ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Smart Phone Based Biometric Authentication for Two Step Verification of ATM Transactions

Gowtham Bharadwaj, Gowtham N M, Puneeth Kumar R, Rahul R Tagadur, Tojo Mathew

B.E Student, Department of Computer Science And Engineering, NIE, Mysuru, Karnataka, India.

B.E Student, Department of Computer Science And Engineering, NIE, Mysuru, Karnataka, India.

B.E Student, Department of Computer Science And Engineering, NIE, Mysuru, Karnataka, India.

B.E Student, Department of Computer Science And Engineering, NIE, Mysuru, Karnataka, India.

Assistant Professor, Department of Computer Science And Engineering, NIE, Mysuru, Karnataka,India.

ABSTRACT:ATM (*automated teller machine)* is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller. On most modern ATMs, the customer is identified by inserting a ATM cardwith a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information. In every ATM, authentication is provided by the customer entering a Personal Identification Number(PIN). We propose a system where we use biometric as authentication. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. We also provide option of PIN authentication on user's request. Once the user is authenticated, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones.

KEYWORDS: Energy efficient algorithm; Manets; total transmission energy; maximum number of hops; network lifetime

I. INTRODUCTION

ATM (*automated teller machine)* is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller. On most modern ATMs, the customer is identified by inserting a ATM cardwith a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information. In every ATM, authentication is provided by the customer entering a Personal Identification Number(PIN). We develop an android application for ATM which operates through bank server. As customers register in our application, server will approve and then a PIN is created for authentication purpose. Using this PIN the user has to authenticate himself, then they are allowed to perform transactions like access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones. The app can find out all the nearest ATMs and can suggest ATMs where the required amount is available.

In any ATM, the customer can insert their ATM cards given by their banks and they are authenticated by giving the Personal Identification Number (PIN). If they are authenticated they can access their accounts and perform variety of transactions like cash withdrawals, check balance etc. Authentication is provided by the Personal Identification Number (PIN). If a hacker or any other person other than the account holder gives the correct PIN, then he can perform transactions and withdraw money. This system is not so secure. Added to this in the real-time scenario, when a person finds an ATM location and reaches there and comes to know that the machine is not in working condition. His search goes in vain; the proposed system overcomes this disadvantage.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. Related work

High Performance Computing (HPC) techniques are essential in complex systems such as Socio-Technical Systems (STSs), where humans and organizations are elements of the same system along with technical infrastructures and hardware/software components. For example, several HPC approaches have been successfully applied to support and facilitate distribution or aggregation of computation power among independent and atomic components (e.g., smart meters to solve and/or simulate complex models). However, HPC techniques have to be studied and developed without underestimating the problem of security that, given the interaction-centric nature of STSs, has to be considered not only from the single component perspective but for the system as a whole. In our previous work, we have proposed SecBPMN, a framework to support the design of secure STSs. It is used to model the interaction design and security policies of a STS and it supports their verification through a querying engine. In this paper, we describe how SecBPMN has been successfully used for the study of security in an Air Traffic Management (ATM) system, and we show how it can result also an efficient support when of HPC techniques when applied in complex and heterogeneous environment

III. Proposed algorithm

We propose a new system of Biometric ATM which authenticates user by their fingerprint and allows accessing their bank account details. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Today many smart phones have the facility to recognize the fingerprint and the rate at which technology is improving, we can expect biometric to be facilitated in all types of phones. So here we use a remote authentication from mobile phone biometric recognition facility to authenticate instead of a ATM PIN to access the account, i.e. when a customer punches his fingerprint on to the mobile and the authentication examined and intimated from the bank server to ATM and for security reason ATM will perform twice authentication before proceed further.We use computers in a network to illustrate this working procedure. Networking is used as the communication between server and ATM with socket programming. One computer will be considered as Server, which contains all the banking details like account, account details, fingerprints etc. Each node will be used as ATM- computers with fingerprint readers. The customers have to provide their fingerprint for authentication. If their fingerprint matches with the one stored in database, then customer is allowed to access his account details. This is a two-step authentication wherein once the fingerprint is provided to access the machine and same fingerprint is used again to authenticate the account.

A. *Types of Authentiacation:*

- Biometric authentication - The default is Biometric authentication, which is nothing but fingerprint authentication. Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints.
- PIN authentication– When the user sends request from the registered mobile number, the PIN will be generated and active for ‘n’ minutes.

B. *Types of modules in the system:*

Registration

When users register to our application, they provide their personal details like name, bank details, account details, etc. These details will be sent to admin (server) for verification. If the bank account is blocked, then user is rejected, else he will be approved.

- File management :All the users’ details will be stored in cloud like name, bank details, account details, mobile number, PIN etc.

- Secure hashing algorithm:The term secure hash algorithm (short SHA) refers to a group of standardized cryptologic hash functions. These are used to calculate a unique check value for any digital data (messages) and are the basis for creating a digital signature. The test value is used to ensure the integrity of a message. If two messages give the same test value, to the equality of messages after normal discretion be guaranteed, without prejudice targeted Attempts to manipulate the news. Therefore it requires a cryptologic hash function,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

the property of collision safety : it should be virtually impossible to create two different messages with the same test value.

- GPS:The user can be at different cities, by the help of GPS, user location and nearby ATM location is found. The user can locate for a nearby ATM which is in a working condition using Global Positioning System (GPS).
- Balance Enquiry: User can enter the required amount and the application finds out whether which ATM has so much balance in ATM and can suggest that ATM.

IV. PSEUDO CODE

```
Step 1: Regitering the ATM and accepting it admin
Step 2: Registration of the customer in mobile application.
Step 3:  Check the below condition for each each customer validation
          if (fingerprint ==valid)
               Make the customer to do the transactions in the ATm
         else
               Display authentication failed
         end
Step 4:  send the detail of transactions to the bank server.
Step 5: Send transaction information to the customer.
Step 8: End.
```

V. IMPLEMENTATION OF SOFTWARE

The software implementation, which provides the right mobile interface for the user to access the features his account details such as withdrawal, balance enquiry, statement slip , locate ATM,check the balance in ATM.

Whereas in admin part we use dontnet frame work to handle account transaction in the bank such as

1. Registering the atm machine and approving of it.
2. Creation of new customers.
3. Modifying the customer details and depositing cash to customers.
4. Loading the cash to atm machines.
5. Genrating the new pin for customer.

Whereas in the user side we provide an android and desktop application for authenticating and doing transactions

Android part includes:

1. Authenticating customer accessing to his accout through his account number and finger print sensor.
2. Searching for nearest ATM and available balance in that ATM.

Desktop side include

1. Bank transactions like withdrawl ,deposit ,checking balance etc.
2. Requesting for new services by customer to the bank (eg:cheque book request).

VI. RESULT

End Users will be provided double security due to the two step authentication through the Mobile app provided. This provides security against card theft or lost or snooping of pin etc. The system is very user friendly and doesn't cause any additional trouble to the user.The system automates the process of authentication.It works on all mobile platform like IOS, Andriod , provided the device has finger print sensore hardware.It also provides user to locate the ATM which are near by.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

VII. Conclusion and Future Work

We develop an android application for customers and standby application for admin which operates through bank server. As customers register in our application, they will provided with mobile-biometric ATM facility.After approval of the customer by the bank server the customer can do the transactions in the ATM which the bank provides. "Thus providing more security for the customers than by the usage of smart cards".Future enhancement may includes ,Providing the customer with transaction going through mobile phones eliminating the usage of ATM machines. Thus only cash machine is to be deployed by banks.

REFERENCES

[1] G. Renee Jebaline ; CSE Department, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India ; S. GomathiJava and J2EE -Balgur swamy and Herbert schildt, "A novel method to enhance the security of ATM using biometrics", IEEE, March 2015

[2] Rainer Koelle ; Walter Strijland ; Stefan Roels, "Towards Harmonising the Legislative, Regulatory, and Standards-Based Framework for ATM Security: Developing a Software Support Tool",IEEE, September 2013.

BIOGRAPHY

Rahul R Tagadur,Gowtham bharadwaj,Gowtham N M,Puneeth Kumar Rare students in The National Institute Of Engineering, Mysore,India. They are pursuing Batchelor Of Enginnering(At the time of publishing) in Computer Science Engineering.(Of batch 2016**). Tojo Mathew** works as an Assistant Professor in the same institution.