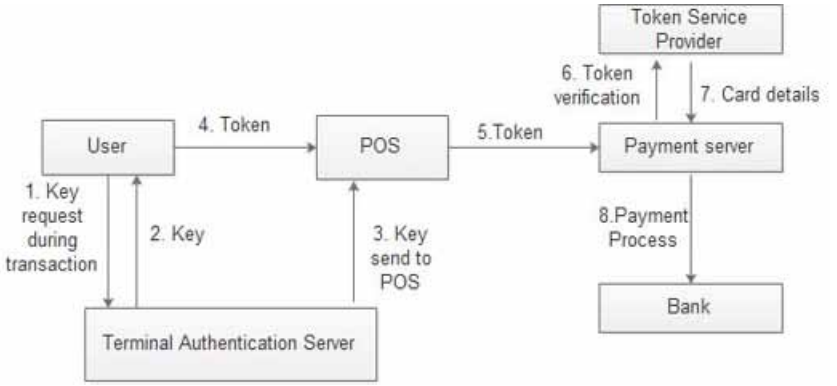
For authentication purpose, the system involved the use of Elgamal encryption algorithm. The algorithm is used for asymmetric encryption which is built on the Diffie-Hellman key exchange. The algorithm is secure as its security depends on difficulty in computing discrete logarithms in the cyclic group which means for instance if the attacker knows g^r and g^t it will be difficult for him to compute g^{rt}, where g is a generator of a cyclic group and r and t are some random numbers.

Mathematical Representation of Phases

The working of the proposed system is divided into 5 phases which includes – Registration phase, Login phase, Key generation phase, Authentication phase, and Payment phase. The notations which are used in the proposed scheme are described in Table 3:

1. Registration phase – In this phase a new user U_a who wishes to use the payment app, will create an account by getting register to the payment application on ASS:
   a. During the registration, U_a will enter the personal details and mobile number and a pin to access the application, which will be stored in the database of application. The U_{id} and P_{in} will be stored in the application database.
2. Login Phase – During the login phase, the user will enter his card details to add it to the application for use:
   a. After getting registered to the application, U_a will login to the application by using U_{id} and P_{in} and enter the payment card number $PC_{i,}$ pin and expiry date.
   b. The details get verified by the issuer bank, and a token T_i for the card generated by TSP will be added to the user account and the key K_i will be stored in secure unit.
3. Key generation phase – In this phase the user will initiate for the payment and send the details to the POS terminal. This phase will work in two parts:
   a. U_a will scan the QR code attached to the payment terminal, by which the application will retrieve the terminal id T_{id}' and will be send along with U_{id} to TAS for the key generation. TAS will generate the keys using Elgamal algorithm, and the public key 'Pk', will be send to U_a along with g_1 and g_2 and private key 'Pv' and U_{id}' to T_{id}. Every private key Pv_i will be defined for every other user U_a for every transaction.

Figure 3. Proposed model



The application will append the T_{id}' to U_{id} to m and encrypt it with the terminal public key, which will be forwarded to the terminal along with T_i and the cryptogram C_z generated by using K_i:

$$C_1 = g_3 * m \quad (1)$$

where:

$$m = (U_{id+} T_{id}') \quad (2)$$

and:

$$g_3 = g_1 \text{^} Pk \quad (3)$$

$$M = T_i + C_z + (C_{1,} C_2) \quad (4)$$

where $C_2 = g_2$, g_2 is derived from generator g and Pk and g_1 is derived from generator g and Pv.

4. Authentication phase – In this phase the POS will decrypt the received message M. The part of message involved in decryption is (C_1, C_2), which will be decrypted by Pv using Elgamal algorithm:

$$Z = D\,(C_1, C2)_{Pv} \quad (5)$$

After decryption, T_{id}' and U_{id} will be retrieved and compared with T_{id} and U_{id}'. And if:

$$T_{id} = T_{id}' \quad (6)$$

and:

Table 3. Terms used in proposed scheme

Terms	Description
U_a	User
U_{id}	User id
P_{in}	User pin/password
PC_i	Payment card number
T_i	Token generated for card PC_i
K_i	Key used for generating cryptogram
T_{id}	Terminal id
M	Appended terminal id to user id
C_z	Cryptogram

$$U_{id}' = U_{id} \tag{7}$$

The terminal will forward T_i and C_z to the payment server for processing the transaction else the transaction will decline at the terminal end.

5. Payment phase – In this phase, the payment terminal will receive T_i and C_z and will verify the C_z, and if verified successfully then send a request to the TSP for card number to the corresponding token and forward the received information to the bank for completing the transaction. In addition, for two level securities the bank will send a transaction confirmation message to the customer registered mobile number. And on confirmation the transaction will be completed.

IMPLEMENTATION

This section of the paper will discuss about the implementation of the proposed system. It will include the hardware and software requirement, results of the implementation and comparison with the related work.

Hardware and Software Requirement

To implement the proposed system, the hardware requirement includes the 2 GB RAM and 2 GB hard disk. The software requirement includes the 32-bit operating system, Visual basic .NET, and SQL server. The language used for implementation is C#. The database is self-created which is maintained in SQL server. The database was created for the credit card data, user personal information, merchant id, and TSP. AVISPA tool is used for simulating the results of the scheme.

AVISPA stands for Automated Validation of Internet Security Protocol and Application. Its main aim is to develop an industrial strength technology that can be used to analyse the large-scale internet security-sensitive protocols and the applications. AVISPA also provides SPAN which stands for Security Protocol ANimator, that can help the users in wiring the HLPSL (High Level Protocol Specification Language) specification. HLPSL builds the Message Sequence Charts (MSC) for the protocol in execution. SPAN can also be used to implement active intruders in the protocol that help in building and finding attacks over the proposed protocol.

To implement the solution on the practical basis, we require Magspoof device – to emulate a magnetic stripe card. In addition, we require a magnetic credit card reader for POS system which can

Table 4. Requirement and specification

Requirement	Specification
Hardware	· 2 GB RAM · 2 GB Hard disk space · Magspoof · MSR90 USB card reader
Software	· 32 bit Operating System · Visual Basic .NET · SQL server · AVISPA
Language	· C# · SQL

read up to 3 tracks and can reads ISO7811, CA DMV AAMVA, and most other card data formats. The servers can be maintained on SQL server.

Results

The data generated during the implementation process was stored in the SQL server and the Fig.4 shows the encrypted message generated and is passed from user device to POS terminal through magnetic secure transmission. The figure contains the encrypted message for different transactions. The message shown in Fig. 4 contains the token T_i which is the substitute value for the original card number along with the cryptogram C_z. The cryptogram and token are separated by '@'. The message which will be transferred from user device to the POS terminal will contain the message, c1 and c2:

$$M=\text{message}+ (C1, C2) \tag{8}$$

C1 and C2 will be used for user and terminal authentication and message will be used to process the payment.

c1, c2 on decryption with the private key on the terminal side will provide the user id and the merchant id which as shown in Fig. 5. The user id will be verified by the terminal with the id send by TAS along with terminal id verification. If the verification is successful, the message value which contains the token and cryptogram will be forwarded to the payment network. The payment network on successful verification of cryptogram will further complete the transaction by sending the transaction details and user details to the bank.

Security Analysis

The following properties are satisfied by our proposed scheme:

- Card anonymity – In this scheme, it is assumed that the card details are kept anonymous. In another word, if the payment request at the terminal is intercept by the attacker, then the true card details of the user will not be revealed.
- Prevention against wormhole attack – In this scheme, to prevent the wormhole attack, the generated token is binded to a terminal. If the token gets captured it cannot be used for transaction on some other terminal.
- Prevention against key stolen attack – The keys used for encrypting the message are dynamic in nature and hence cannot be stolen from user device. In the scheme, it is assumed that the keys transmitted to user and terminal through a secure channel approved by the application service provider.

Figure 4. Encrypted message to POS terminal

Table - dbo.authentic

message	c1	c2
9209343172771905@10649831374010314253	605755698171875	125
9263393798405665@02256585217800682462	3023146158848	16
5195683852144359@03201768438702248295	51524578972224	12
2027395371346198@12289461890752221746	65210795261721	3
NULL	NULL	NULL

Figure 5. Decryption process

Table - dbo.authentic

message	c1	c2
9209343172771...	605755698171875	125

Table - dbo.auth

uid	mid
64683	387683

Figure 6. Proposed system execution on AVISPA

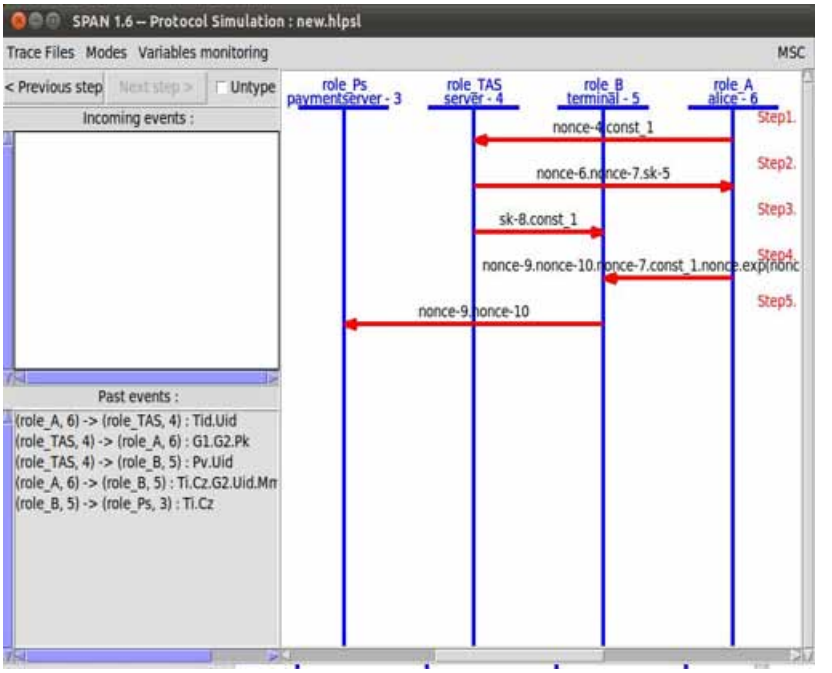


Figure 7. Result of simulation under ATSE model

- Prevention against rogue terminals – The terminals used to carry out the transaction is authenticated by the authorization server which eliminates the use of rogue terminals by the attacker.
- Prevention against the electromagnetic side channel attack – Due the dynamic nature of the keys used in encryption and decryption, the proposed solution secures the system from electromagnetic side channel attack.

Comparison

The proposed system is different from the current use system of Samsung pay as it contains the encrypted user and merchant ids which are not present in the Samsung pay structure:

- If compared to Cortier et al. (2017), the user was able to communicate with the both rogue and honest terminals, but the proposed system will only be able to communicate with the registered terminals.
- The system proposed by Ryu et al. (2017) depends on location authentication by the wireless access point information (WI), but the proposed system is independent of location and location authentication.
- The system proposed by Bai et al. (2017) binds the merchant id and one-way HMAC to the token for authentication and uses static keys which are different from the proposed system as it binds the encrypted user and merchant ids to the token and uses dynamic keys to encrypt them. The proposed system does not use the one-way HMAC.

For every transaction, the generator g and private keys will be dynamically generated and will be deleted on successful comparison by the POS terminals. The encrypted user and terminals ids vary from transaction to transaction which will eliminate the wormhole attack and there is negligible possibility that the attacker uses the same terminal for the wormhole attack while the user is performing

Table 5. Comparison with another proposed schemes

Comparison Parameter	Cortier et al. (2017)	Ryu et al. (2017)	Bai et al. (2017)	Proposed System
Communication with rogue terminal	Yes	Yes	No	No
Location authentication	No	Yes	No	No
Hash	Yes	No	Yes	No
Keys used	Static	No	Static	Dynamic

the transaction. Also, if a token gets captured and if a new token is successfully used it will eliminate the entire previous token with less counter value.

CONCLUSION

In the last few years, the rate of cashless transactions has increased due to the ease provided by them to the customer. Numbers of applications are present to perform a cashless transaction, and they differ based on the method used to carry out the transaction like – QR code, UPI id, NFC, MST, etc. The applications using MST for cashless transactions were detected by wormhole attack. So, in this paper, we proposed a novel framework to overcome the wormhole attack in such applications. To prevent the attack with minimum complexity, authentication server is used to authenticate the communication between the user and the terminal. Some of the earlier proposed schemes are also discussed and the security analysis has been presented. The system simulation on AVISPA is presented along with the result simulation on ATSE model.

REFERENCES

Advantio. (n.d.)https://www.advantio.com/blog/mobile-payments-with-digital-wallets-and-tokenization-how-google-pay-apple-pay-and-samsung-pay-protect-your-card-details

Andersson, D. (2016). *A survey on contactless payment methods for smartphones*. Academic Press.

Bai, X., Zhou, Z., Wang, X., Li, Z., Mi, X., Zhang, N., . . . Zhang, K. (2017). Picking up my tab: Understanding and mitigating synchronized token lifting and spending in mobile payment. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 593-608). USENIX.

Bosamia, M. (2018). *Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures*. Academic Press.

Chakravorti, S. (2003). Theory of credit card networks: A survey of the literature. *Review of Network Economics*, *2*(2). Advance online publication. doi:10.2202/1446-9022.1018

Choi, D., & Lee, Y. (2018). Eavesdropping of Magnetic Secure Transmission Signals and Its Security Implications for a Mobile Payment Protocol. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 42687–42701. doi:10.1109/ACCESS.2018.2859447

Cortier, V., Filipiak, A., Florent, J., Gharout, S., & Traoré, J. (2017, April). Designing and proving an EMV-compliant payment protocol for mobile devices. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 467-480). IEEE.

Dark Reading. (n.d.). https://www.darkreading.com/threat-intelligence/samsung-pay-leaks-mobile-device-information/d/d-id/1330480

DeviPriya, K., & Lingamgunta, S. (2020). Multi Factor Two-way Hash-Based Authentication in Cloud Computing. *International Journal of Cloud Applications and Computing*, *10*(2), 56–76. doi:10.4018/IJCAC.2020040104

EMVCo. (n.d.). https://www.emvco.com

Gupta, B. B., & Narayan, S. (2020). A Survey on Contactless Smart Cards and Payment System: Technologies, Policies, Attacks and Countermeasures. *Journal of Global Information Management*, *28*(4), 135–159. doi:10.4018/JGIM.2020100108

Gupta, B. B., & Quamara, M. (2018). A taxonomy of various attacks on smart card–based applications and countermeasures. *Concurrency and Computation*, e4993. doi:10.1002/cpe.4993

Gupta, B. B., & Quamara, M. (2019). *Smart Card Security: Applications, Attacks, and Countermeasures*. CRC Press. doi:10.1201/9780429345593

Kaushik, S., & Gandhi, C. (2019). Ensure Hierarchal Identity Based Data Security in Cloud Environment. *International Journal of Cloud Applications and Computing*, *9*(4), 21–36. doi:10.4018/IJCAC.2019100102

Magspoof. (n.d.). https://samy.pl/magspoof/

Mendoza, S. (2016, July). Samsung Pay: Tokenized numbers, flaws and issues. In Proc. Black Hat USA (pp. 1-11). Academic Press.

Mirsadeghi, F., Rafsanjani, M. K., & Gupta, B. B. (2020). A trust infrastructure based authentication method for clustered vehicular ad hoc networks. *Peer-to-Peer Networking and Applications*, ●●●, 1–17.

Nedjah, N., Wyant, R. S., Mourelle, L. M., & Gupta, B. B. (2017). Efficient yet robust biometric iris matching on smart cards for data high security and privacy. *Future Generation Computer Systems*, *76*, 18–32. doi:10.1016/j.future.2017.05.008

OnlineC. S. O. (n.d.). https://www.csoonline.com/article/3132360/mobile-security/researcher-unveils-second-samsung-pay-vulnerability.amp.html

Pocket. (n.d.). https://www.pocket-lint.com/apps/news/samsung/132981-what-is-samsung-pay-how-does-it-work-and-which-banks-support-it

Rathee, N., & Chhillar, R. S. (2018). Model Driven Approach to Secure Optimized Test Paths for Smart Samsung Pay using Hybrid Genetic Tabu Search Algorithm. *International Journal of Information System Modeling and Design*, *9*(1), 77–91. doi:10.4018/IJISMD.2018010104

Ryu, G., Seo, C., & Choi, D. (2017). Location authentication based on wireless access point information to prevent wormhole attack in Samsung pay. *Advances in Electrical and Computer Engineering*, *17*(3), 71–77. doi:10.4316/AECE.2017.03009

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*, *108*, 909–920.

The Verge. (n.d.). https://www.theverge.com/platform/amp/2016/8/9/12410716/samsung-mobile-pay-token-hack-defcon

Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In *2016 second international conference on mobile and secure services (MobiSecServ)* (pp. 1-5). IEEE.

B. B. Gupta received PhD degree from Indian Institute of Technology Roorkee, India in the area of information security. He has published more than 250 research papers in international journals and conferences of high repute. He has visited several countries to present his research work. His biography has published in the Marquis Who's Who in the World, 2012. At present, he is working as an Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra, India. His research interest includes information security, cyber security, cloud computing, web security, intrusion detection, computer networks and phishing.

Shaifali Narayan is currently pursuing her Master's degree in Cyber Security from National Institute of Technology, Kurukshetra, India. She has received her Bachelor's degree in Computer Science and engineering from Invertis University, Bareilly, India, in 2015. Her current research interest areas include security in Internet of Things (IoT), authentication in smart card technology and payment systems, and data privacy.