Journal of Information Systems and Telecommunication
Vol.11, No.3, July-September 2023, 232-240

http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

A survey on NFC Payment: Applications, Research Challenges, and Future Directions

Mehdi Sattarivand[1], Shahram Babaie[2*], Amir Masoud Rahmani[1]

[1].Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
[2].Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Received: 19 Apr 2021/ Revised: 04 Dec 2022/ Accepted: 10 Jan 2023

Abstract

Near Field Communication (NFC), as a short-range wireless connectivity technology, makes it easier for electronic devices to stay in touch. This technology, due to its advantages such as secure access, compatibility, and ease of use, can be utilized in multiple applications in various domains such as banking, file transferring reservations, booking tickets, redeeming, entry/exit passes, and payment. In this survey paper, various aspects of this technology, including operating modes, their protocol stacks, and standard message format are investigated. Moreover, future direction of NFC in terms of design, improvement, and user-friendliness is presented for further research. In addition, due to the disadvantages of banknote-based payment methods such as the high temptation to steal and the need for a safe, mobile payments, which include mobile wallets and mobile money transfers, are explored as a new alternative to these methods. In addition, the traditional payment methods and their limitations are surveyed along with NFC payment as a prominent application of this technology. Furthermore, security threats of NFC payment along with future research directions for NFC payment and its challenges, including protocols and standards, and NFC payment security requirements are addressed in this paper. It is hoped that effective policies for NFC payment development will be provided by addressing the important challenges and formulating appropriate standards.

Keywords: Near Field Communication (NFC); NFC Payment; Card Emulation; NFC Security.

1- Introduction

In recent years, the electronic industry is improving significantly in various aspects and profoundly affected people's lives by dispelling some traditional problems. In NFC technology, two NFC-enabled devices can create a point-to-point connection via a wireless channel. The NFC technology has been firstly introduced by two leading manufacturers in the electronics industry, Sony and Philips in 2002. Some advantages of this technology such as flexibility, versatility, and ease to use caused it to extend its application in many fields such as file transferring, health monitoring systems, indoor navigation, ticketing, and financial [1].

Although many electronic devices can be equipped with NFC technology, this technology is mostly installed on smartphones. Also, other mobile network technologies such as 3G, 4G, and 5G have been added to mobile smartphones to provide broadband high-speed internet connection for users [2]. Nowadays, NFC is the most leading technology that can be embedded in smartphones and tablets. The theoretical maximum working distance of this technology is 20 centimeters, moreover, in practice, the range of reliable communication is much smaller, usually about 5 centimeters. In general, a combination of the contactless identification and interconnection technologies can compose an NFC system, which requires two NFC-compatible devices close to each other for a proper response [3].

In general, mobile payment due to its specific features such as safe, secure, convenient, and fast is an increasingly attractive method to pay. It should be noted that smartphone technology plays an essential role in the growth of these transactions [4]. It is reported that over 3.4 billion smartphones will be equipped with Android Pay, Apple Pay, and Samsung Pay by the end of 2017; likewise,

✉ **Shahram Babaie**
Sh.babaie@iaut.ac.ir

this may reach 5.3 billion by 2021. Moreover, Apple Pay transactions grew 450 percent in the first quarter of 2017 in comparison to the same quarter of 2016. In stores, mobile payments can carry out through NFC technology, which stands for Near Field Communication. Also, NFC can also be combined with RFID technology and read its tags also applied as a file transfer system. Therefore, NFC-enabled payments due to the three key reasons, i.e., secure, fast, and convenient can convince vendors to provide their products with this technology. Also, digital payment instead of paying for products with cash, checks, or physical credit cards causes people to carry less cash [5].

In general, safety and security are vital requirements in financial transactions. NFC technology due to the short support range can be considered as a reliable method for these applications [6]. The NFC connection is initiated when two NFC-enabled devices are close to each other almost 5 centimeters. Therefore, eavesdropping on the transaction's data is hard for a third party. Supporting a shorter range leads to improved security as a key NFC advantage over other communication systems. In general, the NFC technology is a short-range half-duplex communication protocol, working at 13.56 MHz frequency band, which is designed for particular applications [7]. NFC can enable a variety of innovative services. As a result, it is right to say that NFC provides smooth content delivery, brings simplicity to transactions, and enables secure information sharing. Moreover, NFC can build various opportunities for vendors, banks, mobile operators, and transport operators [8].

There are two operating modes in NFC, active and passive modes [9]. In the active mode, both devices generate the RF field to establish the connection and transfer data. Whereas, in the passive mode, one active device generates the RF field to establish the connection and transfer the data. Table 1 shows the NFC communication modes; also, Table 2 compares the WPAN technologies.

Table 1. Communication Modes in NFC [10].

Device A	Device B	RF Field Generation	RF Mode
Active	Active	Generated by Both Devices	Active Mode
Active	Passive	Generated by Device A Only	Passive Mode
Passive	Active	Generated by Device B Only	Passive Mode

NFC supports three data transfer rates i.e. 106, 212, and 424 KB/s [11], also, a variety of data coding techniques such as Manchester, modified miller, and NRZ-L are applied in this technology [12]. NFC also supports both 10% ASK and 100% ASK modulation. In fact, data rate, operation mode, RF signaling, and standards are major parameters to determine the modulation type. Figure 1 shows modulation and coding of an NFC connection.

Table 2. Comparison of WPAN Technologies [11].

Parameter	Bluetooth	ZigBee	NFC
Range	10-100 m	10-100 m	4-10 cm
Data Rate	0.8-2.1 Mbps	0.02-0.2 Mbps	0.02-0.4 Mbps
Cost	Low	Low	Low
Power Consumption	High	Medium	Low
Spectrum	2.4 GHz	2.4 GHz	13.54 MHz
Security	Low	Low	High
Network Topology	Piconets, Scatternets	Star, Tree, Mesh	One to One
Devices per Network	8	2-65,000	2
Usability	Moderate, Data Centric	Easy, Data Centric	Easy, Human centric
Personalization	Medium	Low	High
Flexibility	High	High	High
Setup Time	Approx. 6 s	Approx. 0.5 s	Less Than 0.1 s

According to [13], secure elements play a principal role when a secure transaction is needed in an NFC connection for either transmitting and storing data in NFC-enabled devices. Secure elements can create a secure environment for the sensitive data that is transferred and stored in an NFC connection such as users' credit card information and access key information when using card emulator mode. Also, HCE as the latest SE of NFC is another security approach to stores and manages the user's private data in the smartphone.

In this paper, the main goal is to survey the current NFC payment methods including their related architecture, standards, and challenges. Moreover, the existing solutions to overcome these challenges are presented, and future research directions of NFC payment are investigated in terms of design, improvement, and user-friendliness to dispel the challenges. In addition, along with presenting the drawbacks of banknote-based payment methods such as high temptation to steal, mobile payments and NFC payment, which include mobile wallets and mobile money transfers, are explored as a new effective alternative. Furthermore, security challenges of NFC payment are investigated; also various approaches that are applied for securing the NFC payment are introduced and compared in terms of security requirements. Finally, it has been endeavored that new future directions are addressed to improve protocols and standards for and NFC payment security requirements

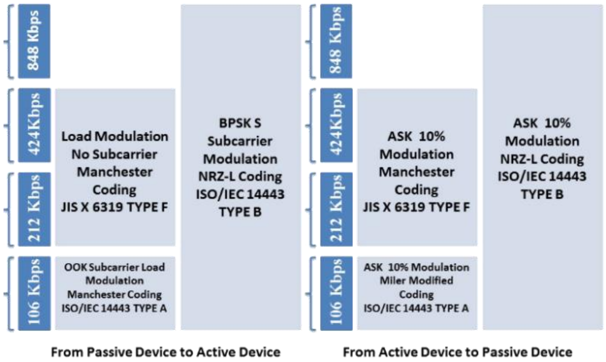
848 Kbps
424Kbps
212 Kbps
106 Kbps
Load Modulation No Subcarrier Manchester Coding JIS X 6319 TYPE F
OOK Subcarrier Load Modulation Manchester Coding ISO/IEC 14443 TYPE A
BPSK S Subcarrier Modulation NRZ-L Coding ISO/IEC 14443 TYPE B
848 Kbps
424Kbps
212 Kbps
106 Kbps
ASK 10% Modulation Manchester Coding JIS X 6319 TYPE F
ASK 10% Modulation Miler Modified Coding ISO/IEC 14443 TYPE A
ASK 10% Modulation NRZ-L Coding ISO/IEC 14443 TYPE B
From Passive Device to Active Device
From Active Device to Passive Device

Fig. 1. Modulation and Coding of an NFC Connection [11].

The rest of this paper is organized as follows: NFC technology and its operating modes are introduced in section 2. Current payment methods and their limitations are discussed in section 3. Afterward, in section 4 the concept of NFC payment is represented. Section 5 presents the NFC payment security and security threats. The future direction of NFC payment is subject to be investigated in section 6. Finally, section 7 concludes the paper.

2- NFC Architecture, Standards, and Protocols

In this section NFC architecture, standards, and protocol are introduced in detail. In some studies, some modules have been proposed to improve the performance of NFC technology. Likewise, secure elements play an essential role in NFC applications, especially in payment cases. A mobile device equipped with NFC technology depending on its application may also have more than one SE. There are three operating modes in NFC, which are investigated in the following subsections.

2-1- Operating Modes

NFC technology similar to other communication systems needs a set of standards and protocols to control how the network elements operate, communicate, and guarantee security. Therefore, increasing the number and improving these standards result in ease of access and guaranteed security; meanwhile, it may make the NFC slightly more complicated than its status. The most significant standardization association for NFC technology is NFC Forum, which develops and improves all of NFC essentials, as well as NFC standards. NFC Forum is a non-profit association, which aims to turn NFC into a better network environment also extend it worldwide [14].

2-1-1- Reader/Writer Mode

Reader/writer mode is an operation mode of the NFC in which an active mobile NFC-enabled device initiates a wireless communication; it can also read and modify the stored data in the NFC tag accordingly. [15]. In this mode, the NFC-enabled device can read and write the NFC Forum’s standard tags, which can be in four types. Consequently, the user can read, write the stored data on the NFC transponder, and carry out the proper action later. Following NFC Forum, messages of the NFC communication have a specific format, which is called NDEF. In general, several NDEF records are chained to each other to create an NDEF message, so that a more substantial payload can be transferred. The protocol stack of the reader/writer mode is also depicted in Fig. 2(a).

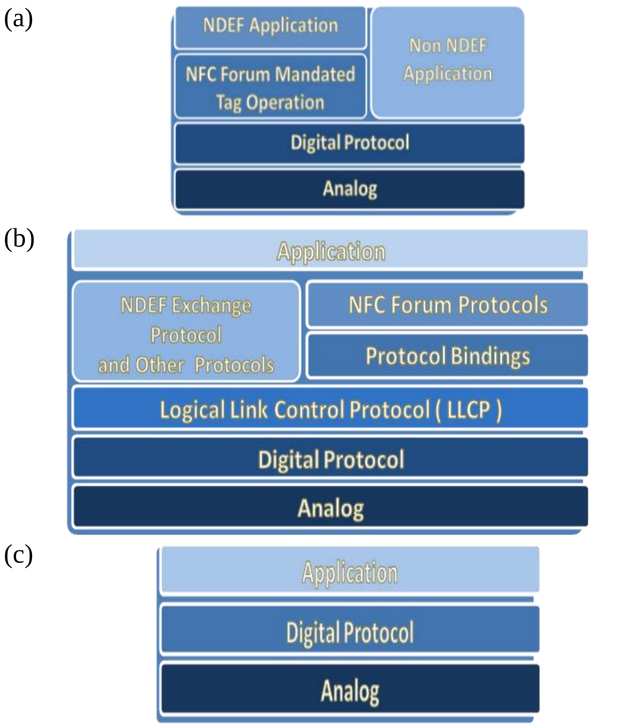

Fig. 2. Protocol Stack of the (a) Reader/Writer Mode, (b) Peer-to-Peer Mode, (c) Card Emulation Mode [17].

2-1-2- Peer-to-Peer Mode

In this mode, a bidirectional connection is made between two NFC-enabled devices, in which two devices can actively transmit any data such as business information, payment transaction information, and file sharing [16]. The RF communication interface in the peer-to-peer connection of NFC is standardized by ISO/IEC 18092 protocol, which is called NFCIP-1 that enables the “request and response” feature for both devices to make sharing data capability. In the mode, both of the NFC devices, i.e., initiator and target are active. Also, the RF uses 13.56 MHz, frequency band. The protocol stack of the peer-to-peer mode of NFC is illustrated in Fig. 2(b).

2-1-3- Card Emulation Mode

In card emulation mode, both NFC devices use the same analog and digital techniques based on the ISO/IEC 14443 type A, type B, and SONY FeliCa. In this operation mode, when a mobile user’s NFC device touches an NFC reader, its NFC device acts as a smart card also the NFC reader deals with the emulate smart card security element.

In this mode, the NFC reader is active, and the smartphone is passive. Applications of the card emulation mode are access control and ticketing. In general, some standards such as ISO/IEC 14443 type A, type B, and SONY FeliCa communication interfaces are applied in these applications. Figure 2(c) indicates the protocol stack of the card emulation mode. A summary of NFC operating modes including reader/writer mode, peer-to-peer mode, and card emulation mode is shown in Fig. 3.

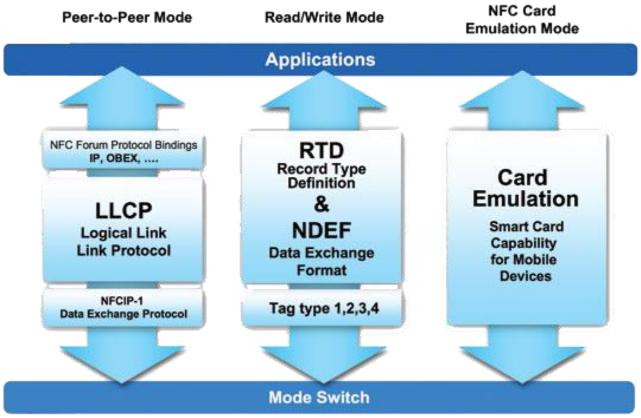

Fig. 3. Three Operation Modes of NFC [18].

2-2- Pros and Cons of NFC

In general, each system and technology has some advantages and disadvantages. Consequently, NFC as new technology has some pros and cons as follows.

2-2-1- Pros of NFC

- NFC uses electromagnetic waves instead of wired connections. Therefore, the wired connection is not necessary for users, so that the transactions, data transferring, media sharing are carried out faster and more reliable.
- The proximity of the two devices is necessary for NFC technology that causes eavesdropping is hard. As a result, this technology is almost secured.
- The NFC technology by reducing the time of sweeping the card, choosing a menu, and entering the password decreases the total time of a transaction; also, it can lead to a faster and more flexible transaction process when it applied in the transactions and card emulation.
- Lower energy consumption should be considered in the NFC design phase [19]. As a result, more energy power is saved in comparison to other payment technologies such as RFID in the overtime and considering the high number of users [20].
- The time needed for an NFC connection to be made less than 0.1 seconds. Therefore, the NFC is an appropriate choice, where there are many users, and they need to perform their payments tandem one after another, such as subway stations.
- NFC is a flexible technology, which can work under a variety of environmental conditions. Therefore, a user is not restricted to environmental conditions and the user can easily use this technology.
- NFC is versatile equipment where many tasks can be carried out. For example, a user can be checking out at a store, read information from a smart poster, and purchase and load a concert ticket through a single NFC-enabled device.

2-2-2- Cons of NFC

Besides the mentioned advantages, this technology has a few disadvantages as follows.

- Most NFC disadvantages are related to their costs and prices. So that increasing the costs in NFC applications is inevitable due to requiring both tags and readers. Generally, NFC device's price is approximately high; also, the maintenance and development of NFC devices are not cheap.
- Although NFC is almost secure due to it needs the devices to be close to each other, remains some challenges of NFC security.
- Another point to be mentioned as an NFC disadvantage is that this technology is not yet fully spread all around the world so that NFC technology is not applied in many countries. Likewise, for various reasons, this technology is not applicable in every country.

2-3- Future Research Directions on NFC

There are some future directions and open issues in NFC tags, NFC protocols, and NFC communication modes as follows. Although some of the proposed research topics are novel, recently some innovative efforts have been made on some matters, which makes these topics as future directions of NFC technology. The suggested future research directions for topics of this section including SE and HCE except for security parts of NFC is listed:

- Analysis of antenna design, antenna coupling, RF efficiency, and simulation of an NFC communication on other proper frequency bands and proposing alternative designs for antennas of NFC.
- Proposing an alternative or developed protocol for SNEP for peer-to-peer transactions.
- Developing a new modulation scheme and a coding technique considering the power management and security issues of this technology.
- Developing alternative NFC protocols for other possible applications and a revision of LLCP and NFCIP-1.
- Proposing a more user-friendly software for Android, IOS, and Windows smartphones with a professionally designed GUI to increase the willingness of users to use this technology.
- Exploring possible ways of setting dynamic NFC tags as alternative hardware for static NFC tags.

3- Current Payment Methods

There are various methods, which can be applied to payment applications as follows. The NFC payment is not considered in this section.

3-1- EMV® Card

EMV® Card is the abbreviation form of “Euro pay, MasterCard®, and Visa®”, which are three major companies that handle payments and transactions from little to large amounts of money. These companies have produced payment cards based on the chip technologies that are disclosing the account information is nearly impossible for anyone who might steal the card. To this end, the microprocessor chip inside the card generates a unique code for each transaction. As a result, due to the uniqueness of transaction codes, the gained codes will be useless when a criminal can get the code from a store.

3-2- Magnetic Stripe Card

A magnetic stripe card can store transaction data by changing the magnetism of a tiny iron-based magnetic layer of the card, which is called magstripe or sweep card. The magstripe cards work by sweeping the magnetic reading head to POS and POP devices. This type of card is most suitable for identity cards, credit cards, and transportation tickets [21]. Limitations of these payment methods are:

- **Bulky Wallets**

It is inevitable to have more than one payment card if someone has multiple bank accounts. As a result, managing these cards and their information will not be accessible. Also, keeping multiple cards cause a thicker wallet.

- **Loss of the Card**

Card-based payment methods have a high risk of being stolen and loss of cards. Furthermore, the extra time and more effort are required for the cardholder to recover the card when its card is lost or stolen.

- **Fake Identity**

When a criminal can steal a credit/debit card (EMV® card or magnetic stripe card), fake identity issues can occur. Therefore, a criminal can claim that it is the cardholder and cause severe and irrecoverable problems for the real cardholder.

4- The Concept of NFC Payment

Generally, mobile payments, which include mobile wallets and mobile money transfers, are actual transactions that take place on mobile devices. Mobile payment technology allows that payment to carry out digitally instead of paying for stuff with cash, checks, or physical credit cards. This type of payment can be applied in both “peer to peer” context and for paying at a brick-and-mortar business. A mobile payment application is applied to pay in a peer-to-peer mobile payment; also, instead of cash or a card, a mobile application is applied to pay for particular commodity and services at the checkout counter in the mobile payment of a brick-and-mortar business. In this instance, a specific type of point-of-sale device is required to process the transactions.

In general, the success of a payment method depends on some factors. To this end, Staykova and Damsgaard [22] investigated the effective parameters of a payment method that are based on entry and expansion. They have built a framework to analyze the entry and expansion strategies of digital payment solutions. They have concluded that the importance of the timing of expansion and importance of the timing of entry are identical. The important factors affecting mobile payment in public transportation have been investigated in [23]. In this study, the role of mobile payment as a payment system has been investigated in the public transport of Oporto, Portugal and Beijing, China. Their research has indicated that users’ age is an essential factor in determining the usage of mobile payment systems so that younger people have tended to use mobile and digital payment systems more than older citizens. According to their statistical results, innovation in representing the service is an important factor that affects users to choose a digital mobile payment system [24].

User acceptance is a major success factor for each new technology. In [25], the user acceptance influence of success a new technology has been studied by Ramos-de-

Luna and Montoro-Rı´os. To meet this objective, they have prepared a questionnaire that 191 audiences have filled it. They have also used PLS v3.0 software to analyze the results statistically. Their results show that attitude, subjective norms, and innovation are vital parameters that can determinant the future intention of using mobile payments.

Likewise, Cocosila and Trabelsi studied the user acceptance of credit/debit cards and other contactless payment methods [26]. Their results show that NFC payment has a great advantage over other methods, but it also has some user doubts. They also surveyed value and risk perception, which had about 290 participants. The authors have claimed that the integrated value-risk perception is a significant factor in the adoption of NFC payments with smartphones so that the user stimulation to be used due to having utilitarian and enjoyment values; also, psychological and privacy risks are the most significant deterrents [27].

5- NFC Payment Security Issues and its Challenges

When a new payment system replaces traditional payment systems, the first issue to be taken care of is its security. In fact, when a user decides to switch from conventional payment methods to NFC payment, the most critical factor is how well the security will be achieved in this transaction. In general, the NFC technology has a proper security property due to its low support range. Although this feature gives users a sense of reliability, some security threats have remained as well. Also, some reports indicate the manipulation of thirds parties has occurred in the NFC transaction [15]. In order to better overcome this challenge, SE and HCE have been added to new NFC generation devices. The SE of NFC provides the security properties for an NFC-enabled device. SE has the following types:

- Embedded hardware: this SE type is the static element in an NFC-enabled device, which is embedded in the smartphone or tablet; also, the user enables to personalize the security settings after buying the smartphone. In fact, this type of SE is embedded in the smartphone at the manufacturing company.
- SMC: a smart memory card element and a smart card controller can make this type of SE. This type of smart card can supply a high level of security. Although many NFC versions are equipped with security elements, SMC is compatible with nearly all of the interfaces and standards such as ISO/IEC 7816, Global Platform, and Java Card [28]. As regards, the SMC is removable and provides a flexible scheme; also it has a large memory capacity and can easily handle the transactions in payments.
- UICC: this type of security element, which is called the Universal Integrated Circuit Card is based on the smart SIM card technique. Therefore, these cards are added to SE of NFC to protect the personal information of the users [13].
- TMB: Mobey Forum has introduced this technology as future technology and a new NFC secure element. This type of SE is located in the CPU of smartphones, which can handle a wide range of NFC's security applications. This facility causes it as a proper candidate for becoming an independent future SE.

There is another classification for SE of NFC technology so that the SE schemes can be classified into non-removable SEs, removable SEs, flexible SE solutions. As mentioned before, HCE is the latest SE for NFC technology and can manage the security applications of NFC with high reliability. In fact, HCE separates the card emulation mode, which is mostly used in payment transactions from SE. In fact, in using the HCE as a SE, a smartphone can perform the card emulation mode, while its security data is stored at the different location such as in another device or even in cloud storage. Figure 4 shows a comparison between SE and HCE.

Although HCE is a perfect approach to ensure an NFC transaction's security issues, there are some remaining challenges. The major challenge for HCE is when its data is stored in cloud memory. In fact, when a user intends to carry out an NFC transaction, maybe he/she does not access the internet, which fails the transaction [29].

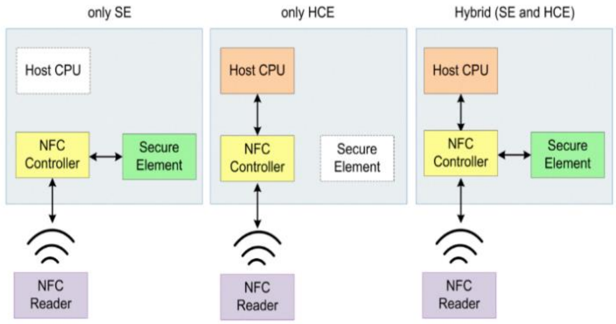

Fig. 4. Comparison of SE and HCE Architecture [30].

Although a decent research background exists for some issues of NFC applications, the future research directions for SE of NFC and HCE are suggested as follows.

- Proposing access control models to secure NFC elements compatible with smartphone OSs.
- Developing an alternative model for HCE as a security element.
- Proposing a secure communication protocol for cloud-based HCE in NFC.

- Developing an alternative model for removable SEs also and improving security SMC and UICC to achieve a more secure SE.
- Exploring possible methods for proposing a more reliable HCE architecture.
- Proposing a novel non-removable SE to apply in the current embedded hardware SEs.
- Evaluation and analysis of the cloud-based HCE for a hybrid system.
- Extensive research concerning market needs and device compatibility with the satisfaction of users who are interested in SE and security issues.
- Analysis of the connectivity between HCE and various smartphone OSs.
- Analysis of the power management and power-saving strategies for HCE and cloud-based HCE [31].

5-1- Security Threats of NFC Payment

There are various security threats for NFC payments that are introduced as follows.

5-1-1- Eavesdropping

Eavesdropping means that an attacker can hear the RF signal of an NFC transaction. Generally, eavesdropping is comfortable in an active NFC-enabled device. According to [32], an active NFC device, which generates its RF signals, can be heard at 10 meters, whereas in a passive device this distance is reduced to 1 meter. In the eavesdropping attack, an attacker uses a powerful active antenna. It seems that physically separating the channel between the two NFC devices can solve this problem.

5-1-2- Data Modification or Corruption

In this attack, an attacker uses a powerful antenna to manipulate the transferred data between two NFC devices at the valid frequency and at the right time. The manipulate data can be rubbish data to interrupt the connection and purposeful data to modify the transaction properties and information. The victim of this type of security threat is passive devices. The threats of this type of attack increase when a weak coding scheme is applied; whereas, a secure coding scheme can prevent the attacker's success. However, there is a trade-off between the security protection level in eavesdropping and data modification or corruption attacks so that the bidirectional active mode with baud data rate equal to 106 is the most unsafe condition to eavesdropping [33].

5-1-3- Man-in-the-Middle Attack

In this attack, a third party cuts off the NFC communication between the two NFC-enabled devices. In fact, the attacker acts as a relay between the NFC devices also transmits the changed information to the actual receiver device without the two devices getting to know that there is a third party. As regards, the support range of this technology is deficient; the occurrence probability of this type of attack in the NFC connection is low. In general, using an active-passive communication link between the NFC-enabled devices can identify the third party and reduce the risk of this type of security threat. In fact, applying both active devices prevent detection of the attacker.

Considering these types of NFC payment attacks, possible future research topics on this subject are suggested as follows.

- Proposing a physical channel protection scheme to avoid eavesdropping.
- Exploring the power-saving mechanisms to develop energy-efficient and functionally secure communications.
- Designing an extra passive antenna to be placed near the NFC payment devices or even inside the NFC device to detect the possible attacker to avoid the man-in-the-middle attack, data corruption, and modification accordingly.
- Modeling a convex problem to solve the trade-off situation in security protection level of eavesdropping attacks, data corruption, and modification attacks. In general, the distance, signal power, and coding schemes can be suitable parameters to model and design the convex problem.

6-Future Directions of NFC Payment

In general, NFC payment is a popular application of the NFC technology, which allows users to perform their transactions. Today, many shops and stores are equipped with this technology, but new efforts are still needed to extend this technology to more stores and smartphones. As a result, the first aim of the NFC Forum is that spreading this technology to more countries, shops, and smartphones. Also, user trust is another important factor in expanding NFC payments in the future, so that the users insist that their money be must securely transfer. The mentioned aims can be achieved by some research that is carried out by statistical experts that survey the completed questionnaires related to users' experience about the NFC payment.

Apart from the market-related issue and matters of the development of NFC technology, protocols, standards, and security are three significant problems related to the NFC payment, which directly affects the NFC payments future directions. In the previous sections, the future directions related to each subject have been suggested. The presented future directions can give useful insights about how NFC payments can be a faster and more secure contactless payment technology to carry out the transactions with real ease. However, a point that should not be forgotten is that much research has to be done to refine NFC's new protocols and standards, also fill out the security gaps of NFC payments for making a bright future for this technology. Although extraordinary research efforts have been carried out to improve NFC technology and NFC payment, there still are some primary future directions as follows.

- Designing the more powerful NFC antennas to dominate the possible attacks and threats.
- Proposing a new communication standard that provides a higher definition of QoS in NFC.
- Proposal for efficient modulation and coding techniques that make eavesdropping is impossible for an attacker.
- Proposing an efficient protocol for NFC-enabled devices for payment applications based on power management and power saving issues.
- Evaluating the integration of this technology with new technologies such as the IoT to accelerate the usage of this technology.

7-Conclusions

In this paper, we have been investigated the current payment methods, also the pros and cons of NFC payment. Our evaluations show that NFC payment can outperform in comparison to the traditional payment methods in terms of speed, reliability, security, and ease of use. Moreover, we conclude NFC technology is growing faster in countries with a younger population. Likewise, security issues and challenges of the NFC payment have been surveyed in this paper. We have been tried to focus on the technical problems since the market-related issues have better solved by users' questionnaires also have analyzed by statistical and marketing experts. The technical challenges discussed in this article mainly related to security, protocols, and standard issues. Moreover, future directions have been proposed for NFC technology and NFC payments in terms of designing, architecture, and protocols.

References

[1] P. Chandrasekar and A. Dutta, "Recent Developments in Near Field Communication: A Study," *Wirel. Pers. Commun.*, pp. 1–20, Sep. 2020.

[2] S. Chabbi, R. Boudour, F. Semchedine, and D. Chefrour, "Dynamic array PIN:A novel approach to secure NFC electronic payment between ATM and smartphone," *Inf. Secur. J. A Glob. Perspect.*, vol. 29, no. 6, pp. 327–340, Nov. 2020.

[3] P. Escobedo, M. Bhattacharjee, F. Nikbakhtnasrabadi, and R. Dahiya, "Flexible Strain and Temperature Sensing NFC Tag for Smart Food Packaging Applications," *IEEE Sens. J.*, vol. 21, no. 23, pp. 26406–26414, Dec. 2021.

[4] N. Song, Q. Wang, D. Jiao, H. Pan, L. Shi, and P. Ding, "Highly thermally conductive SiO2-coated NFC/BNNS hybrid films with water resistance," *Compos. Part A Appl. Sci. Manuf.*, vol. 143, p. 106261, Apr. 2021.

[5] R. Tso, "Untraceable and Anonymous Mobile Payment Scheme Based on Near Field Communication," *Symmetry (Basel).*, vol. 10, no. 12, p. 685, Dec. 2018.

[6] H. Seddiqi and S. Babaie, "A New Protection-based Approach for Link Failure Management of Software-Defined Networks," *IEEE Trans. Netw. Sci. Eng.*, pp. 1–10, 2021.

[7] M. Chung, "Short distance data transmission method using inaudible high-frequencies between smart devices," *Telecommun. Syst.*, vol. 70, no. 4, pp. 583–594, Apr. 2019.

[8] F. Liébana-Cabanillas, S. Molinillo, and M. Ruiz-Montañez, "To use or not to use, that is the question: Analysis of the determining factors for using NFC mobile payment systems in public transportation," *Technol. Forecast. Soc. Change*, vol. 139, pp. 266–276, Feb. 2019.

[9] E. L. Wadii, J. Boutahar, and S. E. L. Ghazi, "NFC Technology for Contactless Payment Echosystems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 391–397, 2017.

[10] R. Lyu, W. Cheng, and W. Zhang, "Modeling and Performance Analysis of OAM-NFC Systems," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 7986–8001, Dec. 2021.

[11] V. Coskun, K. Ok, and B. Ozdenizci, *Near field communication (NFC): from theory to practice*. John Wiley & Sons, 2011.

[12] J. Besnoff, M. Abbasi, and D. S. Ricketts, "High data-rate communication in near-field RFID and wireless power using higher order modulation," *IEEE Trans. Microw. Theory Tech.*, vol. 64, no. 2, pp. 401–413, 2016.

[13] M. de Reuver and J. Ondrus, "When Technological Superiority is not Enough: The Struggle to Impose the SIM Card as the NFC Secure Element for mobile payment platforms," *Telecomm. Policy*, vol. 41, no. 4, pp. 253–262, 2017.

[14] M. D. Steinberg, C. Slottved Kimbriel, and L. S. d'Hont, "Autonomous near-field communication (NFC) sensors for long-term preventive care of fine art objects," *Sensors Actuators A Phys.*, vol. 285, pp. 456–467, Jan. 2019.

[15] N. Druml *et al.*, "Secured miniaturized system-in-package contactless and passive authentication devices featuring NFC," *Microprocess. Microsyst.*, vol. 53, pp. 120–129, 2017.

[16] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card

Module using NFC and Biometric Authentication for Peer-to-Peer Payment," *IEEE Consum. Electron. Mag.*, vol. 6, no. 1, pp. 82–93, 2017.

[17] P. Teengam *et al.*, "NFC-enabling smartphone-based portable amperometric immunosensor for hepatitis B virus detection," *Sensors Actuators B Chem.*, vol. 326, p. 128825, Jan. 2021.

[18] Y. W. Juen and D. Balachandran, "Predicting the diffusion of NFC-enabled smartphone payment in Malaysia," *Int. J. Model. Oper. Manag.*, vol. 8, no. 3, p. 266, 2021.

[19] A. E. Varjovi and S. Babaie, "Green Internet of Things (GIoT): Vision, applications and research challenges," *Sustain. Comput. Informatics Syst.*, p. 100448, Sep. 2020.

[20] S. Naraparaju, P. Jalapati, and K. Nara, "Smart Poster for Tourism Promotion Through NFC Technology," Springer, Singapore, 2019, pp. 507–519.

[21] U. Demir Alan and D. Birant, "Server-Based Intelligent Public Transportation System with NFC," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 1, pp. 30–46, 2018.

[22] K. S. Staykova and J. Damsgaard, "The race to dominate the mobile payments platform: Entry and expansion strategies," *Electron. Commer. Res. Appl.*, vol. 14, no. 5, pp. 319–330, 2015.

[23] Y. J. Ng, "Near field communication (NFC) mobile payment in Malaysia: a partial least square-structural equation modelling (PLS-SEM) approach," *Int. J. Model. Oper. Manag.*, vol. 7, no. 2, p. 134, 2019.

[24] D. Veloz-Cherrez and J. Suárez, "NFC-Based Payment System Using Smartphones for Public Transport Service," Springer, Cham, 2019, pp. 34–44.

[25] I. Ramos-de-Luna, F. Montoro-Ríose, and F. Liébana-Cabanillas, "Determinants of the intention to use NFC technology as a payment system: an acceptance model approach," *Inf. Syst. E-bus. Manag.*, vol. 14, no. 2, pp. 293–314, 2016.

[26] M. Cocosila and H. Trabelsi, "An integrated value-risk investigation of contactless mobile payments adoption," *Electron. Commer. Res. Appl.*, vol. 20, pp. 159–170, 2016.

[27] X. Pu, F. T. S. Chan, A. Y. L. Chong, and B. Niu, "The adoption of NFC-based mobile payment services: an empirical analysis of Apple Pay in China," *Int. J. Mob. Commun.*, vol. 18, no. 3, p. 343, 2020.

[28] D. A. Ortiz-Yepes, "A review of technical approaches to realizing near-field communication mobile payments," *IEEE Secur. Priv.*, vol. 14, no. 4, pp. 54–62, 2016.

[29] M. M. Gharamaleki and S. Babaie, "A New Distributed Fault Detection Method for Wireless Sensor Networks," *IEEE Syst. J.*, vol. 14, no. 4, pp. 4883–4890, 2020.

[30] F. S. M. Tafti, S. Mohammadi, and M. Babagoli, "A new NFC mobile payment protocol using improved GSM based authentication," *J. Inf. Secur. Appl.*, vol. 62, p. 102997, Nov. 2021.

[31] C. Peres, M. Emam, H. Jafarzadeh, M. Belcastro, and B. O'Flynn, "Development of a Low-Power Underwater NFC-Enabled Sensor Device for Seaweed Monitoring," *Sensors*, vol. 21, no. 14, p. 4649, Jul. 2021.

[32] A. B. M. Alim Al Islam, T. Chakraborty, T. A. Khan, M. Zoraf, and C. S. Hyder, "Towards defending eavesdropping on NFC," *J. Netw. Comput. Appl.*, vol. 100, pp. 11–23, Dec. 2017.

[33] C. Thammarat and W. Kurutach, "A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification," *Int. J. Commun. Syst.*, vol. 32, no. 12, p. e3991, Aug. 2019.