ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

# Secure Authentication of ATM Transactions Using NFC Technology and Fingerprint Technology

[1]Jayaraman G [2]Sneha K [3]Rosshima A E [4]Ritula S
[1]Assistant Professor-Electronics and Communication Engineering-Francis Xavier Engineering College-Tirunelveli-India-627003
[2-4]UG Scholar-Electronics and Communication Engineering-Francis Xavier Engineering College-Tirunelveli-India-627003

**Abstract**: Automated Teller Machine (ATM) is a convenient way to meet the banking needs of the users. However, the use of debit card or other types of cards during ATM transactions has some problems like prone to ATM skimming, magnetic strips of card getting damaged, manufacturing and transportation cost of cards, longer time to authenticate users etc. The objective of this research is to consider smart phone in Near-Field Communication (NFC) Card Emulation mode as an alternative to ATM cards. In NFC the distance between the respective devices needs to be very small (typically less than 4 cm) which makes NFC ideal for making payments and for other transactions involving sensitive/private data. In the proposed system, in order to authenticate at the ATM kiosk, the user needs to swipe his/her smart phone in front of the NFC reader. An ATM card is not required for authentication and the system will still have a stronger security compared to the system in which ATM card was used. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

**Keywords:** Secure Authentication, ATM, One Time Password, Near Field Communication, Security Attacks.

## I. INTRODUCTION

Automated Teller Machines (ATMs) play a vital role in providing the people easy access to cash and carry out other banking activities. Thus, it is of paramount importance to safeguard users and provide them convenience while transacting using ATM. Physical ATM cards along with Personal Identification Number (PIN) are in widespread use all around the globe to authenticate at ATM kiosks. However, there are some issues on the use of physical cards during ATM transactions. First, ATM skimming resulting to theft of card information and subsequently card cloning (even for chip based cards) has become a burning issue nowadays. Second the magnetic strip/chip used in the cards get damaged and become non-functional due to repeated usage. Third, manufacturing large number of cards and transporting them to the end users involve considerable cost. Fourth, physical cards require relatively longer time to authenticate users leading to long queue at the ATM kiosks.

The aim of this paper is to propose an architecture which enables the provisioning of secure ATM transaction by providing a cardless transaction to the user .This is implemented using the fingerprint of the user. The main reason for choosing fingerprint for ATM transaction is that every user have an identical fingerprint pattern and any fingerprint cannot be same as other. This leads the user to make their ATM transaction more secure than other type of transaction. In this security of the user is also maintained by sending an one time password to the user. If the Fingerprint is not recognized properly we use an Near Field Communication (NFC) technology in this project we use an NFC card and NFC card reader and the same procedure is repeated same as fingerprint technology. In future we can make use this NFC technology in our Smartphone and do transaction without carrying any card along the ATM

This Project replaces the physical ATM card by implementing with Fingerprint and Near Field Communication which overcome the disadvantages associated with ordinary physical ATM card, Such as ATM card skimming, magnetic strip may get damaged, sometimes card may get lost, initial authentic process may take much longer time, manufacturing and transportation of card to end user may take much time.

The objective of our proposed work is to replace physical ATM cards by smart phones in NFC Card Emulation mode during an ATM transaction to counter the issues prevalent with the use of ATM cards. The combination of NFC with smart devices has led to widening the utilization range of NFC. In card-emulation mode, a NFC device behaves like a contactless smart card. In this mode, the mobile phone does not generate

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

its own RF field; the NFC reader creates this field instead. At the ATM kiosk, in order to authenticate, the user needs to swipe his/her mobile phone in front of the NFC reader. During an ATM transaction, an ATM card is not required and the system will still have a stronger security compared to the system in which ATM card was used. Through data encryption and secure channels, NFC technology keeps the customer information safe. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

## II. RELATED WORK

To carry out secure ATM transactions a NFC enabled solution was proposed by Mandalapu etal. [1]. Here, the first level of authentication involves ATM card swiping or manual ATM card number entry. The successive process features the use of an NFC enabled cell phone having access to Internet. The user is required to tap the cell phone on the NFC tag fixed on the ATM. The tapping opens up a webpage on the mobile phone's browser and requests for a pre-registered phone number as a user input. Following this step, the user is required to enter a Pattern Password that was previously registered online during the registration process to use NFC. The pattern password appears as a random set of numbers. The OTP is then generated on a subsequent page. This OTP needs to be entered on the ATM's screen before a preset timeout. Some of the drawbacks of the solution are the requirement of ATM card to carry out ATM transactions, a need to remember the pattern password and an increase in authentication duration at ATM kiosks.

The usage of the ATM Terminals could be extended to numerous other government related services which could reach the end users at a very fast phase and thus utilize these systems installed efficiently rather than using it only for instant cash withdrawal. Though there is much criticism regarding the usage of ATM terminals for non - financial services, they could indeed be used effectively to meet various needs of the end users. To answer this criticism, it is necessary to look on to the initial purpose of laying this ATM terminal worldwide. The main purpose of the ATM installation was proposed earlier that these terminals would function as a mini financial institution and would encompass all the services of the financial institutions like loan processing, all financial withdrawals and deposit etc. But because of few limitations (like unavailability of man power to get all the deposits from the ATM on a daily basis to facilitate the deposits in ATM) it has been forced to become a currency vendor machine. This state of ATM terminals now could be improved by facilitating socio-public services through the ATM terminals, thus increasing their utilization rate. The main problem involved is in security issue by transferring from a private to a newer public domain. Due to the convenience in cash withdrawals while using ATM terminals, the humans across the globe are willing to possess an ATM card issued by their financial institutions. Thus the ATM system across the globe has now become famous for its instant cash delivery to the customers. Customers need to insert their ATM card provided by their financial institutions into the ATM terminals. To enable an authentication mechanism, a Personal Identification Number (PIN) is present against all the ATM card numbers. When their authentication is complete, the customer is allowed to select the type of transaction to be made by them - either balance enquiry or instant cash withdrawal. All these transactions now happen in a private network of the bank servers. So the process of intrusion becomes almost impossible for all the transactions that are currently happening between the ATM terminals and the bank server. But to implement any non-financial transactions creates an additional routing overhead on the NFS, as all transactions must be routed through NFS due to fact that all ATM networks are in the private network of the bank servers. So, there arises a need to reduce the overhead and extend the usage of ATMs to all other non-financial transactions and making its own operation in the public domain. This increases the efficiency of utilization of the installed Automated Teller Machines around the world and makes it more accessible to the end users. This makes the entire system usage robust.

Our proposed solution detailed in section III of this paper uses NFC technology to secure ATM transactions without the need of a physical ATM card. It does not have the issues prevalent in the above related works.

## III. PROPOSED SYSTEM

In this section, the working principle of the solution is described in details. The objective of our proposed work is to replace physical ATM cards by smart phones in NFC Card Emulation mode during an ATM transaction to counter the issues prevalent with the use of ATM cards. The combination of NFC with smart devices has led to widening the utilization range of NFC. In card-emulation mode, a NFC device behaves like a contactless smart card. In this mode, the mobile phone does not generate its own RF field; the NFC reader creates this field instead. At the ATM kiosk, in order to authenticate, the user needs to swipe his/her mobile phone in front of the NFC reader. During an ATM transaction, an ATM card is not required and the system will still have a stronger security compared to the system in which ATM card was used. Through data encryption and secure channels, NFC technology keeps the customer information safe. Security analysis and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

threat modeling shown in this paper highlights the security strength of the system during authentication.

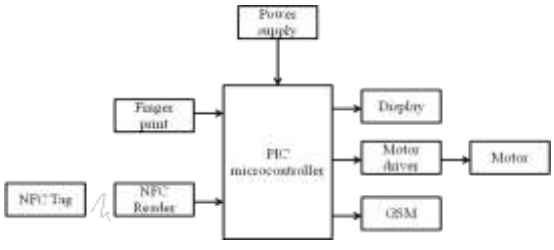
The finger print can be recognized in two ways using the minutiae based and image based methods. In minutiae based method represents the fingerprint by its local feature like termination and bifurcations. The other method uses an image based method, it make matching based on the global features of a whole fingerprint image .It is an advanced approach. In this all the image are stored in processor and stored image feature and the placed finger print is recognized. If it has a same feature then it ask for an verification process and then send an One time password.

Near Field Communication (NFC) is a technology for contactless short-range communication. Based on the Radio Frequency Identification (NFC), it uses magnetic field induction to enable communication between electronic devices. The number of short-range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use in conjunction with mobile phones offers great opportunities. One of the main goals of NFC technology has been to make the benefits of short-range contactless communications available to consumers globally. The existing radio frequency (RF) technology base has so far been driven by various business needs, such as logistics and item tracking. While the technology behind NFC is found in existing applications, there has been a shift in focus most notably, in how the technology is used and what it offers to consumers. With just a point or a touch, NFC enables effortless use of the devices and gadgets we use daily.

Here are some examples of a user can do with an NFC mobile phone in an NFC enabled environment:

Download music or video from a smart poster. Exchange business cards with another phone. Pay bus or train fare. Print an image on a printer.

### 3.1. WORKING OF PROPOSED MODEL




To secure ATM transactions a NFC enabled solution was proposed here, the first level of authentication involves ATM card swiping or manual ATM card number entry. The successive process features the use of an NFC enabled cell phone having access to Internet. The user is required to tap the cell phone on the NFC tag fixed on the ATM.

The tapping opens up a webpage on the mobile phone' s browser and requests for a pre-registered phone number as a user input.

Following this step,

1. The user is required to enter a Pattern Password that was previously registered online during the registration process to use NFC.
2. The pattern password appears as a random set of numbers. The OTP is then generated on a subsequent page.
3. This OTP needs to be entered on the ATM' s screen before a preset timeout.
4. Some of the drawbacks of the solution are the requirement of ATM card to carry out ATM transactions, a need to remember the pattern password and an increase in authentication duration at ATM kiosks.

An authentication solution using digital signature and NFC card emulation on android. In this solution the mobile device of the user saves the server information together with the private key and the server stores the mobile device UUID and the corresponding public key. During authentication the server returns a nonce, which includes the server info, a time-stamp, and a fixed length of random bits, to the client.

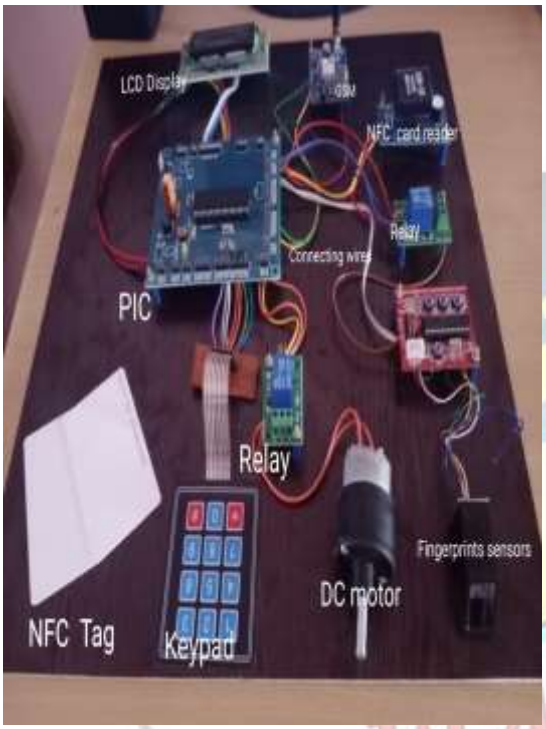
The NFC reader will then start to scan for NFC cards as soon as the client receives the nonce. The user has to swipe his/her mobile device at the NFC reader in 30 seconds once the reader starts scanning. Before the mobile device can communicate with the NFC reader, the user should execute the card emulation application and enter the PIN code. The mobile device signs the nonce with the corresponding private key and sends its UUID together with the signed nonce to the reader. The client then passes the message received from the mobile device to the server for verification. The usefulness of this solution compared to traditional password based authentication has been highlighted in the research. However, the solution has certain drawbacks. The need to store a private key securely and computation of digital signature in the mobile device during each authentication is an additional overhead. The private key would be server specific and hence for each new website/application different private keys needs to be stored by the mobile device.

### 3.2 RESULTS AND DISCUSSION

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

When the initialization of GSM is 100% completed then the LCD display types of transaction in the display .And it ask us to select to any one types of transaction such as cardless transaction or contactless transaction




3.3 Contactless Transaction

When we select contactless transaction (i.e.) the transaction using card then LCD display an message such as SHOW YOUR CARD in display .Then the card must be shown in the NFC reader as shown in the figureIf the card is properly detected the NFC card reader indicates an Blue light when the card is shown to the NFC reader. This shown in the below figureAs soon as the card is properly detected then it ask for human verification, this done by displaying ANY 4 DT 4 HUMAN in LCD display so we have to enter any four digit in order to verifyAfter verification of the user is a human, then it sends a One Time Password to your registered mobile number and display a message of CHECK YOUR MOBILE in order to authenticate the user who is the correct user of the appropriate account

As soon as the OTP is received to the registered mobile number the LCD display displays an message ENTER UR DYANAMIC NO then One Time Password has to be enteredAfter OTP has entered the authentication Process is indicated by running an motor which is connected to relay .when the user is properly verified the relay display blue light indication

Fig 3.1 Next step of transaction.
Detection of card

**Fig 3.2 Verification of user.**
**OTP to registered mobile**

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

Fig 3.3 OTP enter message.

Authentication Indication

3.4 Cardless Transaction


Fig3.4Next type of transaction

When we select cardless transaction (i.e.) the transaction using fingerprint is initialized then LCD display an message such as PUT YOUR FINGER in display .Then the finger must be placed in the fingerprint sensor. If the placed finger print is properly recognized then the
fingerprint controller indicates a green light indication or else blue light indication denotes an error

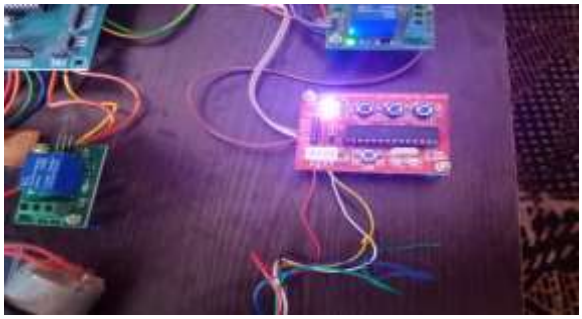


Fig 3.5 Recognization of fingerprint

As soon as fingerprint is properly detected then it ask for human verification,and the process is repeated as same as NFC tag reader

3.3 SCOPE OF PROJECT

1. Fingerprints keep the customer information safe.
2. Security analysis and threat modeling shown in this work highlights the security strength of the system during authentication.
3. In our future work, the plan is to focus on the security aspects of the custom authentication app to be installed on the smart phone. Also, an exhaustive analysis will be carried out on the possible security attacks during ATM transactions which have been addressed in the scope of this work.
4. Using NFC privacy can be maintained than other tag
5. During an ATM transaction, an ATM card is not required. Since it leads an improvement in ATM transaction by introducing cardless ATM transaction for the user.

## IV. CONCLUSION AND FUTURE WORK

This work covered the entire details of Near Field Communication (NFC) technology. NFC can be combined with existing infrared, Bluetooth technologies for improving the range of NFC. NFC offers a secure and simple way for transferring data between two electronic devices. Another advantage of NFC is its compatibility with RFID technology. NFC is actually based on RFID technology. RFID uses magnetic field induction to initiate communication between electronic devices in close vicinity.NFC operates at 13.56MHz and has 424kbps maximum data transfer rate. ATM is a convenient way to meet the banking needs of the users. ATM machines are deployed worldwide and used by a very large population of the world. So it is essential that the ATM transactions are safe and quick. The use of debit card or other types of cards during ATM transactions has some problems like prone to ATM skimming, magnetic strips of card getting damaged, manufacturing and transportation cost of cards, longer time to authenticate users etc. The discussion on the advantages of using smart phone in NFC card emulation mode

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 9, September 2020

over ATM card shows that it is a useful alternative. Security analysis and threat modeling highlights the security strength of the proposed system against the vulnerable attacks during authentication.

In our future we have planned to use Raspberry Pi instead of PIC micro controller to improve the speed and networking of the system. And also to replace the NFC card by using in smart phone this completely enable cardless ATM transaction

REFERENCES

[1] A. Mandalapu, D. Deepa, L. Raj and A Dev, "An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies", 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, Canada, October 15–17, 2015, IEEE Xplore.

[2] A. Meschtscherjakov, M. Tscheligi, C. Gschwendtner and P. Sundström, "Co-Designing for NFC and ATMs: An Inspirational Bits Approach", 15th International Conference on Human-Computer Interaction with Mobile Devices and Services", Munich, Germany, August 27 - 30, 2013, ACM.

[3] H. Lee, W.C. Hong, C.H. Kao and C.M. Cheng, "A User-Friendly Authentication Solution Using NFC Card Emulation on Android", 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, November 17–19, 2014, IEEE Xplore.

[4] R.M. Ranasinghe and G.Z. Yu, "RFID/NFC device with embedded fingerprint authentication system", 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, November 24-26, 2017, IEEE Xplore.

[5] S. Sridharan and K. Malladi, "New Generation ATM Terminal Services", International Conference on Computer Communication and Informatics (ICCCI -2016), Coimbatore, India, January 7-9, 2016, IEEE Xplore.

[6] V. Coskun, B. Ozdenizci and K. Ok, "A Survey on Near Field Communication (NFC) Technology", International Journal of Wireless Personal Communications, Springer, vol 71(3), pp. 2259-2294, August, 2013.

[7] Young-Gon Kim and Moon-Seog Jun, "A design of User Authentication system using QR code identifying method", 6th International Conference on Computer Science and Convergence,Information Technology, IEEE Transactions, pp. 31-35, Nov-Dec 2011