A NEAR FIELD COMMUNICATION FEATURED OF ATM CARD BLOCKING INTRICACIES

Ms Yashaswini S[1] Dr. Prabha R[2]
M.Tech (CNE) Professor(ISE)
Computer Network Engineering, Dr. Ambedkar Institute of Technology, VTU, Bengaluru, India

Abstract-Now a day everyone using credit and debit cards for money transaction. The cybercrimes are also increasing (skimming of ATM cards, brute force attack and Shoulder surfing) as the usage of the ATM (Automatic Teller Machine) Card Transaction. The credit or Debit card provided with single static PIN (Personal Identification Number) and is fixed which is very easy to grab this PIN number to the theft. To take prevention by blocking the ATM card is too longer procedure and take precautions by cybercrimes. The system introduced a new method of three level authentication scheme which includes Encrypted NFC card (The Near Field Communication is a Data Communication Technology with the short-range radio waves at the specific frequency of 13.56 MHz and inter connection providing data exchange) using NFC enabled Mobile phones, Dash Matrix Algorithm (pattern recognition) and Image Description. This system enhances the security level of ATM card for user and cost effectiveness.

Index Terms- **Dash matrix Algorithm, NFC enabled Mobile phones, NFC Cards, NDEF message**

I.INTRODUCTION

In our daily life ATM (Automatic Teller Machine) machine become the daily visited place and also user friendly for everyone. ATM machine where the people can withdraw money or can deposit the money. It is a time consumer for this busy world. Every time people visited to the bank and need to be stand in the queue to do the financial transaction. To keep our money in the packet is not so easy and its risk as well because of the theft. So, to avoid this issue, ATM machines are coming into exits.

Money transaction is very easy to withdraw or deposit our money in the bank anywhere any time. Every business transaction undergoes using ATM card either by using Debit or credit card. The ATM cards are used with our personal identification Number(PIN) for financial transaction. This PIN is having four-digit number which is Static and Fixed To make secure to our ATM cards and remembering our four-digit PIN number is truly difficult. There are many vulnerability and cyber criminals are undergoing now a day because of the financial transaction undergoing using ATM cards.

Now a day's cybercriminal became a major issue which elaborating enormous range. By using computer and network they grabbing the user information. cyber networks are interrupt and attack our privacy, economic, social life. These are the major harmful undergoing in this society. It has also brought accidental moments such as criminal activities, spamming, credit card frauds, phishing, and ATM fraud.

II. RELATED WORK

From the reference [1] where the system provided an embedded fingerprint biometric authentication system. This system used in the automated teller machine (ATM) banking systems. In this system, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level. The disadvantage in this system is very intrusive for some person, and it is still related to some criminal identification. And also, it can make mistakes with dryness or dirty of the finger's skin.

From the reference [2] the system provides the Designing and Implementation of Security Based ATM. They give deals with prevention of ATM theft from robbery. Whenever robbery occurs, Vibration sensor is used here which senses vibration produced from ATM machine. This system uses ARM controller, DC Motors, RTC, camera, keil tools to secure from robbery. The disadvantage is this system is it provided security only form robbery not for any other cybercrimes.

From the reference [4] the system analyse by providing the security to the Debit card by sending the Flash SMS to the Mobile Phone. This security reduces the ATM card Skimmer and Relay attack. The disadvantage is it is not provided the security to other cyber attacks such as brute force attacks. This are the some of the existing system against the security of ATM cards.

III. METHODOLOGY

Technologies used are:-
Mobile Application:

- Android

SERVER SIDE:

- Java Enabled Web Server / App Server(Tomcat)

SOFTWARE REQUIREMENTS:

- Android API 1.5 or higher
- Android Development Tool plugin
- Eclipse 3.4 or higher
- Sun JDK 5 or higher
- Web server Apache Tomcat
- Database GUI SQLYog
- Database My-SQL 5.0
- Card type NFC card (Mifare card)
- One / Two Smart Phones with NFC Features

To secure the ATM card we are providing three level authentications instead of the single PIN number. NFC near field communication is a set of communication protocols that enable two electronic devices, one is a portable device like smartphone other can be any other electronic device. The devices communicate within 4cm of each other with the contactless communication. NFC is used to share the information.

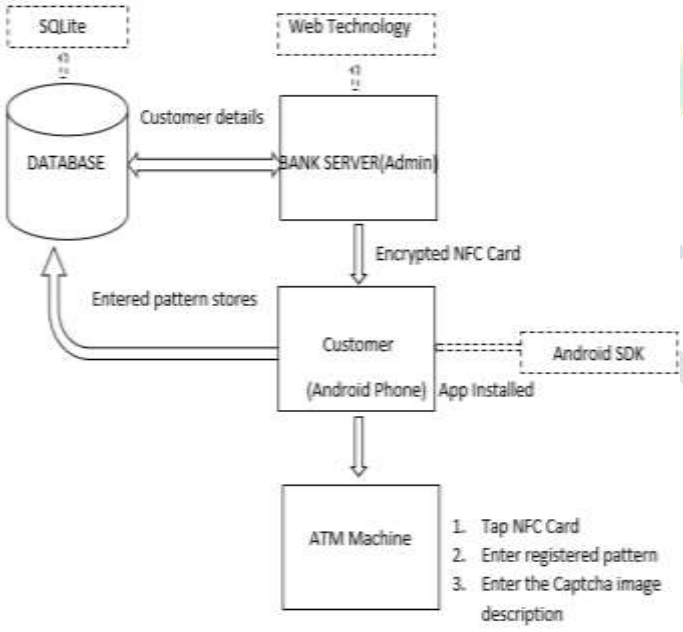

fig.1 system architecture

NFC Writing Module (Tag):

Basically NFC (Near Field Communication) Comes under the family of RFID (Radio-frequency identification) systems They both are permitting end to end communication in two ways. In earlier smartcards having only one-way communication. Since unpowered NFC tags can also be read by NFC devices, it is also capable of replacing earlier one-way applications. In this module the User details like account number., expiry date, branch details, bank name will be encrypted using XOR operation and dumped into the NFC tag, before dumping into the card first data is Declare an Intent Filter to announce to the system that it's enabled to work on NFC. Have a method that Android will call when NFC is detected. Create a method to build a NDEF message. Create a method to write the NDEF (NFC Data Exchange Format) message.

NFC Reading Module (Tag):

When the user taps the card to ATM machine, first XOR data is converted into original data and reading NFC data from an NFC card with language convention English and original data is sent to the server

Dash Matrix Pin Generation Module

User is having the android dash matrix app in his mobile phone, user has to give username and password, if validated, he has to select dash matrix pattern, based on the dash matrix pin is generated and updated to server.

Admin we Application Module

In this module Admin can able to login, admin can able to add user bank details and admin can able to add branch details of the bank and admin can able to change password.

User web server Module

In this module once, user taps the card to ATM machine and updated the pin of dash matrix to server. Once user taps the card to machine, server application ready to receive dash matrix pin, User has to enter pin, if pin is validated user will login to home page, user can make transactions.

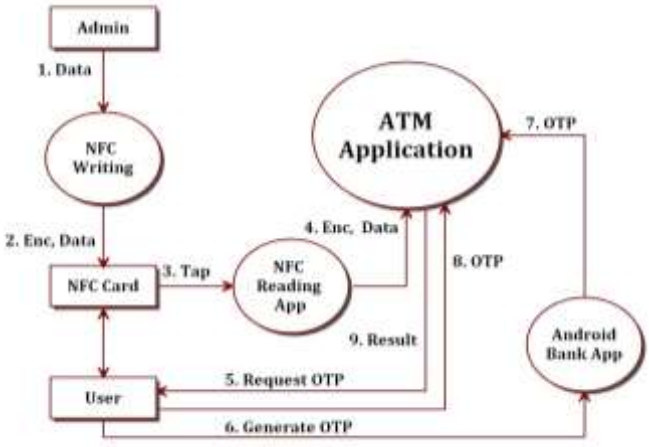

fig.2 context analysis

Above figure shows the Context Analysis Diagram in the three level authentication system using NFC cards.

IV. RESULTS AND DISCUSSION

The ATM skimmer is as shown in the fig where they keep camera to hack the PIN number of the ATM card. Like many vulnerable to password attacks(Brute-Force attack, retrieving passwords from the systems, Peeping attacks,Skimmer) as in the system OTP can change in the three level authentication.

fig.3 ATM skimmer

From the year of 2011 to 2015 finding many cyber criminals shown in the graph in India, Karnataka place a 3rd place in the cyber crime

fig.4 graphical representation of cyber crime found in India

NFC provide more security to access the ATM card with three level authentications by encrypted NFC card, sending OTP to the mobile phone and sending the captcha images with our own description.

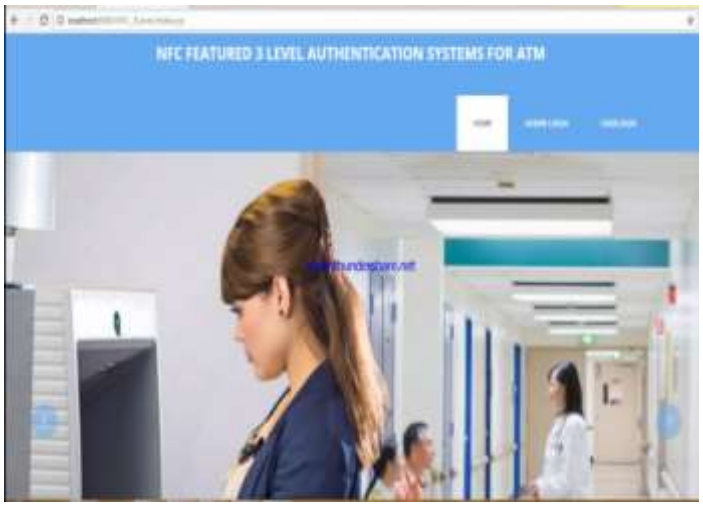

fig.5 admin and user maintain bank information

The above figure shows that the admin can maintain the customer bank information and user or customer can access his Bank information in this system.

Fig.6 NFC card reading in Mobile Application

The above figure shows mobile application install in the Android mobile and can tap the NFC card to decrypt the information. Then enter the pattern which generates the OTP number to enter in the ATM machine. Enter the Captcha image description. Which gives more security to the user to access ATM card.

V. CONCLUSION

This proposed system reduces the concept of four-digit PIN (Personal Identification Number) as a password for the access of an ATM system. In the present days society facing more vulnerable to password attacks (Brute-Force attack, peeping attacks, Skimmers) all

these aspects are overloaded by imparting this new scheme. By using NFC card, it is easy to open a webpage without the wastage of browsing time. The new schema Three level authentication system will give more security.

This schema is for NFC enabled mobile phones. In future we can make these features are available for Non – NFC mobile phones as well by providing the NFC Transmitter and receiver embedder tool kit. And also, can make the ATM card Block by the user itself within few hours by providing QR code.

REFERENCES

[1] *ATM Security Using Fingerprint Biometric Identifer:* An Investigative Study Moses Okechukwu Onyesolu Department of Computer Science Nnamdi Azikiwe University, Awka Anambra State, Nigeria. Ignatius Majesty Ezeani Department of Computer Science Nnamdi Azikiwe University, Awka Anambra State, Nigeria.

[2] *Design and Implementation of Security Based ATM theft Monitoring system*

Sivakumar T.1, Gajjala Askok2, k. Sai Venuprathap3 1M. Tech (Embedded systems), Dept. of ECE, Kuppam Engineering College, Kuppam, Chittoor (dst), A.P, India 2M. Tech (Embedded systems), Dept. of ECE, KEC, Kuppam -AP 3Dept. of ECE, Asst. Professor, Kuppam Engineering College, Kuppam, Chittoor (dst), A.P, India.

[3] *Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective*. Nana Kwame Gyamfi Computer Science Department, Kumasi Polytechnic Kumasi, Ghana Mustapha Adamu Mohammed and Kwaku Nuamah-Gyambra Computer Science Department, Koforidua Polytechnic Ghana. Dr. Ferdinand Katsriku and Dr. Jamal-Deen Abdulah University of Ghana Department of Computer Science.

[4] *Providing Security to Debit Cards Using Message Authentication*, Moshina Priyadharshini1, Arokiaraj Jovith.Department of IT- Information Security and Computer Forensics, SRM University, Kattankulathur, Chennai, T.N., INDIA Department of Information and Technology, SRM University, Kattankulathur, Chennai, T.N., INDIA.

[5] *Review Paper on Real Time Password Authentication System For Atm*. Ms. Soniya B. Milmile Electronics and Communication Engineering, GHRAET, RTMN University, Nagpur, India. Prof. Amol k. Boke Electronics and Communication Engineering, GHRAET, RTMN University, Nagpur, India