Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 1): pp. 7678-7686
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.791

One Card For Every Payment And Identification Purpose Using Near-Field Communication (Nfc) Technology

Ashutosh Dixit Department of Electrical Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002 ashutoshdixit@geu.ac.in

Sandeep Sunori Department of Electronics & Communication Engineering, Graphic Era Hill University, Bhimtal, Uttarakhand India, 263156
sandeepsunori@gmail.com

ABSTRACT

One's quality of life is significantly impacted by advancements in payment technologies. Future opportunities and difficulties are brought about by emerging payment systems. With throughput as its primary metric, contactless payment has gained popularity, especially with suppliers. However, because there is no reliable form of consumer verification, it does present dangers for issuers. In order to remove obstacles to business, it has been decided to create and maintain a well-managed, efficient, trustworthy, and secure unified payment system. a system and module for connecting two cards together Using near-field communication (NFC) technology, funds can be transferred digitally from one bank to another. With this method, all forms of payment and identification are satisfied without the need for actual cash.

1. INTRODUCTION

Digital moneyless payments have grown commonplace despite the fact that the digital payment system has been in use since the 1960s thanks to technological development and the advent of e-commerce. Many online payment methods, like the JW and N models, have gained popularity. In the context of the Internet of Things, research is being done on an intelligent warehouse management system based on NFC. Real-time intelligent logistics management is possible with this system[1]. The Asokan model came into being. E-commerce expansion and cashless payments online have become commonplace. Many online payment methods, like the JW and N models, have gained popularity.The Asokan model was created. The model, which also stipulates that if neither party is engaged in any transaction, the bank and any buyer or seller must end the transaction, was implemented in 1998. When data technology develops, organisations function better as well, which leads to positive developments and organisational progress. One of the technologies that can be employed and applied in a business is NFC [2]. Based on the model, the "third kind" includes electronic checks, cash, and currency equivalents in addition to credit card payment applications. However, the most widely utilised electronic payment method is credit cards. To accomplish this goal, numerous potential solutions have

been created, including.

2. ENERGY STORAGE UNITS

Direct energy storage and indirect energy storage are the two categories under which energy storage systems fall.

1. Limited categories (10MW): flywheel batteries and ultra-capacitors are available in small categories when used in conjunction with DG devices.

2. Medium categories (10MW to 100MW energy): These categories include lead acid, NAS, large-scale batteries, and redox.

3. Compressed Air Energy Storage (CAES) and Pumped Storage are accessible in large categories (around 100MW).

Equation provides storage device efficiency. The applications for energy storage are shown in the table along with some relevant information about their discharging times and storage capacities.

However, in 1997, just 37% of Americans used Speedpass to pay petrol prices at American gas stations. NFC-based credit cards were originally introduced by Barclaycard in the UK in 2007.NFC is the replacement for RFID, which operates at a frequency of 13.56 MHz and communicates across extremely small distances.[4] NFC is not supported by another method, magnetic secure transfer, which gives the consumer the option of using the computer on the POS terminal instead. The introduction of Android Pay occurred in October 2015. By 2025, it's expected that mobile payments will account for 65% of all retail purchases.

3. BY THE NUMBERS

Despite the significant advancements in payment technologies, customer adoption is still lacking. The market is home to a variety of elements that have contributed to the market's strong adoption of mobile wallets. According to a survey, 62 percent of respondents are aware of machine security. Another survey on consumer digital payments from 2015 revealed that 59% of people accept debit cards and 50% of people do not use credit cards, with 16% of current systems favouring digital payments while 67% of people still pay cash.Developed in recent years, near-field communication is a revolutionary low-cost wireless communication technology that greatly simplifies daily tasks including commerce, healthcare, and food quality monitoring [3].

The fact that all mobile payment options require expensive, high-end devices appears to be the major problem. many significant technological advancements, thank you.It is evident that while creating a unified payment system, reliability, robustness, usability, and affordability should be the main priorities [10]. This article introduces the revolutionary Swing-Pay digital card module and examines some of the drawbacks of the existing electronic payment system.

4. ELECTRONIC PAYMENTS:

Multiple potential solutions are offered by digital payment networks. Either they only accept POS payments or they rely heavily on smartphones. In comparison to other options, we needed a single payment system that would support all payment methods, including POS and P2P, and be comparatively safe and affordable.

The device should be portable so that users can use it to make payments at any time, anywhere, and to anyone. The performance of the piezoelectric force sensor, which is affixed to a skin-like surface, is at sensitivities of 1.775, 6.358, and 8.117 V/N, respectively, under applied frequencies of 0.5, 2 and 5 Hz. The sensor can faithfully reflect arterial pulse responses during practical monitoring [5]. People must be able to tender the exact amount with the device (Swing-Pay) so they are not concerned about the scarcity of small de-nominations.High-level cryptography can be used to protect contactless payment using an inert identification. While beginning data transmission by touching is a simple and intuitive process, tapping devices unintentionally can result in issues.

The creators have also suggested using NFC to collect community data. When Google implemented NFC on the Nexus-S system in 2011, enhanced versions of the technology were also investigated. A mobile application created by Stanford's Mobi-Social Lab makes use of the P2P capabilities of the Nexus-S. The server responds to the client's request and processes it. In order to enable developers to create P2P apps, Google released it open source. Improved SNEP protocol to device Protocol OPEN-NPP.

Researchers have looked into using the new GSM network to confirm mobile payments based on the NFC in order to make mobile payments secure. A framework was developed to enable financial transactions to be completed at any POS while being approved by a dependable service manager. Fig 1 shows the Basic Elements of Payments Processing System The biometric information is stored in the second secure item (SE) of the device, which also assesses the biometric characteristic at the time of the action and generates transaction information if the validation is successful. This invention only applies to POS transactions, and the user's smartphone needs to have a fingerprint sensor.

5. MODULES DESCRIPTION

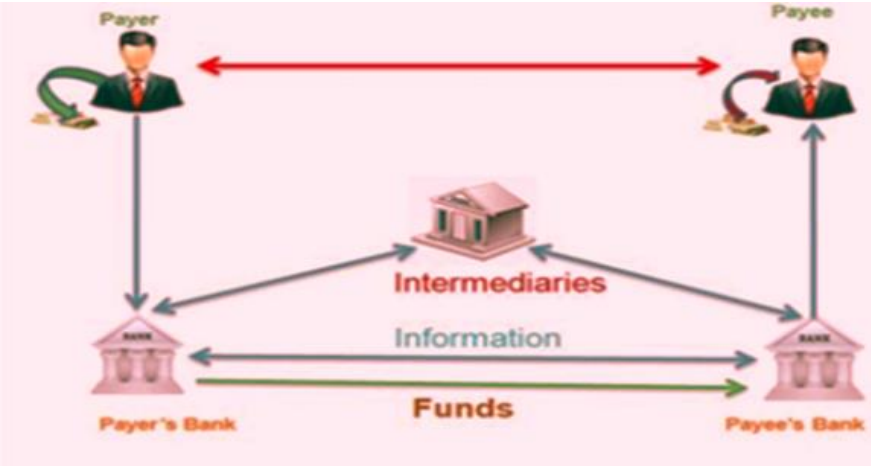

Fig 1: Basic Elements of Payments Processing System

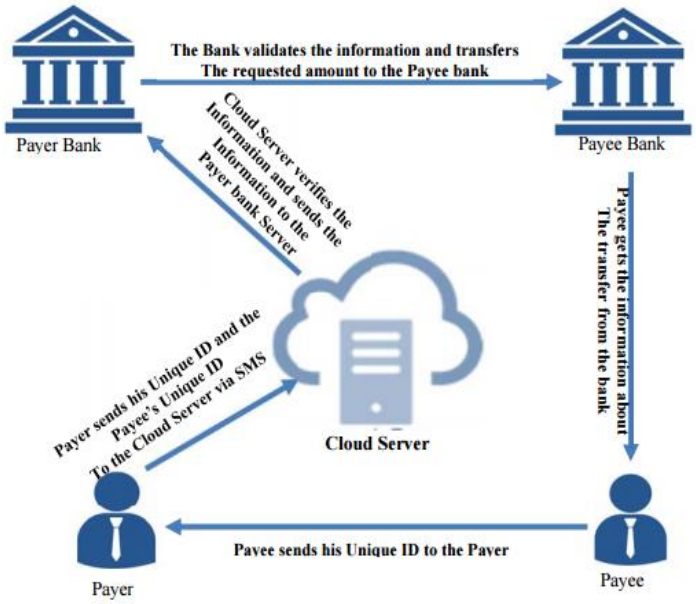

Fig2: Swing-Pay -One Card for all P2P Payments Using Biometric Authentication

An Arduino Due board was equipped with 512 kB of static random access memory (SRAM) and Peripheralinterface (SPI) capability.

Fig 2 shows the Swing-Pay -One Card for all P2P Payments Using Biometric Authentication.This module consists of the FPC2020 processor and the FPC1011F3 area sensor. For metal-oxide semiconductors, the FPC1011F3 complementary fingerprint sensor captures images with 256 grayscale values per pixel. Additionally, the fingerprint information is saved for eventual authentication on an external flash drive.On the phone even after turning off the power. To flip the economy, all you need is power. Millions of incredibly tiny

microcapsules floating in a stream make up the e-Ink monitor. Both negatively and positively charged black and white particles are present in the micro-capsules.

No library for supporting the Arduino Due platform was available. Adafruit offers libraries that will only build on Arduino, Raspberry Pi, and MSP430 AVR-based boards. Additionally, as printing dynamic images and messages requires more SRAM capacity, 2.7-in displays on Arduino boards based on AVR can only display static images.

Due of its wide adoption and short range frequencies, IoT technology like Near Field Communication (NFC) makes a viable choice for token-based security access management [6]. The fringing capacitance principle underlies how capacitive buttons function. As a person approaches the sensor and grounds it, the capacitive plate's fringing electric fields fade toward the earth. The use of NFC technology in a university setting needs to be looked into because present NFC-based educational applications fall short of their full potential [7]. As the hand approaches the sensor, the capacitance increases nonlinearly as a result of fringing effects.

6. P2P –SWINGPAY MONEY TRANSFER

The hardware of the module, the cloud server, and the bank are the three jobs that The Swing Pay occupies on the system. The user will need to create a customised account on the cloud server when purchasing the module for the first time, and at that time, he will be issued a special server ID. All user information, including account number,routing number, and bank name, will be stored in an encrypted file in a registered account. Instead of using GPRS, it is feasible to interact with the cloud server via SMS, which uses less power overall. The P2P capabilities of the NFC can be used to establish communication between two modules. Utilizing SNEP and LLCP protocols, Android mobile

Figure 4 shows the proposed method. The fingerprint card is unlocked by the payee. The card will switch on after the fingerprint has been verified. NFC P2P mode is used to transmit the payee's special ID. If the payer hadn't figured out the payee's distinct identity and indicated the amount to be submitted using the capacitive keyboard, the transaction were delayed. The payer must use their fingerprint to confirm themselves once more after choosing the number. The transaction will be cancelled after a number of trials if the authentication is unsuccessful. If the payer authenticates themselves properly, in all other cases the device will send an SMS. A "Successful Transaction" notification appears on the phone after the SMS is sent successfully. Industry utilises specialised servers as SMS gateways to manage SMS which is shown in fig 3. In the business world, dedicated servers are employed as SMS gateways to manage SMS commands and place calls to web services in accordance with the orders. They are extremely powerful servers with many peripherals.

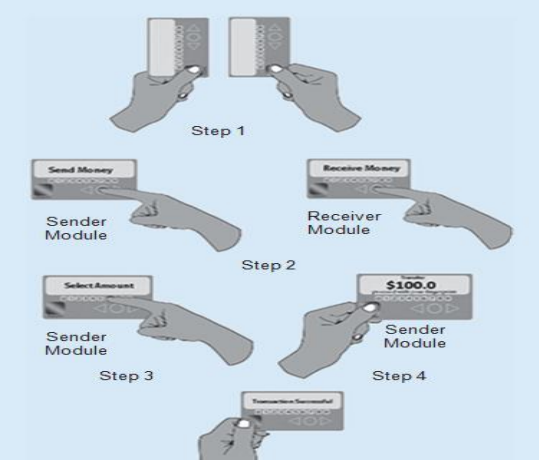

Fig 3: A digital card component for peer-to-peer payments that uses NFC and biometric authentication

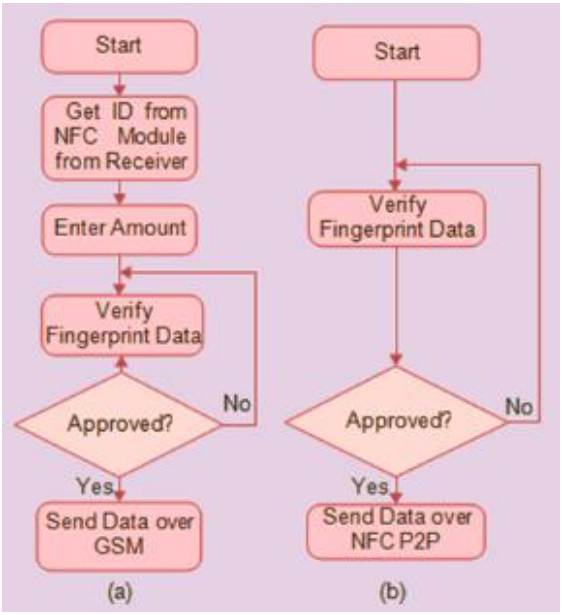

Figure 4 proposed method

6.1. Utilizing Swing-Pay For Additional Services

Several forms of identification, include a driver's licence and a voter ID card. However, because each of these solutions must be performed by hand, there is always a chance that they could be misplaced, and finding new ones takes a more time and work. Swing-Pay uses the virtualization of ID cards as a solution to this problem. The cloud repository maintains the scanned photos of each ID card along with the user's unique ID at the time of registration. The photos are also kept in X-Bitmap format in the module. The unit uses NFC P2P or NFC Beam to transmit a web service call with the user's unique ID and specified parameters for gaining access to any particular online service.ncluding Near Field Communication (NFC) in the

present Virtual Learning Environment (VLE) framework. The ubiquitous learning environment is made possible by (NFC) technology [10].

To serve as a reader, we're running NFC mobile Android. An NFC adaptor and a web view have been developed into a single programme. Using the built-in Android purpose framework, the NFC adapter launches the application and controls the module message transmitted over NFC Beam. Nevertheless, more investigation indicates additional areas where NFC has a substantial impact. There is optimism that recent developments in NFC-based ticketing and medical applications may act as the so-called "Catalyst" for NFC integration [8]. The web view calls the web service to show the ID's details when the programme is first run. The module then sends the information directly to the user. The reader calls, reacts to the post, and gives the web service the information.

7. PROTYPING

The FPC1011F3 area sensor and the FPC2020 ASIC processor are the two parts that make up the FPC-AM3 fingerprint sensor. The FPC1011F3 can virtually scan every fingerprint, dry or wet. SPI is used for communication with Arduino. Adafruit FONA, a quad-band antenna with frequencies of 850/900/1800/1900MHz, is the GSM module. Both GPRS and SMS messages can be received by it. The module also features a circuit for USB recharging of the associated battery. A GSM-style 3-dBi sticker antenna, and an uFL connector were employed.

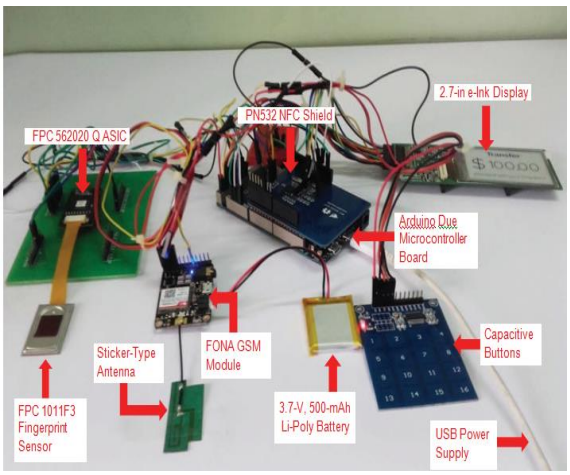

Fig 5: Complete prototype with different components

The Swing-Pay prototype has a 2.7-in RePaper e-Ink panel. It connects to Arduino via the SPI protocol and has an active TFT matrix with a resolution of 264 by 176. Due to its bi-stability, it requires extremely minimal power to refresh the screen. A dedicated temperature sensor and an 8 Mb serial flash memory interface card are included with the e-Ink monitor. TTP229 connects to the host controller using the I2C protocol [9]. Eight pins might alternatively be

interfaced straight from the TTP229 board. The Arduino provides input to the entire module. An Arduino PC manages the board. The proposed module evaluated the built-in Android app as a potential reader for the identity virtualization of the card module, and it was successful. When used in ID card mode, the module works correctly was shown in fig 5.

8. CONCLUSION

There has been discussion of a full digital card prototype that can be used for any identity or payment requirement. A capacitive fingerprint sensor is utilised to strengthen card security. The public library of the e-Ink display has been transferred directly to the Arduino Due, and it runs the e-paper display. In addition to the FONA GSM phone, the TTP229 channel capacitive button phone is interfaced. The module sends a GSM SMS to the cloud with precise information about the payment, payer, and transfer amount when fingerprint authentication is successful. We also created an Android application to receive the SMS and deliver the data to the cloud component for the transaction. To accept web service requests and view the data the server has received, a second programme is developed in ID virtualization mode. For the purpose of obtaining the client's data and completing the transaction, an appropriate web API was created. SHA and MD5 are the appropriate encryption algorithms used to save all the data on a server.

REFERENCES

1. Ye, L., Wang, Y., & Chen, J. (2016). Research on the intelligent warehouse management system based on near field communication (NFC) technology. International Journal of Advanced Pervasive and Ubiquitous Computing (IJAPUC), 8(2), 38-55.
2. Museli, A. and Navimipour, N.J., 2018. A model for examining the factors impacting the near field communication technology adoption in the organizations. Kybernetes.
3. Cao, Zhonglin, Ping Chen, Zhong Ma, Sheng Li, Xingxun Gao, Rui-xin Wu, Lijia Pan, and Yi Shi. "Near-field communication sensors." Sensors 19, no. 18 (2019): 3947.
4. Singh, Manmeet Mahinderjit, K. A. A. K. Adzman, and Rohail Hassan. "Near Field Communication (NFC) technology security vulnerabilities and countermeasures." International Journal of Engineering & Technology 7, no. 4.31 (2018): 298-305.
5. Yi, Zhiran, Jiajie Huang, Zhaoxu Liu, Jingquan Liu, and Bin Yang. "Portable, wireless wearable piezoelectric arterial pulse monitoring system based on near-field communication approach." IEEE Electron Device Letters 41, no. 1 (2019): 183-186.
6. Singh, M. M., Adzman, K. A. A. K., & Hassan, R. (2018). Near Field Communication (NFC) technology security vulnerabilities and countermeasures. International Journal of Engineering & Technology, 7(4.31), 298-305.

7. Abood, M.S., Ismail, M. and Nordin, R., 2016, November. A quiz management system based on P2P near-field communication on Android platform for smart class environments. In 2016 international conference on advances in electrical, electronic and systems engineering (ICAEES) (pp. 83-88). IEEE.
8. Page, Tom. "Technological diffusion of near field communication (NFC)." International Journal of Technology Diffusion (IJTD) 7, no. 3 (2016): 59-75.
9. Giese, D., Liu, K., Sun, M., Syed, T., & Zhang, L. (2019). Security analysis of near-field communication (NFC) payments. arXiv preprint arXiv:1904.10623.
10. Osman, H.M., Singh, M.M., Plasencia, M.S., Shariff, A.R.M. and Bakar, A.A., 2018. Enhanced analytical hierarchy process for U-Learning with Near Field Communication (NFC) technology. International Journal of Advanced Computer Science and Applications, 9(12).