www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 6835-6838

OTP Generation for ATM Theft Protection

D.Priya[#1],R.Suganya[#2], Dr.R.Neduncheliar[#3]

Under Graduate Students[*], Professor[#]

Department of Computer Science and Engineering

Saveetha School of Engineering

Saveetha University

priyapria22@gmail.com[*],rsuganyatnr@gmail.com[*],chelian1959@gmail.com[#]

Abstract:

Anself-governing ATM host has aright to use any bank. There is no security layer is implemented in the ATM card except pin number. It is very costly for the bank to include the fingerprint and Iris scanner. In this paper, we monitor the location of the ATM usage, time taken for the user to accessing the ATM machine, sequence of events processed by the user and expected amount of withdrawal by the user. All these four factors are verified for the authentication purpose of the user along with password. If any of the above said, parameter are differing and then the One Time Password is generated to the User's Mobile number for further more secure authentication system. In the modification phase, an automation user Internet recognition model is designed to enhance the user comfort and detection of the time span spend by the user in the ATM machine. If due to signal problem of the mobile One Time Password will not be received in that cause secret process is used to private ATM users.

Keywords: ATM, Transaction, Identity theft, One Time Password, Secret process.

1.INTRODUCTION

ATM is a machine which is used to dispense and deposit money. [2] ATM processor is a Automatic Teller Machine, i.e. a machine that,when you insert a card, gives you means a exchange. There are two types of ATM machine . The First type is to drop money by the userand get the receipt based on the account . The second type is more advanced in which we will be able to credit card payment , deposit money and user can get information about the account.

ATM is used by many people to drop money. If cash is requiredto user they can get money with the help of ATM machine, which is near to the user location. ATM machine has two input and four outputsas per user needs. [2] Each ATM card has unique number is called as PIN number. If the card is identified, then machine will ask user to enter the PIN number. ATM machine will start the process of transaction if PIN number is correct, if not transaction process will be blocked. Each user can change there PIN number, so that it is easy to remember.Output of the ATM machine is Display screen, Receipt printer ,Cash dispenser, Speakers

1.1 Functional Overview

In this process it consists of recording the following parameters for the transaction:

- Location Tracking
- Minutes Consumed
- Event Processed
- Average Amount

If any misbehaviour take place it will block the enter transaction. One might think that it could be very plausible to have deviation from one of these parameters on a regular basis for the original user of the ATM card. For that purpose, our model declares a transaction as fraudulent only if 3 or more of the 4 factors mentioned above are deviated from the user's record then it is Post Declaring Fraudulent /Legitimate Action. If the transaction is declared as legitimate, the user may proceed with the withdrawal of cash from the ATM. But if the transaction turns out to be fraudulent one, which could happen with a slim possibility for the original user, the user would be sent a text message with a One Time Password to his/her mobile through the ATM's record searching ability and network connectivity. The user may then unblock the transaction with that password. In case of a fraudulent user, the original user would be notified that someone is performing an identity theft with their ATM card and would be prompted to take appropriate action after the realization of such an event. In case of signal problem occurs then use the secret quiz process to unblock the process.

2.SYSTEM ANALYSIS

2.1 Existing System

There is no security layer is implemented in the ATM card except PIN number. It is very costly to include fingerprint and Iris scanner in normal transaction. ATM card falling into wrong hands, and the PIN number being cracked by a stranger. Then stranger can easily use the ATM card.

2.2 Proposed System

Increase the security level by verify the for factors. One time password will let the user know that if hackers are accessing with their ATM cards. If due to signal problem message is not received to mobile in that case secret quiz is used. Then transaction process will be unblocked.

3.SYSTEM DESIGN

3.1 Architecture Diagram

It gives the basic architecture of the developing project

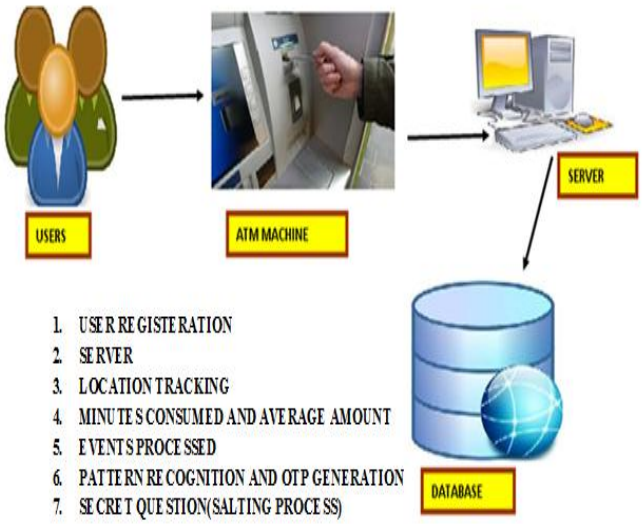

Figure 1.Architecture Diagram

3.2 Flow Chart

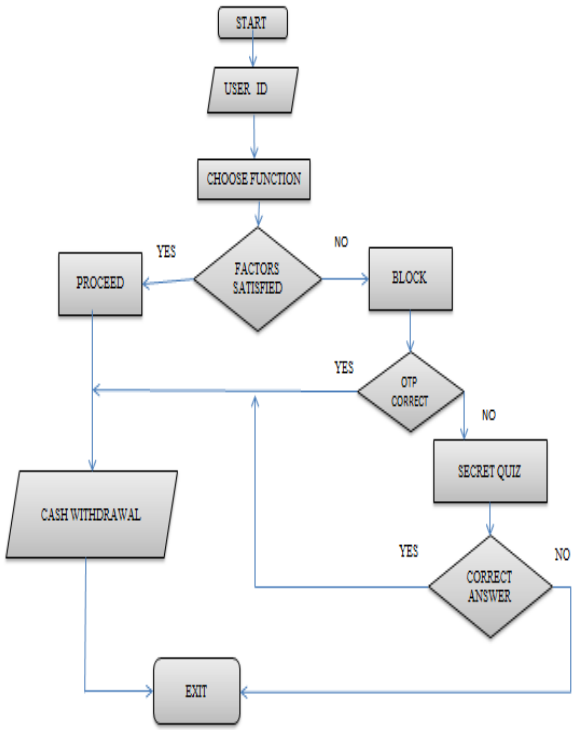

Figure 2.Flowchart

4.SYSTEM IMPLEMENTATION

4.1 Module Explanation

4.1.1.USER REGISTRATION

This module is used to create an user registrationsform.After registering application form the useris able to enter into process. To register the form following details should be given by the user, the

details that should be filled by the user is their personal details and the required details by the bank i.e the card number, pin code, secret password, account type account branch etc. Then only the useris allowed to enter the server.Once they activate their account, they are allowed to access their user id..

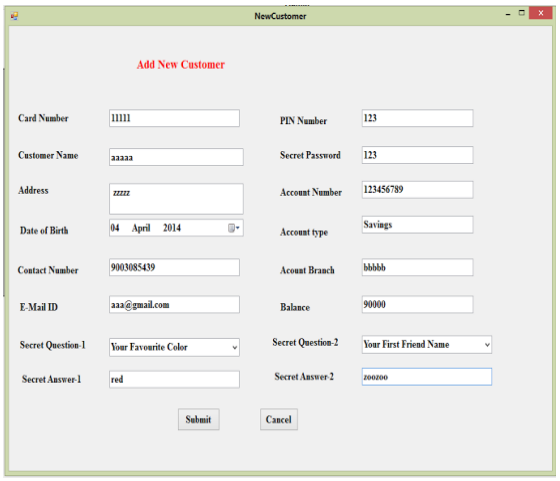

Figure 3.Registration Form

4.1.2.SERVER

The particular server will certainly monitor the complete User's data inside their data source along with verify all of them if expected. Additionally the server will certainly shop the complete User's data inside their data source. Additionally the server has to establish the connection to be able to get in touch with the users. The particular server will certainly bring up to date the each and every user's activities with it is data source. The particular server will certainly authenticate each and every individual previous to many people admittance the application. So that the server will certainly stop the unauthorized individual coming from being able to view the application.

4.1.3.LOCATION TRACKING

In this module, we track the location of the user access. Every time we monitor the location of the system that they are accessing. The user will frequently use the same location to access the location. So that we can monitor the User usage. This will increase the security level. Also the server stores this information in the database.

4.1.4.ACCESS TIME TAKEN AND AVERAGE AMOUNT

Here we will monitor the access information of the users. The server will monitor the users access information along with the time taken to access the ATM. So that based on the Time of usage and amount withdrawn by the users will be stored in the database. So that we may able to retrieve the usage time and amount withdrawn by the users.

4.1.5.SEQUENCE OF USAGE

We also track the usage sequence of each and every user. [4]So that we may able to track the users access details. The system will recognize the user's usage sequence. For an example if the users are login into their account and they check their balance and then proceed to withdraw the cash from their respective account.

4.1.6. OTP GENERATION AND SECURITY QUESTION

The server will check the above mentioned details and generate an One Time Password if these details are varies. This One Time Password will be send to the user's mobile number. So that the user is requested to enter their One Time Password and that will be verified by the Server, then only they are allowed to access to the system. To generate the One Time Password, we are using a Secure Random Number Generation algorithm. To generate the SMS to User mobile number we are using JSMS. Jar file which is used to send the SMS from the Server system to external device will transmit the SMS to the Concerned User's Mobile Number. In very rare cases we handle a difficulty about the coverage of mobile network is nil, so at that time we use security question as an alternative to access the ATM.

Figure 4.Secret Question

4.1.7. SECRET PASSWORD WITH SALTING PROCESS

We propose a salting method which is added by the user with the user's input of secret password.[7]The added values are sent to the server. The server will check the value and desalt the values. Then it check the secret password and compare it with user secret password. If it is matched means the user will be allowed for any operation which they prefer otherwise they won't be allowed. Password stretching method is used here.

Klong=F(Kshort,Salt)

V=fsalt (Kshort, username), Klong =fk(Kshort, dom, V).

By using this formula to create user specific and password is stretch. F() is a function used to hash based. The formula shows that feeble password(kshort) and robust password(klong),Salt is a variable where f is a passwordstretching function.

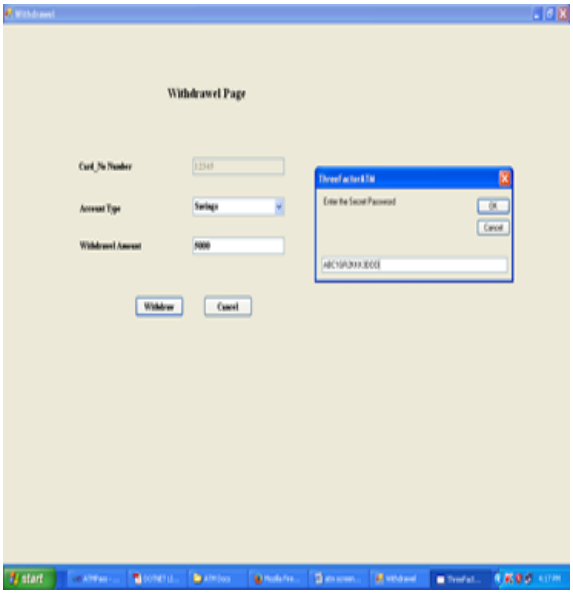

Figure 5. Salting Process

5.CONCLUSION

In this paper we have implemented a new mechanism named OTP generation technique with secret question and salting process will provide more security for accessing the ATM in cost effective manner. If some authorized person uses the ATM we may be able to identify them if the transaction is blocked, the user may easily unblock it with the 'One Time Password' service. If not by using secret question you can unblock the process. From feeble password to generate robust password Strecthing algorithmis used. It will give security against a pre computation attack.

6. FUTURE ENHANCEMENT

We also implement the graphical password authorization scheme along with the pattern recognition mechanism and RSA-ID identification, so that the security level will be further increased.

7.REFERENCE

[1] SkomersicM,Gojevic T, Zuvanic M, "Impact of non-service related signalling in mobile network",MIPRO 2012 proceedings of the 35th international convention.

[2]S Obradovic,DTesic, D Milanovic, A Zoric,DPerisic,@Protocols and programs in ATM Terminal Network", Telecommunications Forum(TELFOR),2012 20th edition.

[3]I Martin,"Too Far ahead of its Time:Barclays, burroughs and Real Time Banking,"Annals of History of Computing,IEEE Volume.

[4]M.K.Harma R.Dubry,"Advancements in Banking using Technology," Computing Scienceand Information Technology-Spring Conference,2009.IACSITCS '09

[5]J.A.Halderman, B. Waters, and E.Felten, AConvienient methods for security managing password Proceedings of the14th International World Wide Web Conference (WWW 2005).

[6] " A Password Strectching method using specific Salts". Changhee Lee, Heejo Lee.

[7]"J. Kelsey, B.Schneier, C.Hall,andD.Wanger, Secure applications of low-entropy keys". Lecture Notes in Computer Science,1396:121-134,1998.

[8] "Stronger Password Authentication Using Browser Extensions, Proceedings" of the 14thUsenix Security Symposium, 2005.Blake Ross, Colin Jackson, Nicholas Miyake, Dan Boneh and John C.Mitchell.

[9]"Making a Faster Cryptanalytic Time-Memory Trade-Off, Poceedings of Cryoto'03," Philippe Oechslin.