NCRISET-2017 e-ISSN: 2456-3463
International Journal of Innovations in Engineering and Science, Vol. 2, No.6, 2017
www.ijies.net

Digital Security System For Secured Banking Transactions

Rutuja Sagale
Electronics and telecom.
GHRIET,Nagpur
9552126463
Rutujasagale18@gmail.com

vishakha wanere
Electronics and telecom.
GHRIET,Nagpur
8412991545
vishakha.wanere@gmail.com

Priyanka kakad
Electronics and telecom.
GHRIET,Nagpur
8605586320
priyankakakad308@gmail.com

kamal kashyap
Electronics and telecom.
GHRIET,Nagpur
9665709380
kamalkumar.kashyap@raisoni.net

Abstract—*Network security consists of different policies and rules predefined by its administrator to avoid illegal access, any modification in network or its accessible resources. It is one of the biggest and challenging domain in the various fields where communication based activities continuously happened and security need to the data is high. One of the well-known applications of networking system is banking on which we are going to focus to provide security. Main issues in that is password hacking, in response, banks and other financial institutions have developed technologies like device identification, one-time password (OTP), Automated Transaction Machine (ATM) etc. But these facilities have limitations to some extent. So we are going to proposed secure online transaction system using MOTP (Mobile one-time password) and identity based Double Encryption for banking purpose which will try to overcome limitations of previous system and making strong authentication based transaction system available for permitted users. The system we called it as strong authenticated because along with double encryption we will be provide International Mobile Equipment Identity (IMEI) as well as Short Message Service (SMS) alert facilities in case of stolen or lost mobile phones. So user will not be worry for security while using our proposed system.*

Keywords—PIN, One Time Password, ATM, Android Operating System Security.

Introduction

Today, e-Banking application has gained popularity because of its innovative and techno based services which useful their customers in terms of time, money and synchronization. Various Banks now making facilities available to their customers using the pub/sub system, where customers able to specify their interested events by means of subscriptions. Without the bank knowing the relevant set of bank users, or vice versa. As smartphones started to replace the computer-based business applications and transactions, which marks the presence of confidential information, it becomes more vulnerable to cybercrimes. Mobile banking is the service that allows a mobile client to freely use his bank account for different services. The main success factors of mobile banking are its convenience, ease of use, ubiquity and reliability. Our work, as described in this paper, enhancing the trials to keep private and sensitive information on modern Android devices, and communicate confidential information with a remote client in a security level compared to wired communication in spite of reported risks and threats to which the Android platform is exposed. The present ATM system uses Bank ATM card and PIN (Personal Identification Number) which user can change at any time through ATM machines. If a thief has stolen the ATM card and if he/she knows the password, he/she can misuse the ATM card. In some cases it may be happen the attackers make a card as your ATM card and mischief with the Bank account. It makes a financial losses of customer so there are chances of security threats in existing system like shoulder surfing, data skimming, card trapping. Various Shoulder surfing resistant PIN entry methods have been proposed for secure PIN entry but they are not success in stop recording attack. Magnetic Stripe technology is most commonly used in which, when the person inserts his card into the card reader, the skimmer captures the card information with the help of skimming devices which is placed upon the reader, so various chances of skimming attacks has been seen. Now a days it is rarely happens that person having an ATM card but not having a mobile. The main purpose to

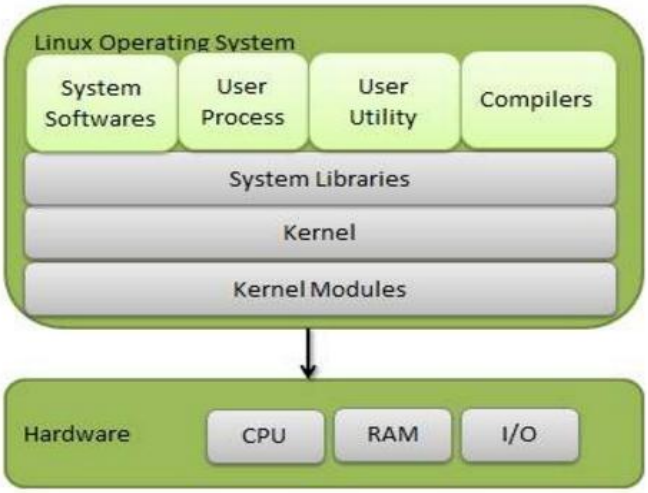
use (one time password) OTP is for uniquely identify of a mobile number registered by an individual on bank.

I. EASE OF USE

A. Android Operating System

Mobile devices most commonly used and recent operating systems are Android, iOS, and Windows8. Through use of these operating systems, Android continuously and rapidly increases its popularity and market share. Based on the information provided by Google in March 2015, Google has shipped 1 billion Android-Based smart phones in 2014. In addition, the open-source nature of the Android platform, the ease of application development and submission process with the Play Store have made Android platform more attractive. However, the security risks and threats have increased and continue to increase more than for other mobile platforms as they are not open-source operating systems, such as Apple's iOS. Android is an open-source operating system that is built on a Linux kernel. It was developed under the leadership of the Open Handset Alliance (OHA) and Google. In this section, an Android OS overview is introduced.Fig.1 demonstrates the Android layered architecture which consists of 5 basic layers, and each layer has different program sets. Layers are Application, Application Framework, Library, Runtime, and Linux layers [3, 7]. The Android operating system has a basic security architecture that tries to secure user information and applications. The architecture provides a security model that adopts security in each layer and maintains flexibilibity in its design because of its open-source.

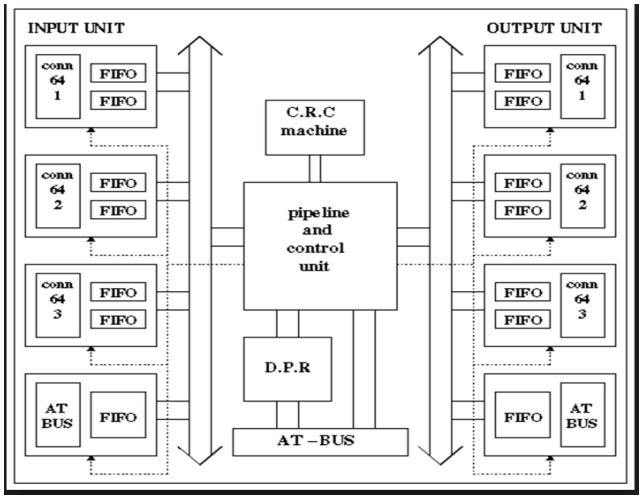
To achieve this goal, it supplies the following security features: 1- Powerful security mechanism on the Linux Kernel Level. 2- Sandboxing which means isolation of each application 3- Secure inter-process communication 4- Digital signature of applications 5- User approved and application specific permissions. 6- Approval for application stores Android applications are generally coded in the Java programming language, and they run on DVM (Dalvik Virtual Machine). In addition, compilation from C/C++ language is available. Applications are installed from a single file with .apk extension. The basic structure of an Android application includes the following: 1- Android Manifest File 2- Activities 3- Services 4- Broadcast Receivers.



B. Automatic Teller Machine

An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space. With the use of an ATM, customers can access their bank accounts for cash withdrawals and check their account balances. Nowadays Automated Teller Machines is considered as very common technology for dispensing notes to cash-holders. The ATM structure for cash withdrawal differs across countries. The first ATM was installed in the USA in 1969. ATMs have a positive effect on the nominal currency growth, but this effect is not very robust. Among all services of bank ATM is consider as more profitable service because it attract number of non-bank customers. The structure of ATM comprise on main components such as CPU, magnetic chip card, PIN pad, Secure crypto processor, function keys and vault. Since the introduction of the first automated teller machine (ATM) in 1967, perpetrators have been devising ways to try to steal the cash inside. Because ATMs eliminate the need for round-the clock human involvement and tend to be located in places that make them more vulnerable to attack, they are often attractive targets for perpetrators. ATM crime is not limited to the theft of cash in the ATM. Many ATM attacks seek to obtain a consumer‘s personal information, such as their card number and personal identification number (PIN). While these types of identity theft attacks take more effort to net cash for perpetrators, the result is the same—illegally obtaining money. According to estimates by Retail Banking Research, there are more than2.2 million ATMs deployed worldwide. This is a figure forecasted to exceed 3 million by 2016. As the number of ATMs in use increases, so do the frequency and sophistication of security threats, making the development of fraud prevention measures a top priority for financial institutions (FIs) and ATM manufacturers. ATM fraud is

not confined to particular regions of the world. To further complicate matters, perpetrators and victims are often on different continents, and the problems of one region can quickly become the problems of another.



II. IMPORTANCE OF ONE TIME PASSWORD(OTP)

In currently, withdrawing money from an ATM machine uses two factor authentication: the ATM card (what you have) and the personal identification number (what you know). Passwords are known to be one of the easiest targets of hackers. Therefore, most companies are searching more ways to protect their customers and employees. Biometrics is known to be very securing, but is used only in special organizations given the expensive hardware needed and their high maintenance costs. As an alternative, banks and companies are using tokens as a way of two-factor authentication. A token is a physical device that generates passwords needed in an authentication process. Tokens can either be software or hardware. Hardware tokens are small devices that can be easily carried. Some of these tokens store cryptographic keys or biometric data. Anytime a user wants to authenticate in a service, he uses the onetime password displayed on the token in addition to his normal account password. Software tokens are programs that run on computers and provide a onetime password that it is changed after a short amount of time. OTP algorithm's security is very important because no one should be able to guess the next password in sequence. The sequence should be random to the maximum possible extent, unpredictable and irreversible. Factors that can be used in OTP generation include names, time, seeds, etc. Several commercial two-factor authentication systems exist today such as RSA Secure ID. The OTP system generator passes the user‘s secret pass-phrase, along with a seed received from the server as part of the challenge, through multiple iterations of a secure hash function to produce a one-time password. After each successful Authentication, the number of secure hash function iterations is reduced by one. Thus, a unique sequence of passwords is generated. The server verifies the one-time password received from the generator by computing the secure hash function once and comparing the result with the previously accepted one-time password.

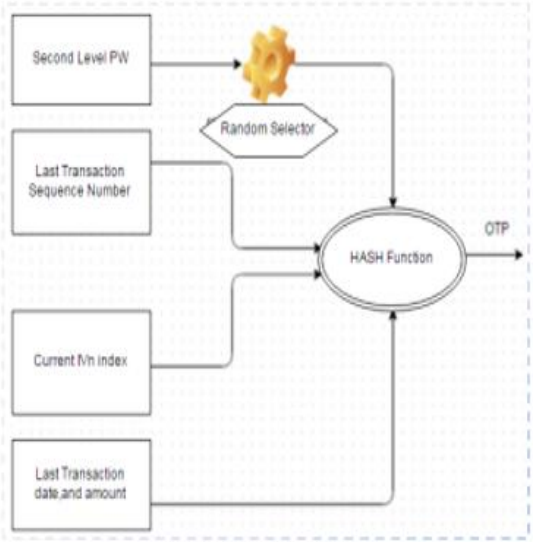


Fig.5 OTP generator

A. Advantages of OTP

1. Smarter, more advanced security system to protect you and your money through ATM.
2. OTPs are not vulnerable to replay attacks as they are valid just for a single login.
3. Provides a stronger method for authenticating your ATM transactions.
4. Acts as an extra level of protection should your Card Number and PIN be compromised.
5. OTPs are generated at random and are valid only for a specific period of time, thus ensuring utmost security.
6. SMS is the cheapest option to distribute OTP to the user.
7. Delivering OTP to mobile phone is simple and secure, as the user carries the mobile phone at all times.
8. There is no need for the user to carry an extra device, say a token, to view the OTP.
9. SMS is familiar, has huge customer base and can reach almost every single user.
10. SMS is available in all kinds of handsets.
11. It's totally free, secure and easy to use.
12. OTP through SMS effectively eliminates the need for Users to create and maintain passwards and falls password Cracking effects by publishers.

B.Wireless public key infrastructure

- As the number of user of mobile phone increases the need of providing mobile with internet services increases.
- The security of the wireless system and the internet should be at the same level.

- But the public key infrastructure ie.PKI used for security of E-commerce in wired internet not suitable for phone platform because of fundamental limitations of performance likewise limited size,memory and capability.
- The main purpose of the PKI is to provide authentication,integrity,confidentially and non-repudiation.
- The PKI relies on following components:-
    a) Certification authority(CA)
    b) Registration authority(RA)
    c) Certificate revolution list(CRL)
    d) X.509 Public key certificate.

C.Future work

- In this project, we have discussed about the increasing number of users of E-commerce sector likewise various facilities provided as ATM,E-banking etc.
- Along with the such sectors security issues arises and a challenge of keeping the sector secured also increases.
- An online banking security system to provide high authentication level they provided 2FA scheme.
- They performed detailed security analysis study related to different types of attack.
- During this work done we have seen that the main problem of this system was application of e-banking was sending data in the plain text format which has been reduced security of the user's data.
- So to overcome this we are designing a system for stronger identification and authentication of the system.
- We have used software-based solution consisting use of encryption algorithms we are trying to build challenged based methods such as short time passwords with symmetric cryptography and software security model.
- We have used IDEA symmetric cryptographic algorithm.
- In this we are increasing the security of the banking transactions by decreasing the reliability of the employ.
- By giving the master key to the customer at the time of opening of the account in the bank it makes the transactions and the account of the customer safe and provides customer service ease.
- As we know ATM provides very ease to the customer for fund transactions' gives us the easy option for the withdrawing and depositing of the money.
- We will provide master key to the customer for better and secured transaction.

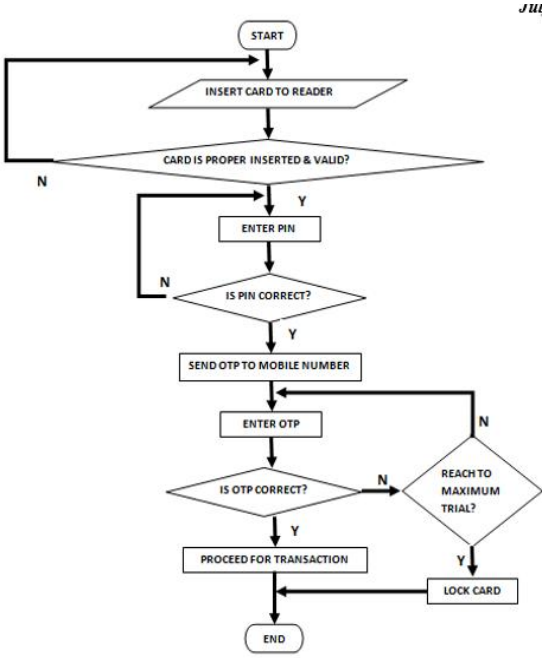


Fig. 1 Flowchart of proposed model

D.CONCLUSION

According to latest scenario ATM fraud is a very grave problem for banks. This project leads to establish authentication results which can be used by banks as well as various organizations. Now a day's security system used in ATMs is completely based on PIN security system which is vulnerable. Banks provide four digits PIN to the user which can be changed later by the user. After first use, user usually changes the password and keeps password quite guessable. This is the main drawback of this PIN type ATM system. When ATM card is lost or stolen it is required to close the ATM card by contacting the bank immediately. The paper indicates the strong authentication of ATM card with the help of One Time Password (OTP) on mobile device. So in this paper with the help of Password authentication and OTP the system will be simple, cost-effective and security level will get increase in an ATM transaction, as cell phone number is unique to every user. The method used in this paper is of significant use. As a result of the work proposed there will be benefit to human beings for the purpose of ATM security. By keeping in mind the point that is the security in the banking field we did successful survey for our proposed system. And during this study we came across various already implemented techniques, some issues related to transactions and solutions over these issues if exists. Some techniques we will definitely going to be utilize in our project and will try to enhance our system so that user will experience the strongly secure transaction system

E.REFERENCES

[1] Pennam Krishnamurthy & M. Maddhusudhan Reddy, ―Implementation of ATM Security by Using Fingerprint recognition and GSM ―International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249–071X, 2012

[2] M.Ajaykumar, N.BharathKumar, ―Anti-Theft ATM Machine Using Vibration Detection Sensor‖, International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, pp.416-418,2013

[3] Mun - Kyu lee _Security notations and advanced method for human shoulder- surfing resistant PIN entry' IEEE trans. on information forensics and security, vol. 9, no. 4, April 2014

[4] R. Rasu, P. Krishna Kumar, M. Chandraman _Security for ATM Terminal Using Various Recognition Systems' International Journal of Engineering and Innovative Technology 4th October 2012

[5] www.atmsecurity.com

[6] Prof. Gajanan Arsalwad etal,"Enhancing Authetication for online Transaction using MOTP and identity based Encryption" ,IJIRST –International Journal for Innovative Research in Science & Technology Volume 1 | Issue 11 | April 2015 ISSN (online): 2349-6010/ PP447-449/April2015.

[7] International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015 paper on secure android based mobile banking scheme by Hisham Sarhan Al-Azhar University Cairo, Egypt., Ahmed Safwat Al-Azhar University Cairo, Egypt.

[8] research paper on enhancement of ATM security and theft protection with the use of one time password,by Prof. (Dr.) Prashant P. Pittalia MCA Department, SJPIBMCA, Gandhinagar, India, ISSN: 2277 128X.