Mobile Payment Transaction Model with Robust Security in the NFC-HCE Ecosystem with Secure Elements on Smartphones

Lucia Nugraheni Harnaningrum[1]
Department of Information Technology, Indonesia Digital Technology University, Yogyakarta, Indonesia

Ahmad Ashari[2], Agfianto Eko Putra[3]
Department of Computer Science and Electronics
Gadjah Mada University, Yogyakarta, Indonesia

***Abstract*—The Near Field Communication embedded (NFC-embedded) smartphone consists of two ecosystems, namely Near Field Communication Subscriber Identity Module Secure Element (NFC-SIM-SE) and Near Field Communication Host Card Emulation (NFC-HCE). NFC-SIM-SE places secure elements in smartphones, while NFC-HCE places secure elements in the cloud. In terms of security, the location of secure elements in the cloud is one of the weaknesses of NFC-HCE. The APL-SE transaction model is developed as a solution to improve transaction security with NFC-enabled mobile. This model moves the secure elements of the NFC-HCE ecosystem from the cloud to the smartphone so that when the transaction is made, the smartphone does not communicate with the outside network to access the secure element. The APL-SE transaction model is tested using dummy data to calculate the processing time measurements for each step. The model is also tested for the encryption process. The encrypted data is compared with the original data, then the randomness is calculated. This transaction model is also tested by looking at the data randomness, which shows that the encrypted data is declared random. Random data increases data security. The transaction model test shows that the transaction runs well because the encrypted data is proven random, and the execution time is 1,074 ms. The time of 1,074 ms is far below an attacker's time to decipher the encrypted data. Random and fast encryption results indicate that transactions are secure. This achievement makes the opportunity for attackers to manipulate data small, so security is increased.**

***Keywords*—Transaction; near field communication; mobile; secure element; encryption**

I. Introduction

Smartphones have become tools and facilities that are used daily by people in general. The use of smartphones is not only for communication itself. It is also used for other purposes such as accessing news, doing office work with applications that can be installed on smartphones, and even for business transactions. According to [1], the development of non-cash transactions is increasing from time to time. Nowadays, mobile transaction uses digital wallets. It is already widely used by banks and non-banks [2].

Payment transactions using Near Field Communication (NFC) are an alternative digital payment method. Payments with NFC have advantages in transaction speed, secure storage of card data networks can be deleted remotely [3]. The implementation of devices for transactions with NFC has been carried out, including the existence of a payment authorization system using Near Field Communication - Radio Frequency Identification (NFC-RFID) devices [4]. Payment systems using a cam-wallet also use NFC to communicate with merchants [5]. Smartphones with NFC hardware were around 64 percent in 2018, and NFC-enabled Point of Sales (POS) reached 53 percent globally in 2007 [6].

NFC-enabled mobile communication has two ecosystems [7]. These ecosystems are NFC Subscriber Identity Module Secure Element (SIM-SE) and Host Card Emulation (HCE). NFC SIM-SE performs transactions without an internet connection because Secure Element (SE) is on the smartphone. NFC-HCE requires an internet connection because SE is in the cloud. This condition makes security a significant problem in using NFC-HCE, so appropriate actions are needed to protect payment security. SE being moved to the cloud causes the need to send credential keys from the cloud to the device. However, the NFC-HCE ecosystem that does not need to use a SIM in its implementation can be an advantage and will be more widely applied in the future. NFC-HCE is also a solution in several countries' NFC mobile payment systems, which enforces SIMs produced without SE.

Therefore, this study develops an application-based NFC-HCE Model to optimize the performance of NFC-HCE in a mobile payment system to allow the use of a SIM with or without an SE to securely make NFC mobile payment transactions. The model implements SE in the NFC-SIM-SE ecosystem into the NFC-HCE ecosystem and stays in the smartphone. This model allows communication between devices (smartphones and NFC readers) by implementing a transaction system with the support of a security system. Overall, the model consists of two main parts: initialization and transactions. The initialization stage involves preparing an NFC-enabled smartphone for transactions, namely by registering to the server, both users (smartphones) and cards (one user can have many cards). The initialization model ensures that the credential data is stored in the smartphone safely and verified [8]. The transaction stage contains transactions between NFC from the card owner's smartphone to the point of sales (POS). In this study, the discussion focuses on developing the transaction section, which sends secure data between the cardholder's smartphone and POS, namely APL-SE.

The result of this research is a model that can be developed into a payment system protocol. The model can be used on a small or large scale of payment. Sellers and buyers must have a smartphone that has NFC-HCE facilities. Payment systems at small and large shops that use online payment systems can use APL-SE as a means.

The structure of this paper is as follows. After this introduction, it will present the research on mobile payment systems that have been carried out before. Then it is connected with the study that will be made and its novelty analyzed. The following section discusses the proposed mobile payment system model. This proposed model performs transactions in the NFC-HCE ecosystem that does not connect to the internet because the secure elements are already stored in the smartphone. Thus, the model reduces the risk of data being misused due to the smartphone connected to the server via a public internet network. This model can prevent attacks that occur because of data retrieval at the time of use and stored for use at another time. The model can also prevent attacks that may occur because the retrieved data is used at other transaction times. Then, the model is tested and analyzed to get a conclusion whether the model can prevent the attack.

II. Related Work

Badra [9] uses a user identity accompanied by a random value for authentication. The Badra model uses the NFC-SE ecosystem, which emulates the card. The solution to prevent NFC-related attacks is using certificate-based authentication between PoS and TTP and shared-secret-based authentication between TTP and NFC-enabled devices. The assumption is that the secret key shared between the TTP and the mobile is securely stored in the SE. Its cryptographic calculations are also performed inside the SE. The Badra model uses five stages, is simpler, and can overcome some of the possible attacks.

Poughomi and Grønli et al. [7] proposed the NFC protocol to be implemented on the Web of Things (WoT). This protocol is divided into two parts; the authentication and transaction sections. Transactions from a merchant terminal (POS) to a communication smartphone use NFC and from a smartphone to an MNO using a GSM line with SMS. Currently, the model of communication with SMS done several times is not so popular anymore.

Nashwan [10] proposed a secure authentication protocol for NFC (SAP-NFC). It is a protocol to overcome replay attacks, impersonate attacks, to track attacks, and desynchronize attacks using the registration and authentication phases. This security model uses a hash function and multiple authentications. The SAP-NFC protocol is more likely to overcome attacks because authentication is carried out for each data exchange.

Cossman and Liu [11] proposed two authentication steps. This research shifts the protection of user data to a user-centered approach. The first authentication uses the system keystore, and the second uses a passcode. Meanwhile, the two-factor authentication proposed by Munch-Elinsen et al. [12] is by providing the user with a PIN code twice. This authentication is divided into five phases. The PIN is entered in the first phase, where the user enters the PIN into the application, and in the fifth phase, the user also enters the PIN again to be verified by the POS. The two proposals for two-factor authentication are attempts to secure transactions. Cossman's proposal is simpler because it does not require other parties, while Munch-Elinsen's proposal requires other parties to send and receive SMS.

Cryptography is used to design security tags by consuming less energy. The cryptographic methods used are Asymmetric Cryptography and Symmetric Cryptography; encryption and decryption using Advanced Encryption Standard (AES-128), and digital signature generation using elliptic curve digital signature algorithm. Özcanhan et al. [13] proposed The EKATE protocol. The protocol uses asymmetric encryption for secure data communication. The AES algorithm is used to encrypt the data to be sent to and from the tag.

The relay attack scenario is made on a system that involves smartcards; smartphones on both Relay attacks attack smartphones by changing peer-to-peer mode into Card Emulation mode, then reading the smartcard. The message is captured and forwarded to the proxy device, and the device sends the message as if it were the real owner of the smartphone. These relay attacks occur at the application layer, so they must take real-time countermeasures. Dang Zhou et al. [14] studied relay attacks on NFC by analyzing the weaknesses of ISO / IEC 14443-4 when facing relay attacks. This drawback appears to be quite common to all types of AFC systems that follow this standard globally. Then an experimental relay method was designed and carried out a relay attack. The results show that the protocol is vulnerable to attack. Two counterattacks are also proposed and discussed the feasibility and practicality of these countermeasures. The results show that the attacks carried out successfully generated delays during transactions. Sujithra et al. [15] proposed a data encryption protocol to be stored on a smartphone with three tiers tested in local smartphone and cloud environments. The test results show that in terms of the speedup ratio, the combined algorithm AES+MD5+ECC is better, and the AES algorithm is better in terms of average processing time.

Al-Fayoumi and Nashwan [16] use the registration stage to ensure that NFC devices are registered in the AuC database. This registration stage uses four steps: sending a registration request message containing identity and a random number, AuC generates a secret key based on the parameters in the request message, and a confirmation message is sent back to the NFC device by the AuC. The NFC device executes a derivative function to obtain the secret keys. The authentication phase is the second stage of the secure authentication protocol for NFC mobile payment systems (SAP-NFC). POS and mobile NFC carry out initial authentication. POS generates random numbers and sends them to NFC mobile. NFC Mobile uses this random number to initiate the authentication challenge message. After the message is processed using these parameters, it is sent to the NFC POS. AuC verifies NFC devices with a set of identity and authentication parameters. The design of the SAP-NFC protocol fulfills the following requirements. First, all parties involved in authentication can generate random numbers. Second, the AuC and the NFC device can update the secret key for each authentication session. Third, both the old secret key from the previous

authentication session and the new secret key from the current authentication session of the NFC device will be stored in the AuC database. Fourth, mutual authentication must be carried out between all parties involved in authentication. Fifth, the KDF function (Derivation function) derives the new session key. Sixth, the identity of the party performing the authentication is hidden by a series of hash functions. As a result, the SAP-NFC protocol claims to achieve the highest level of security with mutual authentication, forward/backward secrecy, anonymity, and untraceability. The SAP-NFC protocol can also defeat attacks such as replay attacks, impersonation attacks, tracking attacks, and desynchronization attacks.

Alatar and Achemlal [17] stated that pure HCE has not been trusted for payments but has attracted the attention of Visa and Master cards. It still needs efforts to earn that trust. Asaduzzman et al. [18] stated that NFC is suitable for IoT devices. This paper discusses the protocol for sending data in NDEF format. This protocol uses certificates. Transaction data security is carried out in several ways. The first way is a modified certificate. This method is initiated by requesting a certificate via a handshake and will terminate the transaction if the certificates are not the same. The second way is with modified data. If the signatures do not match, it means that there is a modification to the data, then the data is discarded. There is a hash code matching mechanism between the message and the signed hash. Jamming attacks can be detected in the presence of interference. So, if there is interference, data is prohibited from being stored.

Alzahrani [19] identified an attack with a reapplication tag with TRD by tracking how many times the tag was read. The tag should only be read once when the goods are distributed and reach their destination. The original tag is already considered a second reading if the verified tag is fake. Pourghomi, Piere, et al. [7] developed an NFC protocol that begins with user authentication. You do this by checking the validation by checking the PIN. Then the data is stored in the tamper-resistance chip. All of that is done in the NFC-HCE ecosystem. Wenxing [20] created an NFC communication mechanism to prevent eavesdropping using electronic circuits. As a result, it can reduce the threat of eavesdropping. Fan et al. [21] created a protocol beginning with initialization. At the initialization stage, a pseudorandom generator and key are generated. Then put both in the valid and legitimate reader tags. At the tag identification stage, the reader generates a random timestamp and random number and sends an authentication to the tag. The time received must be greater than the time to transfer, otherwise, authentication is not successful. From the security side, the attack is detected with a timestamp for an anti-DoS attack scheme.

Nour et al. [22] overcome Replay attacks and Man in the Middle Attacks that often occur in NFC-enabled mobile transactions by creating a security protocol. This security protocol is used for mobile transactions. Prevention of replay attacks is done by using random numbers and timestamps. Meanwhile, the prevention of the Man in the Middle Attack is prevented by mutual authentication between the client's payment device and the small merchant's NFC smartphone. This payment architecture can also facilitate mobility because it uses mobile devices and is secure because the proposed protocol can solve EMV vulnerabilities without changing EMV principles.

The use of cards for travel has been used, one of which is AFC payments using LessPay. Fan Dang et al. [23] research shows that tampering with entrance data and relay attacks on AFC cards must be watched. This study simulates the attack and provides a solution for its prevention.

The NFC transaction security protocol was proposed by Ali Al-Haj et al. [24]. This protocol is successful in preventing malicious network attacks such as the impersonation and replay attack, the session key security attack, the brute force attack, and the Man-in-the-middle attack. These attacks are prevented by mutual authentication, non-repudiation of transaction messages, data integrity, confidentiality, data privacy, and validity of Banking Data. This protocol involves actors. The first actor is NFC-enabled mobile. This device is the main device in this mobile payment. This NFC-enabled mobile will communicate with the Management Authentication Server (MAS) to obtain a session key. The second actor is POS. This POS communicates with NFC-enabled mobile for transactions and with the issuing bank (BI) via a secure channel (TLS). The third actor is BI. BI communicates with POS to verify Mobile payments in online EMV transaction mode. The fourth actor is MAS. MAS provides management and authentication for secure mobile payment transactions.

Prevention of attack by brute force was carried out by Madhoun, M et al. [25]. On payment processing, each transaction takes about 500ms; therefore, to achieve this attack, one needs to have access to the client's payment device for 38 minutes. Although NFC is claimed to be able to communicate at short distances (only up to 10 cm), it has been proven that relay attacks can carry out attacks when communication occurs with NFC. The attack is carried out by adding an amplifier to extend the reading distance. This attack can retrieve credential data and use it for online transactions at another time. Authentication to the client is carried out with a PIN that is verified with the PIN data stored on the server in two ways, namely online verification with symmetric encryption and offline with an asymmetric key to the issuing bank or by comparing the PIN stored in the memory of the client's payment device. Verification can also be done with a signature by the client or without the Cardholder Verification Method (CVM). Verification without CVMini is used for fast payments and in small nominal amounts.

The transaction begins by entering the username and password. If the authentication server identifies as a valid user, the server will send a one-time password (OTP). The transaction will time out after a particular time. The user will be notified if the attacker cannot complete the payment process within the specified timeframe (30 seconds for Apple Pay). It not only places a time limit on the attacker but also raises consent issues [26].

Security and user trust issues are issues that are widely discussed in research on NFC-based mobile payment systems. Protocols or models have been built trying to overcome these problems. However, existing models still have gaps in vulnerability to attacks. One of them is an attack carried out during the transaction because of the communication from the

smartphone to the financial institution server. This study reduces this vulnerability by creating a model that does not require communication between smartphones and financial institution servers during smartphone transactions with POS using NFC-enabled mobile. It also has advantages in the amount of data exchange and the absence of communication from smartphones to financial institutions during transactions. This situation occurs in the HFC-HCE ecosystem.

III. Proposed Method

The proposed NFC mobile payment system consists of two stages: initialization and transaction, and this paper focuses on developing the transaction stage. The payment card is declared safe to be stored on the smartphone during the initialization process. The payment card is ready to be used for transaction processing. The transaction model ensures that transactions between the cardholder's smartphone and the POS are safe and correct. The architecture of the proposed model is shown in Fig. 1.

This transaction model puts the security system in the HCE ecosystem into smartphones. A security system is created in the form of an application that will ensure data security and communication between smartphones and POS. The security system refers to the SE hardware inside the SIM card in the NFC-SIM-SE ecosystem. Element identification is made by synthesizing NFC-SIM-SE elements and NFC-HCE elements in the cloud into application elements. Elements in both ecosystems are analyzed and then adapted to security system applications.

This transaction model is a model for data usage. In this model, data security is carried out only when communication is carried out using NFC-HCE. Two things will be prevented. The first is to make data safe from attackers, and secondly, when there is a data request, the data will be sent to the right place. Secure element created we will refer to as APL-SE. APL-SE on smartphones was used for transactions, and at that time, three entities were involved, namely smartphones, POS, and Financial Institutions. This study focuses on the security of transactions between smartphones and POS.

The smartphone and the POS transaction model are carried out with NFC-HCE communication in card emulation mode. In this mode, when a transaction is made, the smartphone and the POS communicate by acting as the initiator and target. When sending data, the smartphone or POS acts as the initiator and the others as the target. This model is shown in Fig. 2.

The first step, POS as a target, sends data on the number of purchases to the smartphone. Currently, POS is the target, and the smartphone is the initiator. The smartphone activates the HCE service and starts the transaction by sending a connection request to the POS. The smartphone taps it for this delivery. The data sent is String data which contains information on the payment amount. This process is shown in Fig. 3.

The transaction model created to enable these two devices enables the HCE service. In the beginning, POS recorded transaction data, then saved the data to a shared preference variable. The smartphone sends a request as an APDU command to the POS, and the POS responds by providing a response that is processing the APDU command. This response brings the amount of transaction data prepared previously by the POS.

In the second step, the smartphone receives the data, then activates the SE software. Notification of approval to POS is done by sending card data to POS. The smartphone verifies the request from the POS, then activates the smartphone application. The smartphone application requests a pin from the user, and this pin is stored in the data stored on the smartphone during the initialization process. When a pin is entered, it is matched utilizing a pin stored in an encrypted state, decrypted first, and then matched with the input data. If the pin matches the data, the process is continued. Otherwise, it is closed. Currently, smartphones are the target, and POS is the initiator. If the pin is correct, an RSA encryption key (KeyRSA) will be generated. The selected card is retrieved data, then stored in a JSON Object (JSON (Dcard Key data and files, which are already stored during the initialization process, are encrypted (Enkr(Dtrans)). This encrypted transaction data is sent to the POS (ED).

In the third step, after the POS receives the card data, the POS verifies the card data to the financial institution server and gets an approval notification if the data matches. POS as the initiator and financial institutions as the target, the data sent from the smartphone is received by the POS and then decrypted. Previous data plus payment data.

$$Dtrans = Duser + Dpay \quad (1)$$

The data is encrypted by the POS and sent to the Financial Institution.

$$Etrans = E(RV, Dtrans) \quad (2)$$

In Financial Institutions, data is decrypted and matched with customer data. The authorization code is encrypted (OT) if the Financial Institution is verified. If it is not verified, an unverified message is sent. Financial Institutions send data or notifications to POS.

In the fourth step, the POS executes the payment and sends a notification to the smartphone if the transaction has been successful. POS is the initiator, while the smartphone is the target. Authentication data and smartphone data are decrypted, as are user data decrypted. Next, the payment process is carried out. The process is completed by sending a notification to the smartphone. Currently, POS is the initiator, and the smartphone is the target.

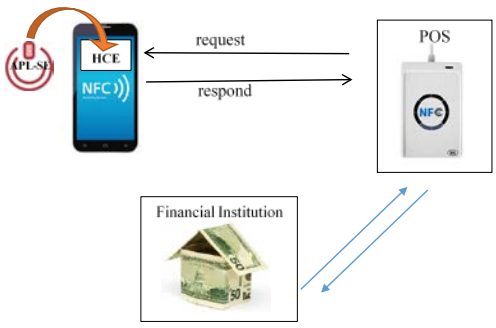

Fig. 1. APL-SE Architectural Design.

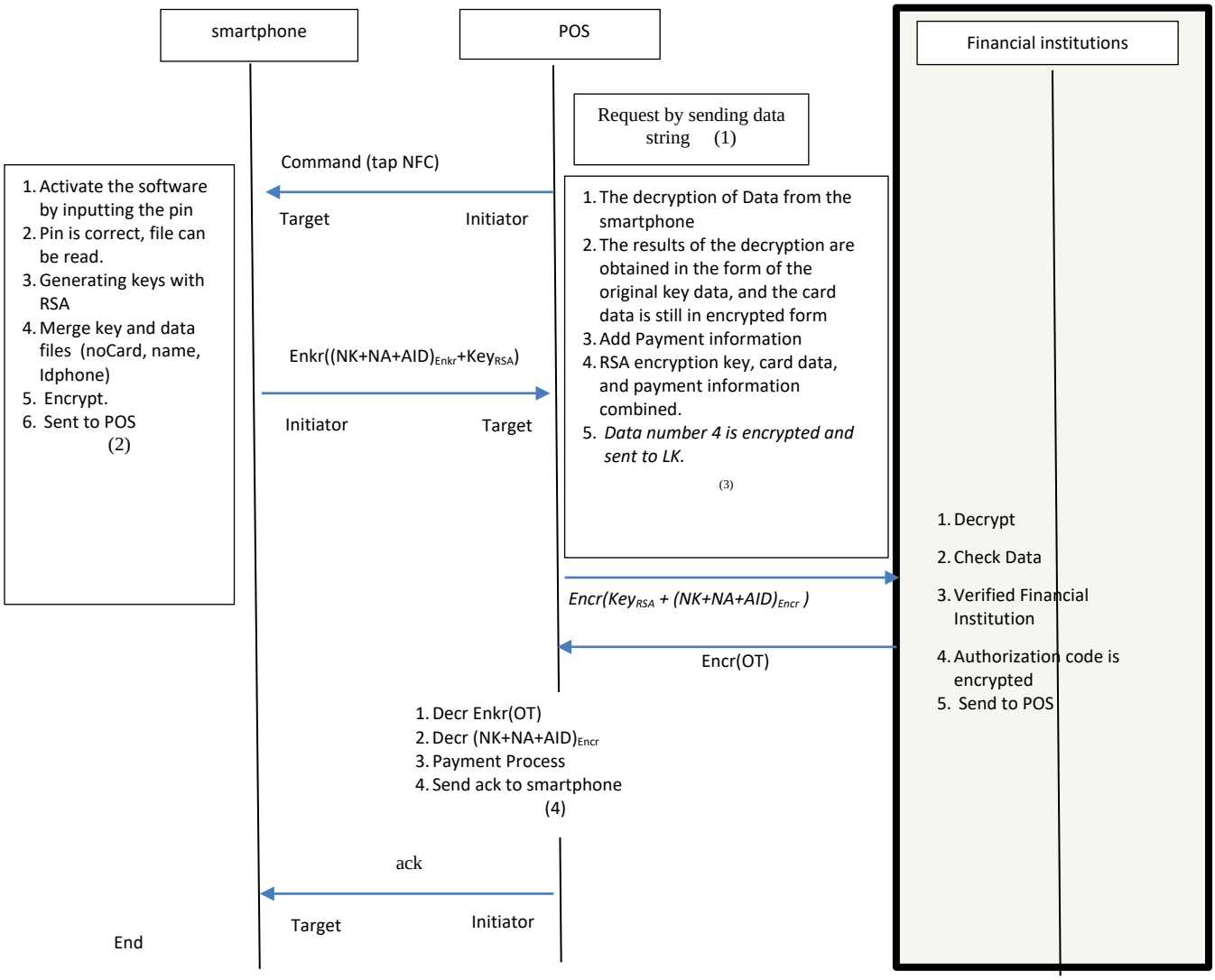

Fig. 2. NFC-HCE Transaction Model without Internet Connection between Smartphone and POS.

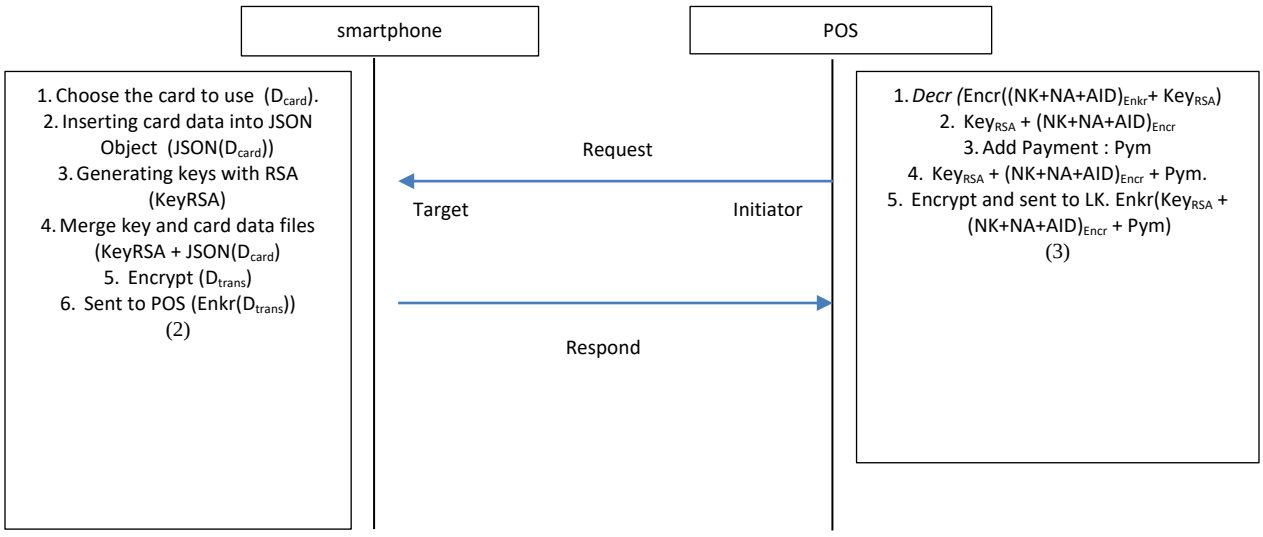

Fig. 3. Transaction Model Steps 2 and 3.

The data sent from the smartphone to the POS will be encrypted and encapsulated first. After the data reaches the POS, the data is parsed to get the original data. Encryption is done using the AES cryptographic algorithm. The algorithm chosen is simple, lightweight, and has modifiable parameters. It is because computing is done on smartphones that have limited memory capacity. At the same time, the parameter options can be modified to be used to add security by changing the parameter value every time there is a new transaction. Until this stage, the transaction model is complete. The model created is a model for normal transactions. Prevention of relay attacks is done by encrypting data when it is stored and transmitted between devices.

IV. Implementation and Evaluation

The proposed transaction model was tested on a smartphone with NFC facilities and the android operating system. The parameters tested were execution time and data randomness analysis using the monobit test.

The model was tested on a smartphone with differences in the android version and memory size. This test ensures that the model runs well and can improve security. Trials were also carried out on different smartphone conditions to determine the model's performance in different situations.

The data used for the trial is dummy data which describes the card user data that is widely used today. This data is inputted into APL-SE at the initialization stage, then used for transactions in this trial.

This encryption time is calculated from the beginning of the encryption process until the data is successfully encrypted. Based on the graphs in Fig. 4 and Fig. 5, we find that the time it takes is far below one second; the average time based on the test results is 1.074 milliseconds. This time is very short compared to the time it takes for the attacker to retrieve and translate the encrypted data, which takes more than one millisecond [25].

The entropy value shown in Fig. 6 and the P value shown in Fig. 7 also indicates that the data encryption results are declared random, based on Shannon Theory.

The communication made by the smartphone and the POS at the time of the transaction is the exchange of credential data needed to declare the transaction successful and correct. In this trial, the smartphone used by the user is a smartphone with the Android operating system, and the one used as a POS is an android smartphone.

Data exchange is carried out using the NFC-HCE ecosystem facilities on mobile devices. Fig. 8 shows the process of exchanging payment amount data from POS to the smartphone.

Data can be sent by POS if there is a request from a smartphone. For this reason, at this time, the smartphone is conditioned as the initiator and the POS as the target. In the beginning, the data sent from the POS to the smartphone is entered into the NFC POS card in the form of a shared preference. When the smartphone taps into the POS, the smartphone sends a request, namely the APDU command. POS receives this APDU command, then processes the APDU command. Payment data and select AID commands are combined and sent to the smartphone. The smartphone will receive the data, then retrieve the payment data. The first request-response process between smartphone (initiator) and POS (target) is finished here.

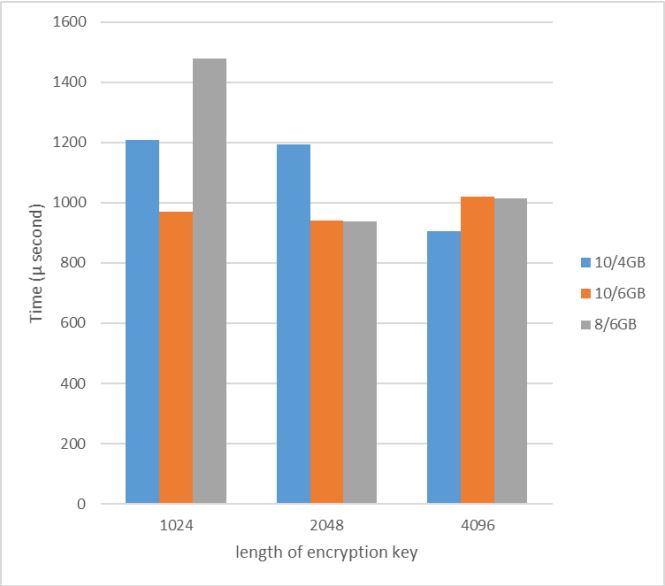

Fig. 4. Data Encryption Time on a Smartphone.

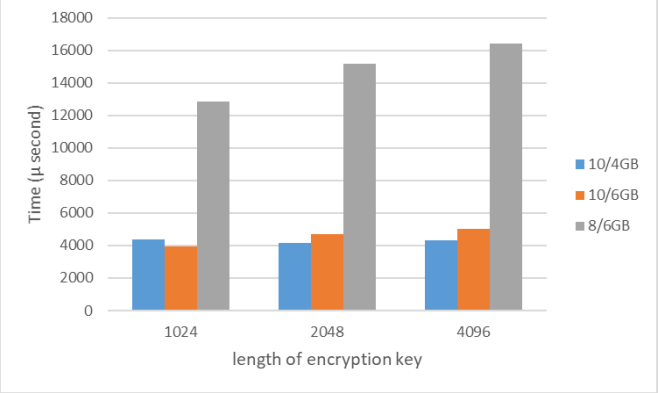

Fig. 5. Time to Send Customer Data to POS via NFC-HCE.

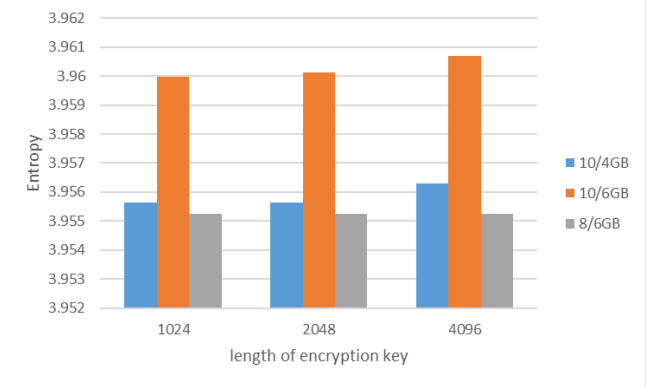

Fig. 6. Entropy Value of Data Encryption Results.

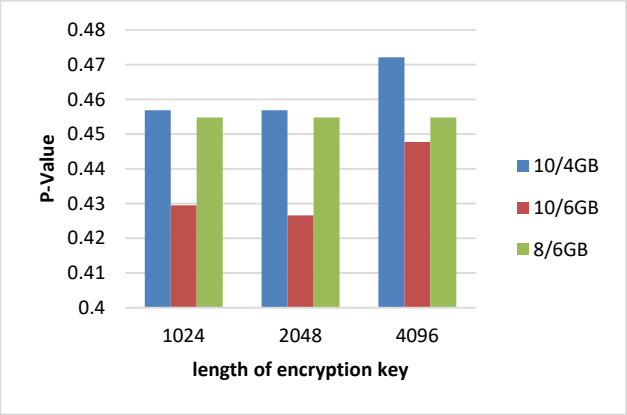

Fig. 7. P Value of Data Encryption Results.

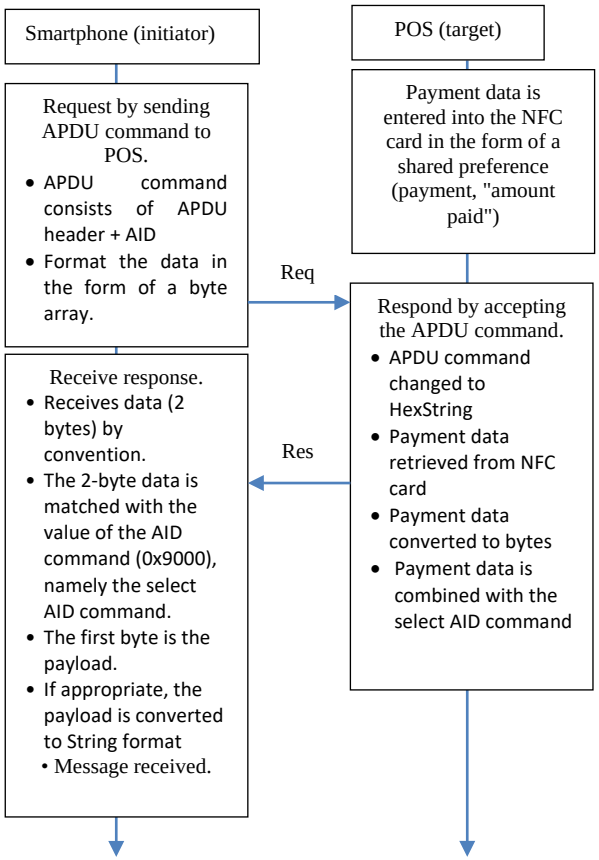

Fig. 8. Request-Respond when Sending Payment Data from POS to Smartphone.

The position of the initiator and target changes, POS as the initiator will make the request, and the smartphone as the target will respond. Fig. 9 shows this process. This process is similar to the process in Fig. 5. The data sent from the smartphone is the card data that will be used for payments. Card data is RSA encrypted in a JSON Object and sent in a shared preference format. When the card data reaches the POS, it is combined with the payment data, and the POS sends it to the server for verification.

Trials were also carried out by simulating smartphones with various positions during transactions. The model is tested using several smartphones to simulate a situation where there is another NFC within reach of the NFC reading area (POS or user) during a transaction. The test shows that the NFC that is read is the NFC that is closer to the NFC reader (reader/initiator). Because the physical situation that must be done is a situation where communication occurs with an NFC tap, then the two NFCs that will communicate are at a very close distance and do not allow other smartphones to occupy a closer position. This physical situation prevents NFC reading errors with unexpected devices.

NFC on smartphones, both POS and users, can be read at a distance of 0-5 cm. The NFC is not readable if their distance is above that distance. So, in that situation, the attack could be prevented because:

1) The data sent is in encrypted form.

2) The distance between smartphones must be close, and the NFC smartphone must be facing, meaning that the back of the smartphone must also be facing the back of the other.

3) The distance between smartphones is not more than 5 cm.

The second situation tested is when the user and the POS communicate, there is another NFC on the side of the user's NFC opposite the POS. When this happens, and the user's NFC is in reading mode (target), the user's NFC will be read by the POS because the NFC position is on the back side of the smartphone, which is facing the POS when communicating. Likewise, if the user's NFC is in reading mode (initiator), the user's NFC will read the NFC POS because the NFC position is on the back side of the smartphone facing the POS. This situation was tested by varying the distance between smartphones. 0-5 cm distance and NFC facing each other (meaning the back of the smartphone is facing each other) can communicate.

The third situation that is tested is if the POS and the user are going to make a transaction, and it turns out that another smartphone is in a position between the two devices. The first possibility is that the POS will read the NFC of another smartphone. Thus, communication between the POS and the user does not occur. If there were such a situation, the possible situation would be as follows:

1) If another smartphone has APL-SE, the transaction can occur, but the transaction is between the POS and another smartphone. In the transaction, authentication is carried out on the device's pin and id. If authentication is performed and another smartphone is identified, then the payment is made by the other smartphone and the accompanying identity.

2) If the other smartphone does not have APL-SE, there will be no transaction because the transaction will only occur if the two devices are connected as POS and user.

The second possibility is that the POS will read the user's smartphone because the NFC is the NFC of the POS and the user. So even though there are closer smartphones, because the NFC smartphones are not facing each other (there is NFC which is more in a straight line position), there is no NFC communication.

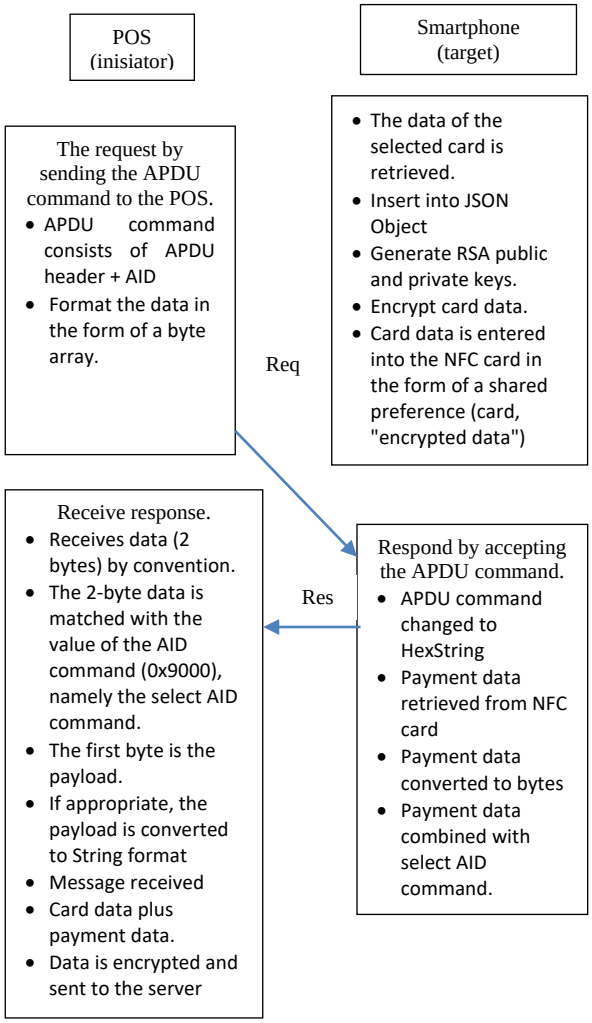

Fig. 9. Request-Response Sending Card Data from Smartphone to POS.

Mutual authentication between buyer and seller is as follows. The initialization model in this study ensures the client by registering client data, card data, and device data. The transaction model ensures that data is safe when sent and received back by the client device because the data is encrypted by each item and encrypted again as a single record before being sent. Smartphone users ensure POS for receiving payment data; POS ensure users receive payment card data. POS ensures financial institutions because the data is verified, and financial institutions ensure POS because the card data sent is correct and in accordance with smartphone owners.

Analysis for security against attackers is carried out as follows. The first attack is an attack that can take data at the time of a transaction, then use it at another time to ensure that the transaction is carried out by the right person (the real account owner). Several processes, namely prevent this attack:

1) Credential data stored on the smartphone is encrypted.

2) When the POS requests the customer's smartphone, the smartphone responds by sending encrypted personal data. The process of sending customer data to the POS can only be done when the customer enters a pin into the system.

3) Sending data from the POS to the Financial Institution for verification is done after the encrypted data from the smartphone is combined with the payment data from the POS, then encrypted.

4) Data originating from smartphones includes customer data and smartphone data. The two data are data pairs registered during the initialization process.

The second attack is an attack that can retrieve and analyze data and how the data can remain safe even though the attacker successfully retrieves the data. Several processes namely prevented the attack:

1) Customer data stored on the smartphone is in an encrypted state. And the results of the analysis of the encrypted data state that the data is random.

2) The encryption process and data transmission process takes place very quickly, far below the time required by the attacker to retrieve and analyze data.

3) Every time a transaction is made, a transaction key is generated, which will be different for other transactions.

The overall process created for this transaction model ensures that transactions are carried out safely and can prevent attacks, especially attacks by retrieving data that is being transmitted and attacks on transactions that use data that is already owned by the attacker.

Authentication in this research is kept simple and doesn't take many steps, but it can ensure that the registered account is correct. So, the account stored on the smartphone is an authenticated account, including the authentication of the smartphone device. Meanwhile, on the level of security, this study uses several levels of security. The first level with an encryption key, the second level encrypts every field of data, the third level encrypts all account data, and the fourth level converts the format to Base64 format.

The condition that requires NFC communication at a short distance and having to face each other on the back of the smartphone is one of the advantages so that the position of an attacker using a smartphone will be difficult. Meanwhile, if there is an attacker who uses another device but can access the data sent in APDU format, then there is a possibility that a third party can retrieve the data. But the format of the data sent does not allow the data to be interpreted in a fast time.

The model made in this study is quite reliable because the use of NFC will continue to grow in the future. The convenience of NFC with just a tap is an advantage, and the tendency of people to do and get more practical things from time to time is increasing.

The implementation of the initialization and transaction model is simple. The model is simply applied to the payment system at the POS, and financial institutions verify their customer account data, and smartphone owners download payment applications. The condition for this model to be implemented is that there is an agreement between POS and financial institutions, and there are customers who use applications that implement this model.

V. Conclusion

The APL-SE transaction model was created to improve the security of payment transactions using NFC-enabled mobile in the NFC-HCE ecosystem. The NFC-HCE ecosystem will be increasingly used because of its practicality in not needing to use a SIM as a place to store secure elements. Thus, financial institutions do not need to rent space from mobile operators. The test results show that the processing time is short and the encrypted data is random, thus increasing security.

This study has not discussed and tested data stored on smartphones when not in use. Data stored on smartphones has many security variables, such as user negligence, and lost or damaged data.

Acknowledgment

The study was supported by "Indonesia Digital Technology University."

References

[1] F. Fainusa, R. Nurcahyo, and M. Dachyar, "Conceptual Framework for Digital Wallet User Satisfaction," ICETAS 2019 - 2019 6th IEEE Int. Conf. Eng. Technol. Appl. Sci., pp. 2019–2022, 2019, doi: 10.1109/ICETAS48360.2019.9117285.

[2] Y. U. Chandra, Ernawaty, and Suryanto, "Bank vs telecommunication E-Wallet : System analysis, purchase, and payment method of GO-mobile CIMB Niaga and T-Cash Telkomsel," Proc. 2017 Int. Conf. Inf. Manag. Technol. ICIMTech 2017, vol. 2018-Janua, no. May, pp. 165–170, 2018, doi: 10.1109/ICIMTech.2017.8273531.

[3] Abdullah Almuhammadi, "An Overview of Mobile Payment, Fintech, and Digital Wallet in Saudi Arabia," 2020 7th Int. Conf. Comput. Sustain. Glob. Dev., pp. 271–278, 2020, doi: 10.23919/INDIACom49435.2020.9083726.

[4] R. M. N. D. Ranasinghe, "RFID / NFC Device with Embedded Fingerprint Authentication System," pp. 21–24, 2017, doi: 978-1-5???-??97-7/1??$31.00.

[5] O. S. Okpara and G. Bekaroo, "Cam-Wallet: Fingerprint-based authentication in M-wallets using embedded cameras," Conf. Proc. - 2017 17th IEEE Int. Conf. Environ. Electr. Eng. 2017 1st IEEE Ind. Commer. Power Syst. Eur. EEEIC / I CPS Eur. 2017, pp. 1–5, 2017, doi: 10.1109/EEEIC.2017.7977654.

[6] J. Zhao and X. Y. Li, "SCsec: A Secure near Field Communication System via Screen Camera Communication," IEEE Trans. Mob. Comput., vol. 19, no. 8, pp. 1943–1955, 2020, doi: 10.1109/TMC.2019.2913412.

[7] P. Pourghomi, P. E. Abi-char, and G. Ghinea, "Towards a mobile payment market: A Comparative Analysis of Host Card Emulation and Secure Element," Int. J. Comput. Sci. Inf. Secur., vol. 13, no. 12, pp. 156–164, 2015.

[8] L. N. Harnaningrum, A. Ashari, and A. E. Putra, "SECURE INITIALIZATION MODEL IMPROVEMENT for NFC-HCE SECURITY in MOBILE PAYMENT SYSTEM," J. Theor. Appl. Inf. Technol., vol. 99, no. 24, pp. 6139–6151, 2021.

[9] M. Badra and R. B. Badra, "A Lightweight Security Protocol for NFC-based Mobile Payments," Procedia Comput. Sci., vol. 83, no. Ant, pp. 705–711, 2016, doi: 10.1016/j.procs.2016.04.156.

[10] S. Nashwan, "Secure Authentication Protocol for Mobile Payment," Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 8, pp. 256–263, 2017, doi: 10.26599/tst.2018.9010031.

[11] M. A. Crossman and H. Liu, "Two-factor authentication through near field communication," 2016 IEEE Symp. Technol. Homel. Secur. HST 2016, 2016, doi: 10.1109/THS.2016.7568941.

[12] A. Munch-Ellingsen, R. Karlsen, A. Andersen, and S. Akselsen, "Two-factor authentication for android host card emulated contactless cards," 2015 1st Conf. Mob. Secur. Serv. MOBISECSERV 2015, 2015, doi: 10.1109/MOBISECSERV.2015.7072874.

[13] M. H. Özcanhan, G. Dalkiliç, and S. Utku, "Cryptographically supported NFC tags in medication for better inpatient safety patient facing systems," J. Med. Syst., vol. 38, no. 8, 2014, doi: 10.1007/s10916-014-0061-x.

[14] F. Dang et al., "Large-scale invisible attack on AFC systems with NFC-equipped smartphones," Proc. - IEEE INFOCOM, 2017, doi: 10.1109/INFOCOM.2017.8057219.

[15] M. Sujithra, G. Padmavathi, and S. Narayanan, "Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud," Procedia Comput. Sci., vol. 47, no. C, pp. 480–485, 2015, doi: 10.1016/j.procs.2015.03.232.

[16] M. Al-fayoumi and S. Nashwan, "Performance Analysis of SAP-NFC Protocol," Int. J. Commun. Networks Inf. Secur., vol. 10 No 1, no. April, p. 125, 2018.

[17] M. Alattar and M. Achemlal, "Host-based card emulation: Development, security, and ecosystem impact analysis," Proc. - 16th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2014, 11th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2014 6th Int. Symp. Cybersp. Saf. Secur., pp. 506–509, 2014, doi: 10.1109/HPCC.2014.85.

[18] A. Asaduzzaman, S. Mazumder, and S. Salinas, "A Security-Aware Near Field Communication Architecture," 2017 Int. Conf. Networking, Syst. Secur., no. January, 2017.

[19] N. Alzahrani, "Securing Pharmaceutical and High-Value Products Against Tag Reapplication Attacks Using NFC Tags," 2016 IEEE Int. Conf. Smart Comput., 2016, doi: 10.1109/SMARTCOMP.2016.7501715.

[20] O. Wenxing, W. Lei, Z. Yu, and Y. Changhong, "Research on Anti-eavesdropping Communication Mechanism for NFC," Proc. - 2015 7th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2015, pp. 839–841, 2015, doi: 10.1109/ICMTMA.2015.206.

[21] K. Fan, P. Song, and Y. Yang, "ULMAP : Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G," Mob. Inf. Syst., vol. 2017, no. April, 2017.

[22] N. El Madhoun, E. Bertin, and G. Pujolle, "For Small Merchants: A Secure Smartphone-Based Architecture to Process and Accept NFC Payments," Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, pp. 403–411, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00067.

[23] F. Dang et al., "Pricing Data Tampering in Automated Fare Collection with NFC-Equipped Smartphones," IEEE Trans. Mob. Comput., vol. 18, no. 5, pp. 1159–1173, 2019, doi: 10.1109/TMC.2018.2853114.

[24] A. Al-Haj and M. A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," 2018 4th Int. Conf. Inf. Manag. ICIM 2018, pp. 184–187, 2018, doi: 10.1109/INFOMAN.2018.8392832.

[25] N. El Madhoun, E. Bertin, and G. Pujolle, "An overview of the EMV protocol and its security vulnerabilities," 2018 4th Int. Conf. Mob. Secur. Serv. MOBISECSERV 2018, vol. 2018-Febru, no. February, pp. 1–5, 2018, doi: 10.1109/MOBISECSERV.2018.8311444.

[26] D. Mahansaria and U. K. Roy, "Secure authentication for ATM transactions using NFC technology," Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2019-Octob, pp. 1–5, 2019, doi: 10.1109/CCST.2019.8888427.