International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 3, May-June-2018, ISSN (Online): 2395-566X

An NFC Featured ATM Cards with Biometric for Secure Transactions

Asst.Prof.Mrs.Vandana
Dept. of CSE, MVJCE computer Science and engineering
Bangalore, India

M. Tech. Scholar Ms.Swetha Y
Dept. of CSE, MVJCE computer Science and engineering
Bangalore, India
swethayreddy06@gmail.com

***Abstract* – With the payment cards such as Debit and Credit cards usage becoming more common and rapid so are the number of ways to exploit the vulnerabilities associated with them and have become common target for cyber criminals. Moreover, the customer goes through the experience of a laborious process of interacting with the customer care center and to do the necessary errands thus increasing the turnaround time to achieve the end goal that is, to get the payment card blocked or to get a replacement card. This document comprising of a Near Field Communication (NFC) device that can be used as a potential solution to overcome the transaction liabilities (brute force attack, shoulder surfing, skimming of ATM cards etc.) involved in using the payment cards. An additional feature involving blocking/deactivating ATM cards is achieved using QR code technology for authentication scheme.**

***Keyword*- Debit and credit cards, ATM cards, QR code, NFC.**

I. INTRODUCTION

The greater part of Society will convey credit and platinum cards in our wallet. The versatile utilization of credit and platinum card exchanges has expanded and further more they have been related with vulnerabilities that make them a run of the mill center for computerized guilty parties/digital lawbreakers. Regularly and genuinely expanded burglary in advanced business is taking and skimming of ATM cards.

In 2008 in excess of 1billion ATM related wrongdoings have been enrolled. A few criminals will take after old mold to split them however there is innovative type of burglary and focusing on it is called skimming. Criminals utilize concealed gadgets like skimmer to take individual card data and they will likewise record the PIN details to gain admittance to the record.

Skimming can occur in two stages initial segment is skimmer itself a concealed card peruse is set over ATM card space in the event that people swipe their card into ATM .Unconsciously swiping it through the shrouded card peruser which will outputs and stores all the card data that is put away on attractive strip. In any case on the off chance that they need to increase full access to the record still they require PIN that is the place concealed cameras comes. Some ATM skimmers will likewise utilize counterfeit keypads to catch PIN.

In Recent years ATM cards are using RFID (Radio frequency technology) to overcome form skimming problem. Even though skimming problems are not reduced RFID skimming can occur. RFID skimmers use electromagnetic field to read the card information that is stored in RFID tags or labels. In RFID ATM card, we use RFID tags or labels to store account information like card holder name, account number etc., RFID technology have a range up to 37 feet so the attacker can place RFID reader in that range and can read all the card information that is how the RFID skimming can happen.

So in order to overcome from all these security issues a new technology called NFC (Near field communication) has been introduced that will provide more security during transactions.

And also ATM card blocking is also long process and we have wait for longer time to block the card so to overcome from that traditional method of ATM card blocking a QR code method have been introduced by using that user can block their ATM by going to the nearest ATM machine.

II. RELATED WORK

In Izabela Lacmanovic [1] Proposed a contactless installment frameworks that don't require physical contact amongst client and end gadgets. It will utilize Radio recurrence distinguishing proof (RFID) innovations which have a range up to 40 feet. They utilized a RFID tag and RFID chip it comprise of IC.

It will use a radio waves to achieve correspondence amongst client and end gadget as RFID innovation have extend up to 40 feet RFID skimming and taking of ATM

card can be a digital crime. Cyber Criminal can put RFID peruse in that range and can take all the card data. So despite the fact of RFID innovation, have disadvantages of RFID skimming.
In Devashish Kumar [2] Proposed a technique to productively enhance the Security of OTP. On the off chance that we utilize web based keeping money and web for our monetary issues it will disentangles our lives. Web based keeping money is in various areas like wellbeing, monetary, instructive and shopping and so forth.. in the meantime digital lawbreakers will take the benefits of the escape clauses which are in our frameworks and can assault and get every one of our points of interest effortlessly.

The cybercriminals can make utilization of these escape clauses and complete exchange which will not come in the information of client and the bank. Late examinations have demonstrated that the OTP which was produced as a piece of two factor validation is helpless against assaults. In this paper, we display another system for upgrading validation amid online exchange which secures our OTP.

Despite the fact that OTP is utilized for secure exchanges OTP have less time traverse like 2 to 5mins after that it will wind up invalid and furthermore OTP may defer recently so that at that point OTP arrive our strength have shut and furthermore as OTP is send through SMS ,have less security.

In Chris Karlof [3] portray another assault against web verification which is called Dynamic Pharming. Dynamic Pharming works by capturing DNS and will send a pernicious java script which at that point abuses DNS rebinding vulnerabilities and the name-based same origin approach to commandeer a true blue session after validation has occurred. Therefore, the assault works paying little heed to the confirmation plot utilized. Dynamic pharming empowers the foe to spy on touchy substance, produce exchanges, sniff auxiliary passwords, and so on. To counter unique pharming assaults, we propose two bolted same-starting point strategies for web programs.

In Yong-Gon Kim [4] proposed Smart Phones which are greatly extending in late versatile market mobiles. They are furnished with numerous highlights like camera that will makes a computerized substance.

For example, photographs recordings and camera assumes a part for media transmission. For example, video calls and scanner tag information. QR code acknowledgment is also Captured in the camera. It will contain an assortment of data like two dimensional standardized identification and make it conceivable of getting information.

This paper breaks down the technique for QR-code acknowledgment and validation distinctive sorts of information can be covered up in QR code that in the event that we examine by utilizing QR scanner that will read the information in that code. Conventional ATM card blocking is a major procedure we need to sit tight for long time so a QR code ATM card blocking strategy is utilized.

In Mayada Al-Tamimi [5] proposed a security convention for NFC communication. NFC is a short range correspondence framework that will trade information between gadgets with in short range. As installment exchanges utilizing NFC innovation has been expanded. Not with standing, a far reaching of NFC-based installment can be ensured, the installment exchanges are made in a secured remote condition.

Tragically, the Euro pay, MasterCard and Visa (EMV) convention, which is as of now used to give the required security, has some genuine vulnerabilities which could prompt clear dangers for clients of NFC-based installments.

This paper exhibits a compelling answer for upgrade the security of NFC installments by fathoming the vulnerabilities of the EMV convention. The proposed convention adds a security layer to the EMV convention keeping in mind the end goal to guarantee privacy of the transmitted savings money information and to give common verification between the diverse on-screen characters of the NFC installment exchanges.

In Zubayr Khalid [6] proposed Dynamic Password (Dyna-pass) techniques to offer security to ATM transactions. In their system, user access the ATM with a debit card and his or her PIN as in the traditional system, but an SMS that contain a secret code called Dyna-pass is sent to the user mobile phone from the bank server if the PIN giving by the user is correct. The user then enters this new code received on his or her phone for confirmation, this again is checked with the bank server for confirmation, and if correct ATM transaction access is given to the user.

III.SYSTEM DESIGN

This document gives the design of the overall project. Software development is the phase which is very important for the supernova of the software, which is called as design phase.

The design phase should satisfy the functional and non-functional requirements for the effectiveness for satisfying all the constraints and objectives of the project. It mainly concentrates on the modules that needed for system. The design phase depends mainly on the specification of feasibility survey.

1. System Architecture

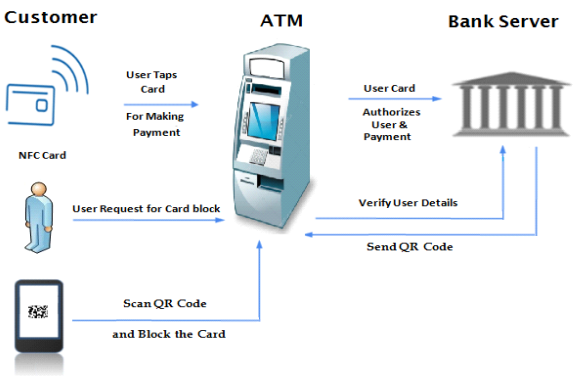

Fig: 1. System Architecture

System involves 3 Steps as follows:

1.1 NFC Registration: User should register their personal information in NFC card before doing transactions. Here the NFC cards used are of type MIFARE cards. MIFARE cards are series of chips that are widely used in contract less smart cards. These chips typically have read/write distance of 4 Cms.

There are 4 Types of MIFARE cards.

1.1.1 MIFARE ultra

It has just 512 bytes of memory with no security. The memory is given in 16 pages and 4 bytes they are so modest so they are frequently utilized as a part of expendable tickets they additionally have compose bolt highlight that keep from re-composing information. It additionally has OTP (one time programmable) bits.

1.1.2 MIFARE great

The MIFARE exemplary cards are only a memory stockpiling gadget, where the memory is partitioned in areas and pieces. They are dependable and minimal effort. They are generally utilized as a part of electronic wallets. The MIFARE Classic 1K card has 1024 bytes separated into 16 divisions and every part is ensured by two unique kinds of keys called KEY An and KEY B.MIFARE plus

1.1.3 MIFARE plus

Brings benchmark AES security to contactless savvy card applications. It offers the advantage of a consistent update of existing MIFARE Classic establishments and administrations with least exertion. This outcome in the likelihood to issue cards, being completely perfect with MIFARE Classic, into existing framework conditions preceding foundation security overhauls.

1.1.4 MIFARE DES Fire

The MIFARE DESFire item family comprises of MIFARE DESFire EV1 and MIFARE DESFire EV2 items and is in a perfect world suited for arrangement designers and framework administrators building solid, interoperable and adaptable contactless savvy card arrangements. It targets multi-application savvy card arrangements in personality get to control, and faithfulness and micropayment applications and in addition in transport plans.

1.2 Secure ATM transactions: First client needs to tap card to make exchanges or for making any installments after that the ATM machine will check client and client card if it's a substantial client gets verified and will allow us to make exchanges as NFC innovation has been utilized as a part of ATM , it will give more security than RFID and attractive cards.

1.3 Block lost ATM cards: An ATM card blocking capacity is made accessible on ATM home screen. At the point when a card is lost client needs to pick ATM square choice ATM screen and enter card subtle elements on the approval of the client a snappy response(QR) code is created on ATM screen. The QR code is checked on mobile phone and a URL is created after opening it in the versatile program, an affirmation page is asked for to the client. On client affirmation, a win screen is shown. All the while, the hint of this demand to obstruct the card is sent to the bank server

2. Working of NFC

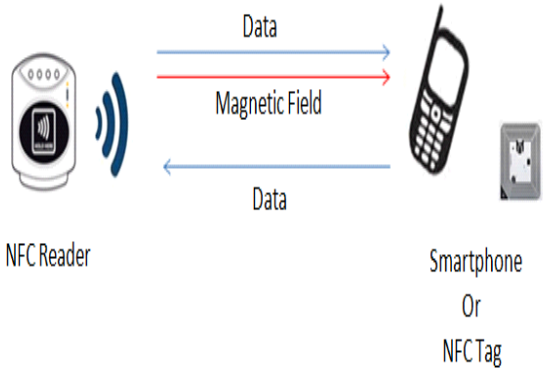

Fig.2. working of NFC

NFC remains for "Close Field Communication" and, as the name suggests, it empowers short range correspondence between good gadgets. This requires no less than one transmitting gadget, and another to get the flag. A scope of gadgets can utilize the NFC standard and will be thought about either uninvolved or dynamic.

Latent NFC gadgets incorporate labels, and other little transmitters, that can send data to other NFC gadgets without the requirement for their very own power wellspring. In any case, they don't generally process any data sent from different sources, and can't interface with other detached parts.

These frequently appear as intuitive signs on dividers or advertisements Dynamic gadgets can both send and get

information, and can speak with each different and additionally with uninvolved gadgets. Cell phones are by a wide margin the most well-known type of dynamic NFC gadget. Open transport card peruses and touch installment terminals are likewise great cases of the innovation.

Since we know what NFC works same as Bluetooth and WiFi, and all way of different remote signs, NFC takes a shot at the standard of sending data over radio waves. Close Field Communication is another standard for remote information advances. This implies gadgets must hold fast to specific determinations keeping in mind the end goal to speak with each other appropriately. The innovation utilized as a part of NFC depends on more established RFID (Radio-recurrence distinguishing proof) thoughts, which utilized electromagnetic acceptance so as to transmit data.

This denotes the one noteworthy distinction amongst NFC and Bluetooth/Wi-Fi. The previous can be utilized to incite electric streams inside detached parts and in addition simply send information. This implies detached gadgets don't require their own particular power supply. They can rather be fueled by the electromagnetic field created by a dynamic NFC part when it comes into run. Tragically, NFC innovation does not summon enough inductance to charge our cell phones, but rather QI charging depends on a similar guideline.

The transmission recurrence for information crosswise over NFC is 13.56 megahertz. You can send information at either 106, 212, or 424 kilobits for each second. That is sufficiently speedy for a scope of information exchanges from contact points of interest to swapping pictures and music.

To figure out what kind of data will be traded between gadgets, the NFC standard as of now has three particular methods of task. Maybe the most well-known use in cell phones is the shared mode. This permits two NFC-empowered gadgets to trade different snippets of data between each other. In this mode the two gadgets switch between dynamic when sending information and latent while getting.

Read/compose mode, then again, is a restricted information transmission. The dynamic gadget, potentially your cell phone, connects up with another gadget so as to peruse data from it. NFC advert labels utilize this mode. The last method of activity is card imitating. The NFC gadget can work as a brilliant or contactless charge card and make installments or take advantage of open transport frameworks.

3. Implementation

Implementation is a process of preliminary arrangement of application or the execution of plan which may lead to the successful outcome of the project. The usage of system must require the technologies involved for the context of module to operate, the idea behind the planning, performing the algorithms as a programming execution and the software and hardware requirements specification of computer system using the successful deployment of installations, configurations, running of project, execution of project. And mainly testing will enhance the design of project. The implementation is the realization of application, algorithms and the software components of the system should be deployed.

The implementation stage requires the following tasks.

- Careful arranging.
- Investigation of framework and imperatives.
- Design of techniques to accomplish the changeover.
- Evaluation of the changeover technique.
- Correct choices in regards to choice of the stage
- Appropriate determination of the dialect for application advancement.

VI. LANGUAGES USED FOR IMPLEMENTATION

Execution stage ought to flawlessly outline configuration record in a reasonable programming dialect with a specific end goal to accomplish the vital last and right item. Regularly the item contains imperfections and gets destroyed because of erroneous programming dialect decided for usage. In this venture, for execution reason Java is picked as the programming dialect. Hardly any Purposes behind which Java is chosen as a programming dialect can be plot as takes after:

1. **Platform Independence**: Java compilers don't create local protest code for a specific stage yet rather 'byte code' directions for the Java Virtual Machine (JVM). Influencing Java to code take a shot at a specific stage is then just an issue of composing a byte code translator to mimic a JVM. What this all methods is that the same incorporated byte code will run unmodified on any stage that backings Java.
2. **Objects Orientation:** Java is a pure object-oriented language. This means that everything in a Java program is an object and everything is descended from a root object class.
3. **Rich Standard Library:** One of Java's most appealing highlights is its standard library. The Java condition incorporates many classes and strategies in six noteworthy practical zones:-Language Support classes for advanced language features such as strings, arrays, threads, and exception handling.

- Utility classes like an irregular number generator, date and time capacities, and holder classes.
- Input/yield classes to peruse and compose information of numerous kinds to and from an assortment of sources.
- Networking classes to permit between PC correspondences over a nearby system or the Internet.

4. **Applet Interface:** Notwithstanding having the capacity to make remain solitary applications, Java designers can make programs that can download from a site page and keep running on a customer program.
5. **Familiar C++-like Syntax:** One of the components empowering the quick selection of Java is the closeness of the Java linguistic structure to that of the prominent C++ programming dialect.
6. **Garbage Collection**: Java does not expect developers to unequivocally free powerfully designated memory. This makes Java programs simpler to compose and less inclined to memory mistakes.
7. **Swing support:** Swing was created to give a more refined arrangement of GUI parts than the prior Abstract Window Toolkit. Swing gives a local look and feel that copies the look and feel of a few stages, and furthermore underpins a pluggable look and feel that enables applications to observe and feel inconsequential to the fundamental stage.

V. PLATFORM USED FOR IMPLEMENTATION

A stage is a pivotal component in programming improvement. A stage may be basically characterized as "a place to dispatch programming". In this venture, for usage reason Windows XP stage is utilized and purposes behind picking this stage are Integrated Networking support, More steady and secure than past variant, Contain remote work area association and reestablish choice, Enhanced gadget driver verifier, Dramatically lessened reboot situations, Improved code assurance, Side by side DLL bolster, Windows File Protection, Preemptive multitasking engineering, Scalable memory and processor bolster, Encrypting File System (EFS) with multiuser bolster, IP Security (IPSec), Kerberos bolster, Smart card bolster, Internet Explorer Addon Manager, Windows Firewall, Windows Security Center, Fresh visual outline.

VI.CONCLUSION

The proposed system uses near field communication technology for ATM cards. That can be used as a potential solution to overcome the transaction liabilities (brute force attack, shoulder surfing, skimming of ATM cards etc.) involved in using the payment cards. In this system an additional feature involving blocking/deactivating ATM cards in achieved using QR code technology for authentication scheme.

REFERENCES

[1]. Izabela Lacmanovic, Biljana Radulovic and Dejan Lacmanovic, “Contactless payment systems based on RFID technology” MIPRO, 2010 Proceedings of the 33rd International Convention.
[2]. Devashish Kumar, Amit Agrawal and Puneet Goyal“Efficiently improving the security of OTP”, Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances.
[3]. Chris Karlof, J.D. Tygar, David Wagner and Umesh Shankar “Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers.
[4]. Young-Gon Kim, Moon-Seog Jun “A Design of User Authentication System Using QR code Identifying Method” Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference.
[5]. Mayada Al-Tamimi, Ali Al-Haj “Online security protocol for NFC mobile payment applications” Information Technology (ICIT), 2017 8th International Conference