An IOT based secure transaction system using Micro field communication

Sanjay Kumar 1, Dhananjay Singh 2, Rahul Singh 3, Gagan Gupta 4, Dr. S K Singh 5

2Student, Department of Information Technology, Galgotias College of Engineering & Technology, Gr. Noida, Uttar Pradesh, India
1,3,4Assistant Professor, Department of Information Technology, Galgotias College of Engineering & Technology, Gr. Noida, Uttar Pradesh, India
3Professor, Department of Information Technology, Galgotias College of Engineering & Technology, Gr. Noida, Uttar Pradesh, India

Email: dhananjay0397@gmail.com, skhakhil@gmail.com

Abstract. The humans have always tried to improve quality of living and technology plays a major role in this cause. Modern technology has been evolving with the emergence of smart technologies. Cash Based transaction involves lot of human effort of withdrawing and then storing the cash. It is also an insecure way of payment involving fears of theft etc... With large amounts of data transfer and e-payment needs, NFC is one of the prime technologies contributing towards fast and secure transmission of electronic signals, data and money. This paper focuses on NFC technology utilisation for a simplified and secure unified transaction system using IOT. Internet of things is a technology of present and future which has its applications in various fields like healthcare, transportation, manufacturing etc… There has already been a lot of research and developments on utilisation of NFC technology for transactions, but we propose a secure wireless transaction system by providing features such as database connectivity and user authentication in the system.

Keywords: Near field communication, NFC technology, Rfid, smartcard, Contact less payments.

1. Introduction

Near Field Communication is a set of rules/ protocol which ensures simple wireless connectivity within a small range. This technology is primarily useful in contactless payment system, it can allow payments with mobile devices such as mobile, smartcards etc. It is not just limited to simplified payments transactions, NFC enabled devices can also be used for social networking, e-ticketing and file sharing (such as photo, video, contacts etc...). It is a short range wireless connectivity that uses magnetic field by bringing them within the range of 4cm. It is implemented through electromagnetic induction for simple secure and safe exchange between two devices. It has been successfully implemented for the first time by NOKIA in their smartphones. It operates on the principle similar to
that of smart card and RFID tags. The reader starts the communication and retrieves data from the card or the NFC enabled device.

2. Operation Modes of NFC

NFC is a short range RF system which transmits data between NFC enabled devices. One device acts as the initiator which is an active device generating magnetic field. It initiates the communication. The other device is the target. It is the passive device responding to the initiator. NFC enabled devices such as NFC Card performs read/write operations from tags and also be utilised a digital storage for NFC readers both at the same time NFC operates on various modes. The Operation modes of NFC are:
1. Card Emulation Mode
2. Peer to Peer Mode
3. Reader/Writer Mode

![Operating Modes of NFC](image)

**Figure 3 Operating Modes of NFC**

**2.1 Card Emulation Mode:**
In this mode the NFC cared stores multiple smart application in the smart card. Card emulator gets rid of the hassle of carrying numerous cards which fatten our wallets and are difficult to maintain. It helps make one unified smart card which caters to variety of our transactional needs.

![Card Emulation Mode](image)

**Figure 4 Card Emulation Mode**

In this mode the NFC reader generates the field enabling payment and ticketing system. It is compatible to work with the existing smart card systems.

**2.2 Reader/Writer Mode:**
In this mode NFC enabled device performs the role of reader like the smart cards which work without any contact between them. The NFC device can perform the task of reading and writing data into the detected NFC tags i.e. card with read/write operations. It enables communication of an NFC enabled device with the NFC tags. This mode functions in 2 sub modes, Reader mode and Writer mode. In reader mode data is read from NFC tag consisting of required information and program. In writer mode the NFC device such as mobile acts like initiator writing data to the tag. Its application are in Remote shopping, Poster Scanning etc.
2.3 Peer to Peer Mode:
In this mode the NFC devices are able to transmit and receive data between themselves. It is through a bi-directional channel in which data is transferred one at a time. One device waits until the other transfers data. Its applications are in money transfers, data exchange, Mobile Social i.e. Social Networking etc...

3. Current Usage Trends of NFC

NFC is a new yet a very resourceful concept. The concern while developing such system was, would it also have practical application or would it just be limited to a theoretical term. But in recent times there has been an enormous growth in the number of NFC enabled devices.
With several large companies investing in this technology, this technology looks to completely take over the contactless payment market in future. Google, Apple, Microsoft, Master Card are few of the many companies venturing and investing in NFC based payment systems.

Some major examples of NFC based contactless cards already in use are:

1. Express Pay
2. Master Card PayPass
3. Visa Paywave
4. RuPay Contactless
5. QuickPass etc...

With so many companies investing in this field, the value of NFC transaction will continue to increase, with projected value by 2020 estimated to be about USD 47 Billion.
4. Limitations of NFC Card Based Transactions

The previous models had many limitations such as follows:

1. Failure Rate: The NFC cards which are usually made up of plastics are used in harsher environments and as a result of wear and tear they encounter a higher failure rate. One way of overcoming this limitation is to use the card keeping them in an enclosed cover.

2. Privacy: This is another issue faced by the smart card systems. As the card are used in a mass transit system, the transaction operator and the authorities can track individual movements thus posing privacy risks.

3. Use abroad: It is easy to convey data at a quick speed in inland networks but it is not possible when such cards are used abroad.

4. Theft and Fraud: High value transactions are considered safe as they require the user to enter PIN each time the transaction is initiated. Whereas, in low transactions it is not necessarily required. This makes the card being vulnerable to being stolen or frauds.

5. Multiple Card detection: When two or more cards are within the range of the NFC the system may get confused as to which card is intended for the transaction and reader may charge the wrong card. For example in a wallet containing many cards a NFC reader intended for parking entry would detect the apartment entry card and reject the transaction.

5. Implementation & Result

We propose a model which takes into consideration all the drawbacks of previous NFC cards, and have also implemented the proposals in our project. To overcome the multiple card detection issue, we have proposed a unified NFC card which can cater all the transactional requirements irrespective of the bank or the field in which the card is being used. e.g. healthcare, ticketing, identification, payments etc.. To overcome the issue of authentication we propose a system connected to a GSM module. In our system the NFC card sends the card id to Sql database with the help of Arduino which works on scanning card in the MFRC 522 NFC reader setup. This ensures the authentication of the card as each card has unique credentials of the user associated with it. Further, the Arduino UNO board is connected with GSM800 module which provides internet service connectivity to the NFC card. This
provides SMS compatibility and as soon as any transaction in the card is processed, an SMS update is sent to the user’s registered contact number. This enables both authentication and accountability of the system.

Figure 10 Proposed Model Setup

6. Conclusion

Concluding, we would like to state that NFC is technology which continues to grow day by day with enormous future scope in implementation. Based on the recent trends the day would not be far when the people would completely rely on cashless and contactless modes of payment. Based on our understanding we have proposed a solution but there is still a lot of work which can be done in order to make the implementation of this system more secure and feasible for the common people. One such scope is to extend this NFC Card system to a JAVA based web based project which further can be used for complete transaction and database management over a website secured by username and password credentials. The user can add value, receive reports of previous usage and transactions and also add and delete records. In today’s busy world where people have less time, this system is a technology of the future which can help to achieve the target of simplifying the lives of people.

References

[1] Majumder, Alak. ShirshaGhosh, JoyeetaGoswami, and Bidyut K. Bhattacharyya. "NFC in IoT-Based Payment Architecture." (2017).

[2] Anguranak, Taweechai. “NFC Technology Payment System for Android Operation.” Journal of Software, 2015.
[3] Desai, Ekta, and Mary Grace Shajan. "A review on the operating modes of near field communication." *International Journal of Engineering and Advanced Technology (IJEA)* 2, no. 2 (2012): 322-325.

[4] Current Trends in Near Field Communication. 2017. http://nearfieldcommunication.org/current-trends.html (accessed May 18, 2019).

[5] Kumar, Sanjay, Ashish Negi, and J. N. Singh. "Semantic Segmentation Using Deep Learning for Brain Tumour MRI via Fully Convolution Neural Networks." Information and Communication Technology for Intelligent Systems. Springer, Singapore, 2019. 11-19.

[6] Brian, A. Larsan Aro, L. Arockiam, and P. D. S. K. Malarchelvi. "An IOT based secured smart library system with NFC based book tracking." *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)* 11, no. 5 (2014).

[7] Kumar, Sanjay, Gagan Gupta, and Kunwar Rajat Singh. "5G: Revolution of future communication technology." In 2015 *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 143-147. IEEE, 2015.

[8] Monteiro, David M., Joel JPC Rodrigues, and Jaime Lloret. "A secure NFC application for credit transfer among mobile phones." In 2012 *International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1-5. IEEE, 2012.

[9] Dutot, Vincent. "Factors influencing near field communication (NFC) adoption: An extended TAM approach." *The Journal of High Technology Management Research* 26, no. 1 (2015): 45-57.

[10] Sharif, Rabia, Syed Waqas Ahmad, Hirra Anjum, Naveed Ramzan, and Shahid Raza Malik. "Effect of infusion time and temperature on decaffeination of tea using liquid–liquid extraction technique." *Journal of Food Process Engineering* 37, no. 1 (2014): 46-52.

[11] van der Aalst, Wil MP, and Akhil Kumar. "Xml–based schema definition for support of interorganizational workflow." *Information Systems Research* 14, no. 1 (2003): 23-46.

[12] Gavish, B. and Gerdes, J. (1998) Anonymous Mechanisms in Group Decision Support Systems Communication. Decision Support Systems, 23(4), 297-328.

[13] Von Alan, R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design science in information systems research." *MIS quarterly* 28, no. 1 (2004): 75-105.

[14] Mulliner, C. (2009) Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. In *Proceedings of 2009, International Conference on Availability,Reliability and Security*. 695-700.

[15] Strommer, Esko, Jouni Kaartinen, Juha Parkka, Arto Ylisaukko-oja, and Ilkka Korhonen. "Application of near field communication for health monitoring in daily life." In 2006 *International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 3246-3249. IEEE, 2006.
[15] Tiwari, Naveen Kumar, and Sanjay Khakhil. "Security System for DNS using Cryptography." *International Journal of Computer Applications* 120, no. 17 (2015).

[16] Gupta, Anil Kumar, Shashank Shukla, Sandeep Saxena, and Sanjay Khakhil. "A Journey towards Workflow Scheduling of Cloud Computing." *International Journal of Computer Applications* 123, no. 4 (2015).

[17] Gupta, Anil Kumar, Shashank Shukla, Sandeep Saxena, and Sanjay Khakhil. "Bloom filter for elasticity in DBaaS." In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 672-677. IEEE, 2016.

[18] Shukla, Shashank, Anil Kumar Gupta, Sandeep Saxena, and Santosh Kumar. "An evolutionary study of multi-objective workflow scheduling in cloud computing." *International Journal of Computer Applications* 133, no. 14 (2016): 14-18.

[19] Shukla, Shashank, Anil Kumar Gupta, Santosh Kumar Upadhyay, and Ashu Gupta. "Wireless Sensor Data Collecting to MobileCloud Device." *International Journal of Computer Applications* 138, no. 11 (2016).

[20] AMAZON, MULTI-OBJECTIVE WORKFLOW SCHEDULING IN. "International Journal OF Engineering Sciences & Management Research."