International Journal of Computer Applications Technology and Research
Volume 9–Issue 04, 133-138, 2020, ISSN:-2319–8656

The Challenges of Contactless Payment Models using Near Field Communication Enabled Devices

[1]Charles O. Okunbor [2]Yinka A. Adekunle [3]Adewale O. Adebayo

[4]Alao, O.D. [5]Eze, M.O.

[12345]Babcock University,
Department of Computer Science, School of Computing and Engineering Sciences
Ilishan-Remo, Ogun State,
Nigeria.

Abstract – The goal of financial institutions is to improve customers experience by making transactions safer, faster, easier, and more convenient. The use of electronics and computing has been a reliable and fast way of achieving these goals. One of such improvement is contactless payment. Contactless payments is the use of mobile phones, electronic cards, and other devices with Near Field Communication(NFC) technology to conduct transactions that do not require a physical connection between the Point of Sales (POS) terminal and the device of the consumer. NFC is the wireless technology that is used to transfer card payment data from the device to the payment terminal via radio waves. Electronic cards has been the most popular means of payment around the world but financial institution want these cards to be emulated by NFC enabled mobile devices which is perceived to be more fashionable, convenient and more secure due to their computing capabilities. Despite the auspicious features of contactless payment using NFC enabled device, its adoption has been slow due to some challenges associated with their models. Host Card Emulation(HCE) and Secure Element(SE) models for contactless payment on NFC enabled devices were reviewed in this paper and its challenges were highlighted.

Keywords: Contactless payment, Host card emulation, Near field communication, Secure element.

1.0 Introduction

Contactless payment is the process of making secure payments using a short-range wireless technology between a contactless card or payment enabled device and a contactless enabled checkout terminal [1]. Payment information is sent or transmitted for authorization when a contactless card or an enabled contactless device is tapped or placed close to a contactless point of sale(POS) terminal. Transactions involving contactless payments are about twice as fast as transactions involving cash, debit, or credit cards. This technology give retailers a way to encourage more frequent visits by customers who prefer this payment method, as well as to potentially speed up transactions and reduce operational costs. In general, some transactions using contactless payment, especially those that involve little amount require no PIN verification or signature and hence makes it beneficial for users that value speed [2], [3]. Security has been a concern for contactless payments and because of that, financial institutions and countries have policies placing limits on this form of payment to reduce risky transactions [4], [3]. Due to this reason, it has been challenging for people to adopt this technology and its growth has been slow. With the recent trends and advancement in computing, the world is moving towards a cashless economy and contactless payment will be a big contributor to achieving this [4]. According to a research carried out by [1], it is predicted that by 2025, 65% of all transactions will be by smartphones and 50.2% of the transactions will be contactless. Contactless payments are used on a range of devices including pre-paid, debit and credit cards; wearable devices, such as watches and wristbands; and mobile devices, such as smartphones and tablets [5]. Contactless devices used for contactless transaction uses a short-range radio frequency identification chip (RFID) known as Near Field Communication (NFC) technology. This technology is used to transfer payment information and other forms of data via radio waves when a user places a smart device or card within 4 inches or 10 centimeters of a reader or just waves it near a reader [6]. This process is also referred to as “tap and go” or “wave and pay” transactions.

2. REVIEW OF LITERATURE

2.1 Contactless Payment

Contactless payments refer to mobile phones, credit cards, and other devices that do not require a physical connection between the Point of Sales (POS) terminal and the payment device of the consumer. Transactions involving contactless payments are about twice as fast as transactions involving cash, debit, or credit cards [4]. This technology give retailers a way to encourage more frequent visits by customers who prefer this payment method, as well as to potentially speed up transactions because they do not require PIN verification or signature at the POS to authorize a transaction [2], [3]. Despite the convenience presented by this form of payment, users have questioned the security implications of using this technology [2].

2.2 Near Field Communication

NFC enables the mobile phone to act as a means of identification and a credit card for customers. NFC is a communication protocol that enables contactless transaction by establishing a short range wireless communication between two technical devices using frequency of 13.56 MHz, for instance between a mobile phone and a point of sales (POS) terminal [7]. NFC tags communication and data exchanges are based on standards like ISO 14443 A, MIFARE and FeliCa. It provides high comfort level and ease of use as there are no further configuration steps required to initiate a session to share data [8]. NFC is similar to WiFi, Bluetooth and other forms of wireless signals because they work on the principal of transmitting information using radio waves but NFC uses a different standard for wireless data communication which means that devices adhere to some specifications in order for them to properly communicate with each other [9].

NFC as a subset of RFID, was developed to provide a more secure, short-distance, and implicit paired communication capability. A good important aspect of NFC technology is its inherent security due to its very short communication range which makes it suitable for contactless payment. In NFC communication, bringing two devices very close to each other starts communication and separating the devices beyond a certain limit terminates the communication immediately [10].

Mobile payment is the driving force behind NFC technology over the past years, it is mostly used in contactless mobile payment. VISA estimates that mobile payment via NFC will replace the bank card in the coming years and most manufacturers of smartphones like Samsung, Apple have equipped their devices with this technology [11]. To enable mobile contactless payments, the NFC-enabled mobile device operates in card emulation mode and appears to an external reader to be a traditional contactless smart card [12].

2.3 Europay, Mastercard, and Visa (EMV)

EMV stands for “Europay, Mastercard and Visa”. EMV is an open-standard set of specifications for smart card payments and acceptance devices. Globally, financial institutions have migrated from magnetic stripe bank cards and infrastructure to EMV chip cards and infrastructure. [13] data shows that majority of POS terminals have been converted to EMV-enabled because of the shift of blames that occurs when fraudulent transactions take place. NFC mobile contactless payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol which is currently used by contactless EMV credit and debit cards [14].

3.0 CONTACTLESS PAYMENT MODELS

Two major architectures are used for mobile phones to store and communicate sensitive information such as card number, primary account number and other payment information. They are either by a hardware with Secure Element (SE) or a software with Host Card Emulation(HCE) [15], [16]. When card emulation is performed using an NFC mobile phone with a secure element, the interface to the payment reader (e.g. a point-of-sale or POS) is the same as for a traditional payment Credit/Debit card. This is similar with NFC mobile gadgets using the HCE, a POS or reader sees an application hosted in the mobile phones operating system as a standard EMV card (Andersson, 2016).

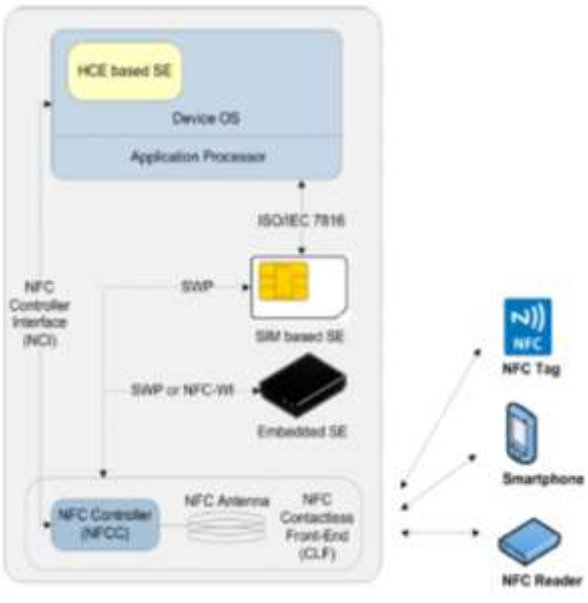

Figure 2.1. General architecture of an NFC smartphone. *Image source:* Coskun, Ozdenizci & Ok (2015).

3.1 Secure Element (SE) Model

When mobile devices with NFC are used to emulate smart cards, credentials like secret cryptographic keys used by payment applications are stored in a tamper resistant hardware module known as the Secure Element (SE) in accordance with the security requirements set forth by a known and trusted authorities [18]. The SE which is a tamper resistant hardware used to store sensitive credentials, has a direct connection with the NFC controller/antenna [16].

To make simple the idea of SE, [15] describes SE as a smart card in mobile devices. SE is known to have the highest level of security for applications residing on it. The level of security provided by SE is the same as the security level of classic smart cards [19]. One of the key advantages of SE is that it is a standalone component that creates a tough security against malicious sophisticated attacks. For SEs to offer a good level of interoperability and unparalleled rich portfolio of vital services, they are supported by mature ETSI, 3GPP, GlobalPlatform and Java Card standards.

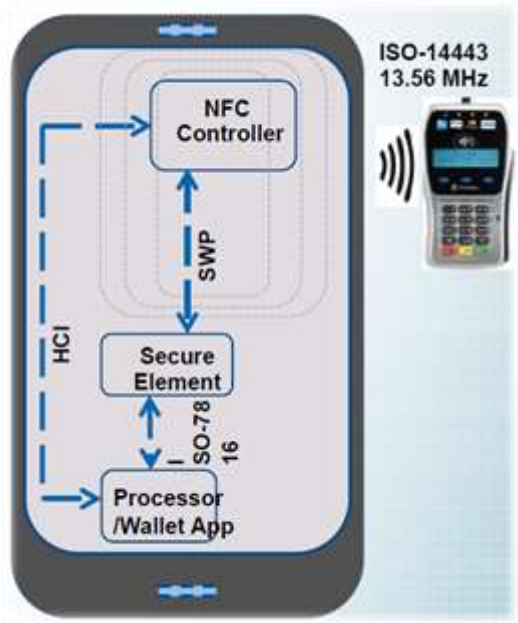

Figure 2.2. A mobile phone with a Secure Element. (*Image Source; Swaminathan, 2017*)

The introduction of SE led to the development of new business models and partnerships regarding to the ownership and management issues of SE. NFC ecosystem actors such as mobile network operators (MNOs), mobile handset manufacturers, financial institutions like banks and transport institutions have tried to impose an alternative to SE using a specific business model from which they could benefit most [20]. The SE was modeled in three forms that could benefit these actors. According to[18], the secure element can reside in an embedded secure smart card chip on the handset, on the Subscriber Identity Module (SIM) or Universal Integrated Circuit Card (UICC), or on a secure digital (SD) card that can be inserted into the mobile phone.

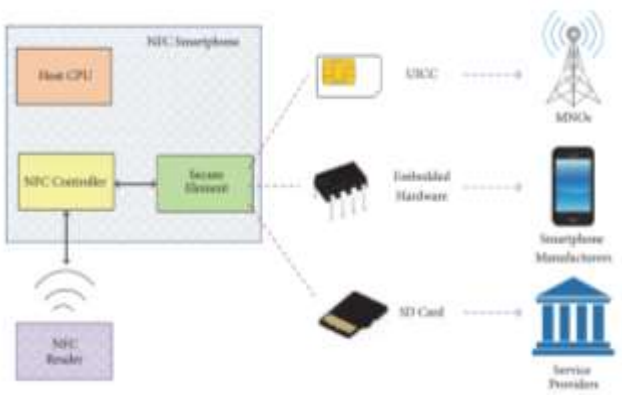

Figure 2.3. Diagram of different model of SE for card emulation. Image source*; Ozdenizci, Ok., and Coskun (2016).*

3.2 Host Card Emulation (HCE) Model

Host Card Emulation (HCE) was proposed as a short-cut for mobile NFC payments as it could allow financial institutions to launch mobile NFC products without the need of MNOs UICC/SIM card, mobile manufacturers embedded SE chip or other forms of Secure Element (SE) that will need a business agreement between NFC actors. HCE model allows the mobile device operating system (OS) to communicate directly over the NFC interface in card emulation mode. This would allow financial institutions like banks to offer mobile NFC services to customers over the top (OTP), bypassing the need to cooperate with mobile operators, phone manufacturers and other actors in the ecosystem, with the aim of reducing cost and complexity [19]. It simplifies the ecosystem by providing OTT technology for applications used for NFC contactless transactions at the expense of increasing payment transaction risk management.

3.2.1 Tokenization

Storing payment credentials and cryptographic keys in the mobile device OS instead of the SE is considered less secure as discussed in HCE model, which is why additional security measures like tokenization is needed for HCE (Pandy & Crowe, 2016). Wadii, Boutahar and Ghazi (2017) defined tokenization as a process by which the primary account number (PAN) is replaced by a substitution value referred to as a Token.

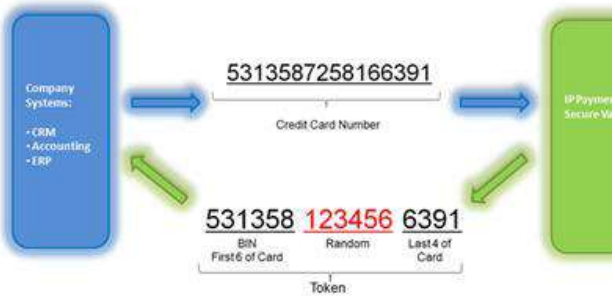

Figure 2.4. A token been generated in a banking transaction. Image Source; *Wadii, Boutahar and Ghazi (2017)*

4.0 IDENTIFIED CHALLENGES THE MODELS

In payment system, trust is a primary factor that cannot be overlooked because an accepted payment system must be perceived as being secure so that in the event of fraudulent transaction, a user is certain to be protected and refunded if need be (Smart Payment Association, 2015). With the introduction of NFC contactless payment, users and Issuers have questioned the safety of transactions and the storage of payment information. The following are the challenges faced by contactless payments models using NFC enabled devices.

4.1 Challenges of SE Model

SE is seen to satisfy the fundamental security paradigm, that a sensitive application must only be run in a secure computing platform, certified as tamper resistant [21]. Despite SE certified as a temper resistant, it has some challenges that has contributed to the slow growth of this technology as highlighted below;

a) As pointed out earlier, SE was model into forms that could benefit various actors within the ecosystem. These alternative models brought disagreement among actors because each party wanted to hold a favourable business positions were they could benefit the most [19]. Unfortunately, a satisfactory agreement could not be reached by these actors. These disagreements was one of the shortfalls of SE which contributed to limiting the development of NFC contactless payment systems and other services in card emulation mode [20].

b) UICC-based SE model created an advantage and opportunity for MNOs because they are issued and managed by them. A major challenge faced by financial institution for this model is that before a UICC/SIM can be used to host any financial application, a business agreement must be made with MNO before access and host space can be granted [19]. For customers, only UICC of MNO's who have an agreement with their financial institution can be used. This means that users will need to go through the inconvenience of swapping UICC's or exiting a MNO in other to have access to contactless payment using the UICC of another MNO who has an agreement with their financial institution.

c) SE has a problem of limited storage. It cannot accommodate so many applications for different Issuers and payment networks due to inadequate storage capacity on MNO's UICC's and smart phone embedded chips used for SE.

d) Beyond the complexity and cost of establishing a relationship with a third party, only the SE provider determines who and what can access the SE. Some mobile carriers have a vested interest in limiting access to the secure element because they offer their own mobile wallets. For example, according to [22], Google wanted to install its application for contactless payment on UICC's. Major mobile phone operators such as Verizon, AT&T and T-Moble declined their cooperation, instead promoted their own application which was initially called Isis Wallet but was later renamed Softcard.

4.2 Challenges of HCE Model

In other to find a more independent solution for SE led to the discovery of cloud based SE known as Host Card Emulation. HCE model have helped to remove the dependence of SEs owned and managed by third parties by allowing the mobile devices operating system (OS) to communicate directly over the NFC interface in card emulation mode. However, the relaxed security of HCE is still an important obstacle in its way [23]. Below are some of the challenges faced by HCE.

a) Isolation and sandboxing provided by mobile OS is regularly broken, and consumers often root or jail break their device which unknowingly makes them risk sensitive data leakage. This makes access to users sensitive information for transaction such as payment credentials held by the HCE application hosted on the device's OS exposed and can be extracted and used by criminals for fraudulent transactions.

b) The HCE runs on a non-secure platform, meaning that other applications resident in the mobile device, malicious or not, may compromise the integrity of payment applications. Malwares, spywares, viruses and other malicious programs can find themselves into users mobile OS and end up compromising the integrity of HCE applications. They can cause a Denial of Service (DoS) by maliciously modifying routing table from Android OS domain table or even saturating it by declaring a lot of AIDs (Application Identifiers). These malicious programs can steal,

expose and transmit sensitive information from applications without the users knowledge.

c) When a device having the HCE application is lost or stolen and falls into the hands of criminally minded persons, they could connect to all the information stored within the application and use them to make fraudulent payments.

d) HCE depends on a network connectivity to retrieve payment credentials from the cloud. This service becomes inaccessible if devices cannot connect to their service providers due to network failures.

e) Tokenization was introduced to minimize the risk of financial institutions and their customers using HCE by substituting payment credentials with temporary tokenized pseudo data. Tokenization comes with its challenges:

   i. It increases the cost of processing transactions because a fee needs to be paid to tokenize and detokenize the card information of a customer for every transaction.

   ii. The process of tokenization and detokenization before transactions can be processed and approved reduces transaction speed.

   iii. Good tokens do not give room for data to be reconstituted, hence data analysis cannot performed on tokenized transactions on HCE.

5.0 CONCLUSION

This paper has been able to highlight the challenges facing contactless payment using NFC enabled devices. Most of the challenges faced with this form of payment are security issues relating to secure storage of payment credentials and lack of cooperation between actors within the contactless payment ecosystem. In other to mitigate the identified challenges faced with contactless payment models, cooperation is needed between financial institutions, MNO's, device manufacturers and other actors within the ecosystem. Cooperation is needed because aside the renting of SE, other services such as network connectivity, NFC enabled devices, supporting operating system and so many others provided by different actors is also needed to make the payment system successful. HCE should be seen as a viable alternative to SE and minimum security requirements should be set for the implementation of HCE through standardization.

REFERENCES

[1] VISA (2018). Contactless Payments. Retrieved on 24th October, 2018 from; https://usa.visa.com/pay-with-visa/contactless-payments/contactless-payments.html

[2] Fuller, A. (2017). Contactless Payments – The pros and cons of tap and go. Retrieved on 24th October, 2018 from; https://www.finder.com/contactless-payment

[3] Heropay, (2018). Contactless Card Payment. Retrieved from: https://www.heropay.com/glossary/contactless-card-payment/

[4] Banka, L., & Ambre S. (2016). Contactless Payments. Retrieved from: https://www.arx.cfa/up/post/2461/Contactless%20payments.pdf

[5] Phair, N. (2016). The Truth about Contactless Payments. Center for Internet Security. Retrieved from; http://www.canberra.edu.au/cis/storage/Contactless%20payments.pdf

[6] Quibria, N. (2008). The Contactless Wave: A Case Study in Transit Payments. Federal Reserve Bank of Boston: Emerging Payments Industry Briefing.

[7] Chae, J. S. U., & Hedman, J. (2015). Business Models for NFC based mobile payments. Journal of Business Models, 3(1).

[8] Trivedi, D. (2015). Near field communication. Masters degree thesis, Nirma University, Ahmedabad-382481.

[9] Triggs, R., (2017). NFC Tags - How Do They Work. Retrieved from; https://www.android authority.com/nfc-tags-explained-271872/

[10] Coskun V., Ozdenizci B., & Ok K. (2015). The Survey on Near Field Communication. Sensors 2015. Basel, Switzerland. 1424-8220

[11] Wadii, H.E., Boutahar, J., & Ghazi, E.S. (2017). NFC Technology for Contactless Payment Echosystems. International Journal of Advanced Computer Science and Applications,

[12] Noh, S. K., Lee, S. R., & Choi, D. (2014). Proposed m-payment system using near-field communication and based on WSN-enabled location-based services for m-commerce. *International Journal of Distributed Sensor Networks*, *10*(4), 865172.

[13] NCR (2015). The Road to Contactless Payments, EMV, Apple Play and Tokenization Patents Pending 15FIN3279A-0615.

[14] Smart Card Alliance (2011). The Mobile Payments and NFC Landscape: A U.S. Perspective. A Smart Card Alliance Payments Council White Paper. Publication Number: PC-11002.

[15] Lepojevic, B. (2012). Management of secure element in systems based on NFC technology. (M. Sc. thesis), Faculty of organizational sciences, University of Belgrade, Serbia.

[16] Pannifer, S., Clark, D., & Birch, D. (2014). HCE and SIM Secure Element: It's not black and white. A Discussion Paper from Consult Hyperion.

[17] Andersson, D. (2016). A survey on contactless payment methods for smartphones. Faculty of Computing, Blekinge Institute of Technology, Sweden. Thesis no: BCS-2016-05

[18] Smart Card Alliance (2014). Host Card Emulation. A Smart Card Alliance Mobile & NFC Council White Paper. Retrieved from; http://www.smartcardalliance.org.

[19] Lepojevic, B., Pavlovic, B., & Radulovic, A. (2014). Implementing NFC service security – SE VS TEE VS HCE. Ministry of Defence Republic of Serbia. Retrieved from; https://www.researchgate.net/publication/263506976_Implementing_NFC_service_security_-_SE_VS_TEE_VS_HCE

[20] Ozdenizci, B., Ok, K., & Coskun, V. (2016). A Tokenization-Based Communication Architecture for HCE-Enabled NFC Services. Hindawi Publishing Corporation Mobile Information Systems. 2016 (5046284).

[21] Smart Payment Association (2015). Is host card emulation (hce) the big enabler for mobile contactless payments? *An SPA Position paper*.

[22] Grustniy, L. (2019). Secure Element — securing contactless payments in smartphones. Kaspersky daily. Retrieved from; https://www.kaspersky.co.uk/blog/secureelement/13687/

[23] Alattar, M., & Achemlal, M. (2014). Host-based card emulation: development, security and ecosystem impact analysis. Proceedings of the IEEE International Conference on High Performance Computing and Communications