An Overview of Near Field Communication and its Application in the Payment Sector

Roshni Sen[1], Dr. Nagaraj Bhat[2]
[1] *Student, R.V. College of Engineering, Bengaluru*
[2] *Assistant Professor, R.V. College of Engineering, Bengaluru*
[1]*roshnisen.ec17@rvce.edu.in*, [2]*nbhat437@gmail.com*

Abstract: *With electronic payment systems becoming the quintessence of today's technologically driven society, the integration of Near Field Communication (NFC) technology in this field has made the experience of consumers at point of sale (POS) terminals exponentially favorable. This technology, based on Radio Frequency Identification (RFID) and implemented to allow for short range communication to be possible, has been adapted worldwide in a variety of applications and has enabled secure bidirectional exchange of data between two NFC enabled devices. NFC allows communication between two NFC-enabled devices within a range of 10 centimeters. The integration of NFC into mobile devices has greatly increased the capabilities of mobile phones, with the potential to do even more. This occurrence has prompted a number of studies on NFC. At the same time, there are substantial issues about customer satisfaction, privacy, speed and convenience, among other things.*

This paper introduces NFC technology and its various modes of operation, followed by a review of its application in the payment sector with the help of the architecture of an NFC device. Furthermore, threats to the security of short-rage data exchange with respect to NFC are also analyzed.

Keywords: *Near Field Communication, radio frequency identification, inductively coupled antennas, NFC device architecture, mobile payment applications*

1. Introduction

As wired technology is rapidly being replaced by wireless technology, it is a norm for end consumers today to access a range of services from a single device, including various forms of entertainment such as movies, television shows, music, communication with one's peers and colleagues, and financial services such as net-banking, viewing of bank statements, electricity bill payment, etc. [1]. To ensure the security of online transactions, smart payment cards or dedicated payment applications is widely used today's society. This has resulted in significant advancements in the domain of contactless technology, including NFC. The majority of today's smartphones are NFC-enabled [2]. Contactless or proximity payments, often known as NFC Payments, are one of NFC's many applications which has proven to be a faster, more secure and more convenient method for users than other digital payment technologies [3]. Besides smartphones, tags with integrated circuits that use NFC technology are available and have the ability to store data which can be read by all NFC-enabled devices. NFC-enabled tags vary in their capability to store data and are categorized into 4 types based on this. All NFC-enabled tags have a unique identification number and are used in a variety of real-time applications.

Unlike Bluetooth technology, which has a range of up to nearly 30 meters, communication via NFC technology deals with a shorter range of 4 to 10 centimeters [1]. It uses a radio frequency of 13.56 megahertz of to establish a link between two NFC-enabled devices to send data across. NFC eliminates the requirement for any external programming to connect the devices by serving as an enabler. Instead, by simply touching two capable phones that support NFC or a phone that supports NFC and an NFC-enabled tag against each other, any two such devices or a device and an NFC-enabled tag can pair. In an such scenarios, communication is performed when one device initiates the transfer of data from itself to the target device by creating a magnetic field and the receiving device is activated by making use of this magnetic field and receives the data sent.

Depending on the type of data to be sent, the NFC standard provides three different modes of operation [4]. The peer-to-peer (P2P) mode, which allows two NFC-enabled devices to exchange data, is perhaps the most widely utilized. When sending data, both devices are said to be active, and when receiving data, both devices are said to be passive. Android Beam makes use of the P2P mode to transfer data from one Android smartphone to another by touching them against each other. The read/write mode of operation is the second mode which occurs when an active NFC device, such as a smartphone, establishes a link with a passive NFC device, such as a tag or a sticker, in order to read data from it. The final mode of operation is called host card emulation (HCE), in which the NFC enabled device can be used as a contactless credit, debit or loyalty card to make payments [3]. It essentially allows the NFC device to emulate a payment card which can then be used instead of physical payment cards at POS terminals for processing money transfer. In this mode, the NFC-enabled reader device creates the RF field instead of the smartphone doing the same.

2. Background

NFC devices are of two types: active and passive [1]. An active NFC device can transmit as well as receive data. The majority of Android smartphone devices today are active NFC devices whereas only the latest Apple smartphone devices are active NFC devices [5]. NFC is commonly used to store and transfer contact or payment card information. On Android smartphone devices, apps like Google Pay allow you to pay at stores, which have NFC readers, by merely tapping your device. Apple however does not allow any payment application besides Apple Pay to serve as an NFC-payment option for its smartphones as of today.

On the other hand, passive NFC devices are limited to data transmission, although it does have an added benefit: the devices can operate without power. Passive NFC can be found on a variety of devices that need to communicate with others. Students of Carnegie Mellon University, for example, make use of NFC technology in their student identity cards. When a student touches their card on the bus' card reader, it sends information via NFC to the active card reader, allowing it to recognize that the student is from Carnegie Mellon University and hence, charge their journey to the university. NFC can also be used on billboards and signs. NFC functionality can also be used on billboards and advertisements. One can typically acquire more information on the issue presented on the board by tapping one of these with one's smartphone.

2.1 Magnetic Induction

Magnetically induced signals are used by NFC devices to communicate. As a result, instead of electromagnetic radiation used in typical wireless communication, energy is linked between transceivers during transmission. In the process of magnetic induction, the NFC-reader emits a small electric current that produces a magnetic field surrounding it. This field is intercepted by another coil in the receiving device, which converts it back into electrical impulses for data transmission. When NFC is activated, the NFC chip in the hardware of the smartphone is sent a signal. The integrated circuit then generates a magnetic field as electricity flows through it. At this point, the smartphone is the device that generates the magnetic field. A magnetic field is generated in the transponder as a result of this. As a direct consequence of this, the transponder generates a radio field that interacts with the electromagnetic field produced by the mobile device.

NFC antennas that are inductively coupled and separated by a small distance (between 4 to 10 centimeters), are shown in Figure 1. Magnetic induction allows data to be communicated between these transceivers when they are close together [4]. Figure 2 depicts the equivalent circuit diagram for the antennas shows in Figure 1. The variation of power at the receiver with distance is to be analyzed here.

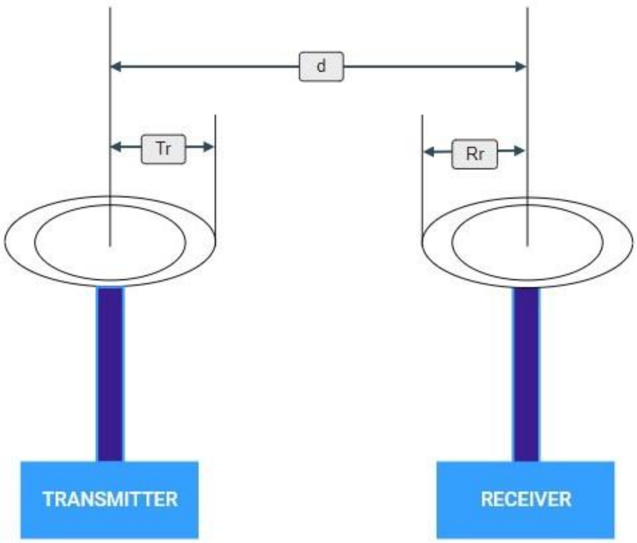

Figure 1. Inductively coupled NFC antennas

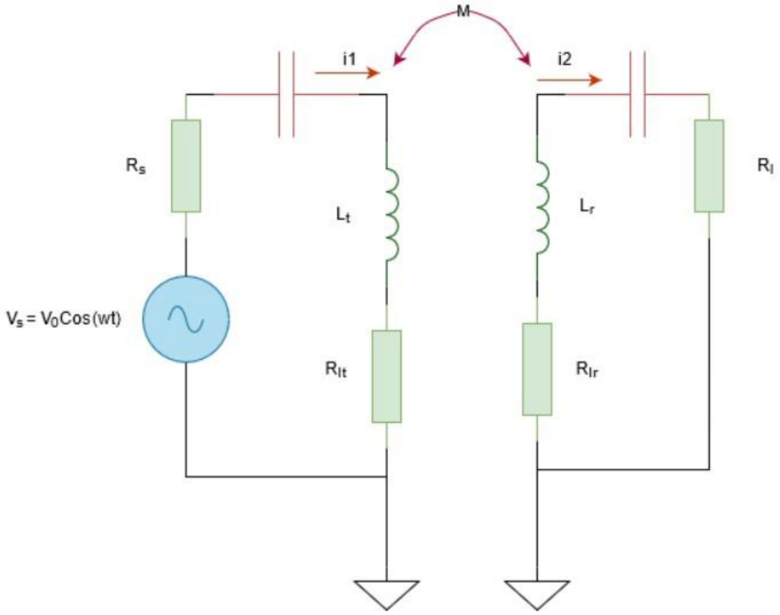

Figure 2. Equivalent circuit diagram of inductively coupled NFC antennas

[6] provides a mathematical derivation for the receiver power for the circuit in Figure 2, and receiver power is written as

$$P_R(\omega) = \frac{P_T Q_T Q_R \eta_T \eta_R (r_T^3 \mu_0 \mu_T r_R^3 \mu_0 \mu_R \pi^2)}{(r_T^3 + d^2)^3} \tag{1}$$

where

- d: Distance between transceivers
- r_T, r_R: Radii of transmitter and receiver antenna coil respectively
- μ_0: Permeability of air
- μ_T, μ_R: Relative permeability of antenna coil core of transceivers
- P_T: Transmission power
- Q_T, Q_R: Q-factors of transmitter and receiver antenna respectively
- η_T, η_R: Transmitter and receiver antenna efficiency

From Eq. (1), it can be observed that the power at the receiver is influenced by multiple factors. As a result, changing any of the parameters has an impact on the expression on the left. For the purpose of our analysis, we ran a simulation in MATLAB using the above Eq. (1) and the following parameters:

- d = 0 cm to 35 cm
- r_T, r_R = 3 cm, 2 cm
- μ_0 = 1
- μ_T, μ_R = 1, 1
- P_T = 25 dBm
- Q_T, Q_R = 48
- η_T, η_R = 75%

Figure 3 depicts the simulation outcome for the above situation. The power at the receiver diminishes with the sixth power of distance, as shown in the plot and in the power equation above (1). When compared to typical wireless transmission, where signal strength declines as the square of the distance in empty space, this is substantial.

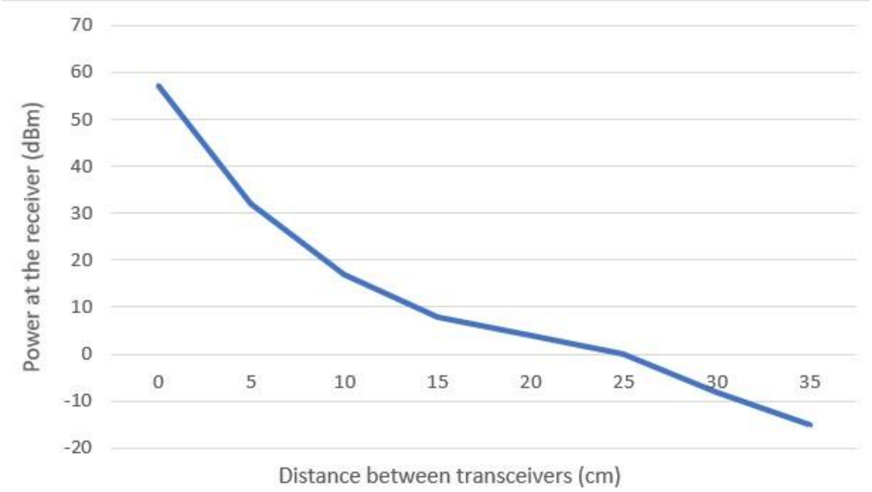

Figure 3. Power at the receiver at various distances between transceivers

2.2 NFC-enabled Device Architecture

An NFC-enabled smartphone device is comprised of two integrated circuits: NFC Interface and Secure Element (SE) [5].

i. *Secure Element:* Secure element is a tamper-proof microcontroller that allows confidential data to be stored and executed in a safe environment. It safeguards against attacks on both a physical and logical level, protecting the integrity and confidentiality of its data. SE can be implemented in 3 ways:

   a. SE in the form of a Universal Integrated Circuit Card (UICC) or subscriber identification module (SIM) card.
   b. Embedded SE, in which case chips are directly attached to the device mother board. In this case, unlike the others , the SE cannot be swapped out or extracted; it is linked permanently to the device.
   c. External (add-on) SE by inserting NFC-enabled microSD in the microSD slot of smartphones.

   An application of secure element is authentication. A robust authentication mechanism based on credentials saved and handled in a SE may be used to safeguard access to a web service instead of using a username and password. Another application is allowing for digital payment transactions [7].

ii. *NFC Interface:* Further, the NFC Interface consists of two parts: an NFC antenna and an integrated circuit called an NFC controller. This allows NFC transactions to be possible [3].

   The most crucial component of any smartphone is the baseband controller or host controller. The host controller and the NFC controller, which directs the data from the NFC-enabled reader to the SE, are linked by the Host Controller Interface (HCI), as shown in Figure 4. The host controller is in charge of determining the NFC controller's modes of operation, processing data transmitted and received through the HCI, and forming a link between the NFC controller and the SE.

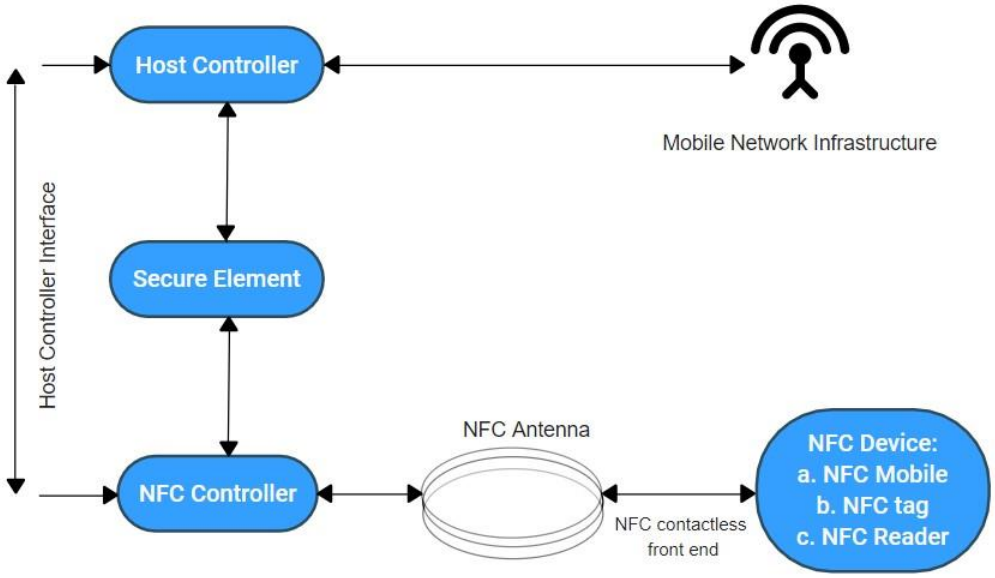

Figure 4. NFC-enabled Device Architecture

iii. *NFC Tags*: Besides NFC-enabled phones, NFC-enabled tags or stickers are also available. Smart billboards, POS terminals, electronic gadgets, and other goods with readable NFC tags are common examples of items with NFC tags implanted in them. It's a chip that's normally buried beneath a sticker with the NFC logo on it to alert users to its presence. Small data, such as contact information, unified resource identifiers (URIs), and login credentials, are generally contained in these tags.

3. NFC-enabled Mobile Payments

Tap-to-pay technology is used many NFC-enabled mobile devices to perform all sorts of payment transactions by loading the consumer's payment details onto the NFC mobile device [8]. It can safeguard and store payment card (credit/debit/loyalty cards) information and use this data for transactions at any store with capable NFC readers. It's simplicity, portability and ability to perform transactions in a manner of mere seconds are its most attractive features [4].

3.1 End-to-end working of NFC payments

For each transaction, NFC payment considers and associates two significant pieces of data: RFID and a secure encrypted password. A unique code is transmitted by a secure radio, which is present in the mobile device, to the payment system of the retailer. The transaction information is then provided to the user. To confirm and approve a particular transaction, the user is required to enter a personal identification number (PIN). The NFC secure radio is designed in such a way that just one app on the mobile device can approve a transaction and is segregated from the rest of the device's operating system to safeguard it against from viruses and hackers. Hence, NFC is considered to be extremely safe due to this technology [9].

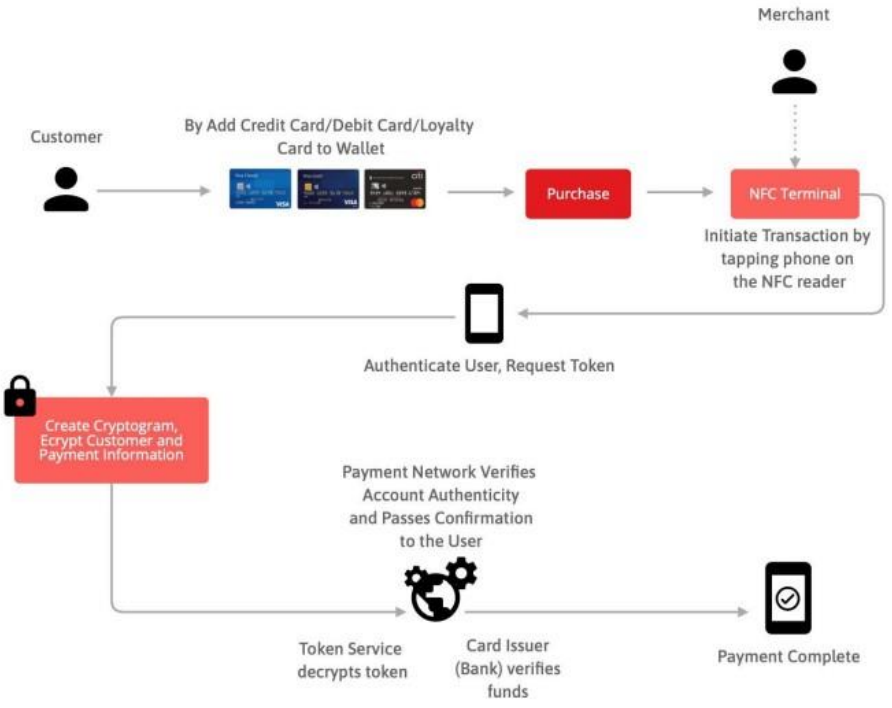
Merchant
Customer
By Add Credit Card/Debit Card/Loyalty Card to Wallet
Purchase
NFC Terminal
Initiate Transaction by tapping phone on the NFC reader
Authenticate User, Request Token
Create Cryptogram, Ecrypt Customer and Payment Information
Payment Network Verifies Account Authenticity and Passes Confirmation to the User
Token Service decrypts token
Card Issuer (Bank) verifies funds
Payment Complete

Figure 5. A typical NFC-based payment transaction

Figure 5 shows the end-to-end flow of a typical payment using NFC. The prerequisite for any NFC-based payment mobile application to work at any point-of-sale (POS) terminal is that a user must have added a credit card, debit card or loyalty card, which is specific to that store, to that particular mobile application. The user will initiate the payment transaction at the NFC terminal on the merchant end by tapping their phone on the NFC reader [4]. This will trigger an authentication step on the user's mobile phone which they will verify using either their local security set up (fingerprint, face ID or pattern) or a PIN. This step ensures that in case the phone is stolen, no payments can be made without the owner's authentication. After the user has authorized the payment from their end, their card details are sent to the card network (i.e., Visa, Mastercard, American Express, etc.) which creates a token out of the card details, such as card number, cardholder name, expiry date and card verification value (CVV). The token is a string of random characters and hence cannot be decrypted, making this method of transferring card details absolutely secure [1]. This token is sent to the backend servers and at the point of a payment, a cryptogram is created using the token and the transaction details of the user. This cryptogram is sent via NFC to the NFC reader at the merchant end. The cryptogram received by the NFC reader is further forwarded to the card network, where the card details corresponding to the token in the cryptogram are extracted. The card network verifies the account authenticity and the card issuer verifies the funds. Once the funds are verified, the payment transaction is completed and a "Payment Successful" message is displayed to the user on their mobile screen. This process happens in a matter of seconds [9].

3.2 Security Concerns regarding NFC Technology

New users of near field communication technology, particularly those using it for financial purposes such as storing payment card information, are understandably anxious regarding the security and protection of their personal information initially. Eavesdropping, data corruption or manipulation, interception attacks, and physical theft are all possible security threats.

i. *Data Corruption:* Data corruption, a type of denial of service (DoS) attack, he attacker may try to disrupt communications by sending potentially genuine data or by obstructing the channel, causing legitimate data to be distorted [10]. This type of NFC security breach is detectable. Monitoring the data as it is communicated will allow them to identify any such assault since the power required by the system for a successful attack is substantially larger than what the NFC device receiving the data can detect.

ii. *Relay Attacks:* In network security, a relay assault is sometimes known as a "man in the middle" attack. In this situation, a n attacker intercepts a signal from the transmitter, makes modifications to it, and delivers it to the receiver, and vice versa. Despite this being a significant concern in large network security, it is incredibly challenging, if not impossible, to do so in NFC since both transceivers can detect radio fields during communication and are aware of unknown RF fields or collisions. Devices must be in an active-passive pairing in order to avoid such attacks [11][12].

iii. *Eavesdropping:* When an attacker “listens in” on an NFC transaction, this is known as eavesdropping. To obtain private information, the attacker is not required to intercept every single signal. Eavesdropping can be avoided using two approaches [10][11]. The range of the NFC transaction is the first consideration. Because the devices must be near together to deliver signals, the attacker only has a little window of opportunity to intercept signals. The next approach is that of secure channels. The data is encrypted when a secure channel is formed which can only be decoded by an authorized device. It is ideal for users of NFC to make sure that the organizations with which they conduct business employ secure channels. Figure 6 shows a visual representation of eavesdropping.

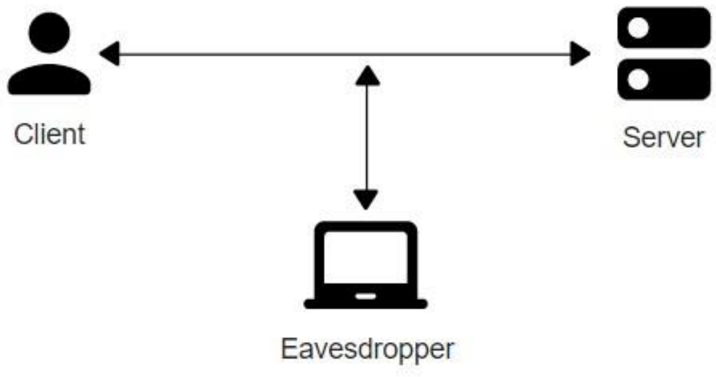

Figure 6. Eavesdropping Attack

iv. *Lost devices:* Mobile devices are prone to being misplaced. They do, however, contain sensitive information such as debit/credit card details and personal information. As a result, anyone who locates the misplaced device can use it in the same way that a lost debit/credit card can be used [12]. Pre-existing security measures in mobile devices, such as securing access with PIN codes, fingerprint or facial identification, is the only answer in this situation.

4. Conclusion

In this paper, we have discussed the fundamentals of NFC, how it is based on the principle of magnetic induction, observed how the power at the receiver diminishes as the range between transceivers grows and looked at various types of NFC devices such as smartphones, tags, stickers, etc. In terms of payments, all forms of authenticity and data confidentiality is handled by the secure element. Although there are security problems with NFC, compared to other communication technologies, it is extremely difficult to breach. Among the many applications of NFC technology available, the mobile payment solution is one of the most commonly and widely used [13]. We have established that, though it is not the optimum solution, it improves not only a variety of user impressions but also operational resilience.

REFERENCES

[**1**] N. S. S. Shobha, K. S. P. Aruna, M. D. P. Bhagyashree and K. S. J. Sarita, "NFC and NFC payments: A review," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), 2016, pp. 1-7, doi: 10.1109/ICTBIG.2016.7892683.

[**2**] T. Dahlberg, N. Mallat, J. Ondrus and A. Zmijewska, "Past present and future of mobile payments research: A literature review", Commer. Res. …, 2008.

[3] V. Sharma, P. Gusain and P. Kumar, "Near Field Communication", Proceeding of the Conference on Advances in Communication and Control Systems, 2013.

[4] S. K. Timalsina, R. Bhusal and S. Moh, "NFC and its application to mobile payment: Overview and comparison," 2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012), 2012, pp. 203-206.

[**5**] I. A. Brohi et al., "Near field communication enabled payment system adoption: A proposed framework," 2017 IEEE 3rd International Conference on Engineering Technologies and Social Sciences (ICETSS), 2017, pp. 1-5, doi: 10.1109/ICETSS.2017.8324199.

[**6**] J. I. Agbinya and M. Masihpour, "Power equations and capacity performance of magnetic induction communication systems", Wirel. Pers. Commun., vol. 64, no. 4, pp. 831-845, 2012.

[**7**] "NFC-Enabled Cellphone Shipments to Soar Fourfold in Next Five Years IHS Online Newsroom", press.ihs.com, 2014, [online] Available: http://press.ihs.com/press-release/design-supply-chain/nfc-enabled-cellphone-shipments-soar-fourfold-next-five-years.

[**8**] S. Dhar and A. Dasgupta, "NFC technology: Current and future trends in India," 2014 International Conference on Contemporary Computing and Informatics (IC3I), 2014, pp. 639-644, doi: 10.1109/IC3I.2014.7019680.

[**9**] J. Chen, K. Hines, W. Leung, N. Ovaici and I. Sidhu, NFC Mobile Payments, 2011.

[**10**] C. Mulliner, "Vulnerability analysis and attacks on NFC-enabled mobile phones," Proc. of International Conference on Availability, Reliability and Security (ARES '09), pp. 695-700, Mar. 2009.

[**11**] E. Haselsteiner and K. Breitfu, "Security in near field communication (NFC)," Proc. of Workshop on RFID security, 2006.

[**12**] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger, "NFC devices: Security and privacy", ARES 2008-3rd Int. Conf. Availability Secur. Reliab. Proc., pp. 642-647, 2008.

[**13**] V. Patil, N. Varma, S. Vinchurkar and B. Patil, "NFC based health monitoring and controlling system," 2014 IEEE Global Conference on Wireless Computing \& Networking (GCWCN), 2014, pp. 133-137, doi: 10.1109/GCWCN.2014.7030864.