SWITCHABLE AND CONFIGURABLE INSTRUMENTS FOR PAYMENT

Kalki

M.E, Ph.D.,UG Scholar Department of CSE Sathyabama Institute of Science and Technology
Chennai, India

Dr.M.Maheshwari ,

M.E, Ph.D.,UG Scholar Department of CSE Sathyabama Institute of Science and Technology
Chennai, India

Abstract

NFC stands for "Near Field Communication" and has been present on the market since quite a long period. This term designates the contact-free data transmission which makes use of the Radio-frequency identification (RFID-) technology. When compared to the other short-range radio technologies, NFC is extremely short ranged and what we can refer to as *people-centric*. Some of the other short-range communication technologies have similar characteristics, for example RFID, while others are completely different yet complimentary to NFC. Near-field communication (NFC) is a new wireless technology that could unite various standards and proprietary technologies found in the millions of standalone contactless cards. NFC readers connect with only one NFC payment device at a time. This eliminates all the possibilities of a nearby customer accidentally paying for someone else's purchase..NFC also allows its users to store multiple debit and credit cards on their mobile devices. With this, the users no longer need to carry cards in their wallets.

Keywords – NFC, API, FLUTTER, NFC TAGS PHP, MYSQL

I. INTRODUCTION

NFC stands for "near-field communication," the technology that enables communication and data-sharing between wireless-enabled devices in close proximity. NFC has many applications, including key fobs for access control systems, ID verification and wireless device pairing. NFC is easy to use. Accepting NFC mobile payments is a lot like using a traditional credit card with a magnetic stripe. In fact, many card readers are enabled to accept NFC payments. The difference with NFC is that a transaction is initiated not by reading a magnetic stripe on a card, but by having an NFC reader send a signal that's picked up by an NFC antenna on an NFC-enabled device.

1. NFC payments use an NFC-enabled reader. When this reader is initiated through point-of-sale (POS) system, it sends out a signal that searches for an NFC-enabled. payment device. When the reader detects the antenna of an NFC-enabled device, such as a phone or NFC-enabled credit card, the payment device communicates the payment info to the reader, and the payment is processed.
2. NFC mobile payments are contactless digital payment options that allow phones, tablets, or credit cards to communicate with NFC-enabled readers. NFC technology allows businesses to accept customer payments quickly and conveniently without requiring employees to handle or cards.
3. NFC mobile payments are an ideal payment-processing option for a range of businesses, including retailers, restaurants and professional service providers

II. LITERATURE SURVEY

The concept of a low-cost tag that can turn any item into a smart gadget is not necessarily new[1]. Yet, the majority of inexpensive smart tags without batteries or sophisticated circuitry can only carry out basic tasks like passively storing and communicating identification data about an object.The researchers had to create customised multi-antenna beamforming algorithms that work with Wi-Fi devices to detect the notches in the reflected Wi-Fi spectrum. It can be challenging to discern the LiveTag's reflected signal from all the other Wi-Fi signal reflections coming from walls, objects, and even people moving around in a room, thus this was necessary.

The algorithms project beams from a Wi-Fi device in a variety of directions in order to filter out those additional signal reflections. As a result, the LiveTag notches remain distinct and constant in the spectrum picked up by the Wi-Fi device receivers, but most objects end up having a variety of reflection characteristics that can be filtered out by the algorithm as background noise. Radio frequency identification (RFID) chips that may be printed as flexible paper-like tags were often used in some of the more prevalent historical instances of smart tags. When affixed to items like garments in retail outlets, these RFID tags can offer identity and location-based information. Researchers have even demonstrated how RFID tags woven into clothing or bedding could serve as patient health monitors in medical facilities.

Since recent years, NFC technology has become increasingly prevalent in our daily lives, particularly in the form of mobile payment systems and access control systems. However, as with any wireless technology, NFC is vulnerable to a range of security and privacy threats that can have serious consequences for users[2].

One of the key security threats facing NFC is eavesdropping. While eavesdropping on an NFC transaction is more difficult than with other wireless technologies due to the limited communication range between devices, it is not impossible. Attackers can potentially intercept and read the data being transmitted between devices, compromising the security of the transaction.

In addition to eavesdropping, other security threats include data modification and corruption, as well as attacks on the sequential devices in an NFC transaction. For example, in the case of smart posters, an attacker may use a malicious website to direct users to download malicious software onto their devices. This software can then be used to eavesdrop on the user's keystrokes or attempt to access sensitive information stored on the device, compromising the security of other applications.

To mitigate these security threats, encryption is often used to secure NFC communications. However, the choice of encryption method can have a significant impact on the performance of the device. Symmetric encryption, for example, requires the distribution and management of keys, while asymmetric encryption can increase transaction time and battery usage, particularly on low-powered devices. Advanced encryption techniques such as ECC can help address these issues, but the appropriate encryption method will depend on the specific use case.

While NFC technology can certainly make our lives easier and more convenient, it also raises significant privacy concerns. For example, the use of NFC tags can allow attackers to track users' movements and actions, potentially compromising their privacy. Additionally, malware on a device can collect sensitive information, such as login credentials or credit card numbers, and send it back to the attacker without the user's knowledge.

In conclusion, while NFC technology has the potential to revolutionize the way we interact with the world around us, it is not yet mature and has significant security and privacy issues that need to be addressed. While it may be suitable for entertainment purposes, for business use, it may not be suitable due to its security and privacy issues. It is important for users and developers alike to be aware of these issues and take steps to mitigate them, such as using appropriate encryption methods and keeping devices up-to-date with the latest security patches.

NFC technology payment gateways would provide a detailed analysis of the existing research and literature on the subject. The survey would begin by providing an overview of NFC technology payment gateways, including how they work, their components, and the payment process involved [3]. It would then explore the benefits and limitations of using NFC payment gateways for transactions, including a discussion of the convenience, speed, security, and efficiency of NFC payment gateways, as well as the challenges associated with their adoption, such as technical issues, user adoption challenges, and security concerns.

The survey would also delve into the technology behind NFC payment gateways, including how they use radio frequency identification (RFID) technology to facilitate transactions. This section may also discuss the technical requirements for using NFC payment gateways, including the necessary hardware and software. The survey would also provide an analysis of the current state of adoption of NFC payment gateways around the world and in different industries, including statistics on the number of NFC-enabled devices and the percentage of transactions being conducted using NFC payment gateways.

In addition, the literature survey would compare NFC payment gateways with other payment methods, such as traditional payment methods like credit cards and cash, as well as other mobile payment technologies like mobile wallets and QR code payments. The survey would also explore potential future developments and challenges in the NFC payment gateway space, including emerging trends in technology, changing consumer behavior, and regulatory considerations. Overall, the literature survey would provide readers with a comprehensive and detailed understanding of NFC technology payment gateways and their implications

III. PROPOSED WORK

A. Hardware Requirements

To build this project you will need the following :

- NFC Enabled Devices
- NFC Tags
- Bank Cards

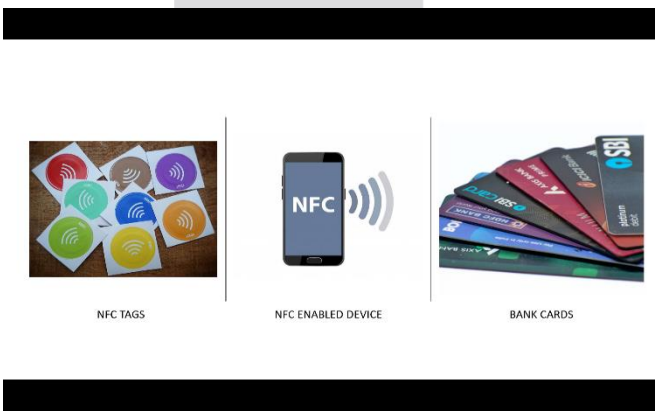

Fig.1. Hardware components

B. Software Components

To complete this project, you will need the following software and documentation.

- Flutter
- MySQL
- PHP
- PostMan

The working of project can be broken down into the following modules:

A. Flutter:

Flutter app front-end involves several key steps that must be completed in order to produce a fully-functional, polished app. The first step is to set up the development environment, which involves installing Flutter and an integrated development environment (IDE) such as Android Studio or Visual Studio Code, and connecting an emulator or physical device for testing. Once the development environment is set up, the app's user interface can be designed using Flutter widgets, which can be customized to reflect the app's branding, color scheme, and typography. After designing the user interface, the app logic must be implemented using the Dart programming language. This involves handling user input, managing app state, and connecting to APIs, which can be integrated using Flutter packages. In order to make the app more interactive and engaging, animations and effects can be added using Flutter's built-in tools, such as fade-in and fade-out animations, sliding transitions, and ripple effects. Once the app has been designed and implemented, it must be tested and debugged using the emulator or physical device. Flutter's debugging tools, such as the Dart DevTools and Flutter Inspector, can be used to identify and fix bugs. Once the app is fully functional and polished, it can be published using Flutter's publishing tools, such as the Flutter CLI and Google Play Console, to the Google Play Store or the App Store. Overall, creating a Flutter app front-end involves several key steps that must be executed with precision in order to produce a high-quality app. From setting up the development environment to designing the user interface, implementing the app logic, and testing and debugging the app, each step is critical to the app's success.

B. PHP:

PHP (short for Hypertext PreProcessor) is the most widely used open source and general purpose server side scripting language used mainly in web development to create dynamic websites and applications PHP can actually do anything related to server-side scripting or more popularly known as the backend of a website. For example, PHP can receive data from forms, generate dynamic page content, can work with databases, create sessions, send and receive cookies, send emails etc. There are also many hash functions available in PHP to encrypt user's data that makes PHP secure and reliable to be used as a server-side scripting language.

C. MySQL:

MySQL is a Relational Database Management System (RDBMS) MySQL has turned out to be one of the most popular open-source databases used by organizations for web development. It is the central component of LAMP, which is a software stack model that facilitates building web applications and websites. It offers one of the most secured databases in the world and is hence used by well-established web applications like Facebook, Twitter, Instagram, etc. Its various security features like Firewall, Encryption and User Authentication are the helping hands in protecting sensitive user information from intruders.

D. NFC :

Near Field Communication (NFC) technology allows users to make secure transactions, exchange digital content, and connect electronic devices with a touch. NFC transmissions are short range (from a touch to a few centimetres) and require the devices to be in close proximity.NFC is the technology in contactless cards, and the most common use of NFC technology in your smartphone. NFC is an upgrade of the existing proximity card standard (RFID) that combines the interface of a smartcard and a reader into a single device. It allows users to seamlessly share content between digital devices, pay bills wirelessly.

V. RESULTS AND CONCLUSION

NFC technology has significant advantages for payment, including convenience and security. However, challenges such as infrastructure and interoperability must be addressed for widespread adoption. Despite these challenges, the future of NFC for payment looks bright, with potential developments including integration with biometric authentication and blockchain. The convenience and security provided by NFC technology for payment have made it increasingly popular in the digital payment landscape. However, the need for infrastructure and interoperability remain significant barriers to widespread adoption. Businesses and merchants will need to invest in NFC-enabled point-of-sale terminals, and the competing standards for NFC payments can create confusion for consumers and businesses alike.

Looking ahead, the integration of NFC payments with other emerging technologies, such as biometric authentication and blockchain, could further enhance the convenience and security of NFC transactions. This could also help to address some of the

challenges facing NFC for payment, such as interoperability.In conclusion, while there are challenges to be addressed, the future of NFC technology for payment looks promising. As the technology continues to evolve, NFC payments could become even more convenient and secure, offering significant benefits for consumers and businesses alike.

REFERENCES

1. Smart Tags Add Touch Controls to Ordinary Objects By using reflected Wi-Fi signals, a chipless smart tag can put touch-responsive controls on almost anything.
2. Near Field Communication (NFC) Hussain ahamed IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012
3. An Analysis of Security and Privacy Issues in NFC-Enabled Mobile Payment Systems" by M. Z. A. Bhuiyan, S. A. S. Mamun, and A. Hossain. This paper was published in the International Journal of Computer Applications in 2014.
4. "A Secure Mobile Payment System with NFC Technology" by Y. Huang, Z. Li, and Q. Sun. This paper was published in the Journal of Networks in 2012.
5. "Towards a Mobile Payment Gateway for NFC Devices" by R. Plötz and M. Schäferling. This paper was published in the Proceedings of the 3rd International Conference on Mobile Wireless Middleware, Operating Systems, and Applications in 2010.
6. A.P. Felt et al., “A Survey of Mobile Malware in the Wild,” Proc. 1st Workshop Security and Privacy in Smartphones and Mobile Devices (SPSM 11), 2011, pp. 3–14.
7. Z.Kfir and A. Wool, “Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard,” Proc. 1st Int’l Conf. Security and Privacy for Emerging Areas in Communications Networks (SECURECOM 05), 2005, pp. 47–58.
8. R. Silberschneider, T. Korak, and M. Hutter, “Access without Permission: A Practical RFID Relay Attack,” Proc. 21st Austrian Workshop Microelectronics (Austrochip 13), vol. 10, 2013, pp. 59–64.
9. M. Roland, J. Langer, and J. Scharinger, “Applying Relay Attacks to Google Wallet,” Proc. 5th Int’l Workshop Near Field Communication, 2013, pp. 1–6.
10. M. Roland and J. Langer, “Comparison of the Usability and Security of NFC’s Different Operating Modes in Mobile Devices,” Elektrotechnik und Informationstechnik, vol. 130, no. 7, 2013, pp. 201–206.
11. Vasudevan et al., “Trustworthy Execution on Mobile Devices: What Security Properties Can My Mobile Platform Give Me?” Trust and Trustworthy Computing, Springer, 2012, pp. 159–178.