Securing ATM with OTP and Biometric

Mohammed Hamid Khan
Shah and Anchor Kutchhi Engineering College
Mumbai, India.
Email: mailathamid@gmail.com

Abstract:- In today's world, money can be required at anytime or anywhere such as shopping, travelling or health emergencies etc. The need of money can only be satisfied when you are carrying money with you. That also increases the risk of getting robed. Bank is a safest place to keep money. Bank provides Automated teller machine (ATM) which can provide money any where you want. ATM is an easy way to get money, you just need to insert card and password and you just got the money. But what if someone will steal your card and somehow he/she will know your password, it will grant him/her full access to your money. That raise question on present security and demands something new in the system that can provide second level of security.

One time password (OTP) is password that validates an authentic user for only one login to the respective system. If user is unauthorized, system will not allow further access. OTP can be generated by using different cryptographic hash functions that provides a fixed string which can be used as second level security at ATM. In generation of OTP there are many factors that can make OTP unique every time it is generated.

Factors that can be considered are time at when the user is accessing the machine, account number of the user, mobile number of the user, Location of the user, International Mobile station Equipment Identity (IMEI) number which is unique for every mobile device. By taking into consideration factors like daily life problem (general problems) that is phone got switched off, battery is down; less coverage of network can affect the OTP solution etc. To avoid application based problem this report also suggest a solution i.e. biometric security; by using biometric security the alternative security will be as same as OTP.

In this report, the flow of system I am developing, topics related to ATM banking and security, about OTP and biometric solution are discussed.

*****

I. Introduction:

In the war of functionality versus security, the functionality wins more often. Security has always been viewed upon as an overhead or afterthought by software developers. But in the case of banking and money transactions, the security should hold highest priority. Increase in daily attacks on ATM and banking security [1] the developers getting on right track and putting security their important aspect in developing projects.

The multifactor authentication is an approach to authentication which requires the presentation of two or more authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). After presentation, each factor must be validated by the other party for authentication to occur [2].

In present days the ATM holds only one thing (i.e. PIN) to secure the money saved in the bank if we are not considering the physical attacks. In our system we are going beyond this level of security to enhance security of the ATM. We introduce the concept of one time password (OTP) [3] in ATM banking. Our system will provide the second level of security using different factors to generate OTP. This will send over customer's mobile number stored in records.

In secure ATM, user will have to register mobile and its IMEI number in bank system. When user puts/swipes card into machine, user get request to insert PIN (which is current way of ATM banking). In the proposed system user will get OTP on mobile. When user enters OTP to the system, he/she will be having access to the machine else no transaction can be made.

In addition to the OTP for security the user will be having another option for second level security i.e. Biometric [4]. Through biometric the basic problems (like loss or forgotten mobile device or currently not available with the authentic user due to some reason) can be resolved. So to enable this option the user have to register his/her biometric information at the time of opening the account or have to update the current information. At the ATM a scanner will be attached and that scanner will scan the fingerprint of the user which is compared with the database of the user.

II. Problem statement

The problem with current ATM banking is, every day there is something new that make bad impact on security related to ATM banking. This leads to necessity of new techniques

or algorithms to deal with new possible attacks that can happen.

This project will give a good way to solve problems like card fraud, skimming, card data stealing/trapping. This project will be presenting an algorithm, which will be capable of considering more than two factors to generate an OTP. While generating an OTP, the proposed algorithm will consider current time, location of ATM the IMEI number and mobile number of user.

This project is also considering application based problem of ATM where the factors like, user forgot the mobile device at home, mobile battery is down, and user is not in the network coverage to make difficulties in OTP security service. For covering such difficulties another option is given in the ATM that is Biometric. By using biometric authentication legitimate user can do transaction even if he/she is not having his/her mobile device for receiving OTP.

III. Proposed System

a. Existing system

In present days the ATM holds only one thing (i.e. PIN) to secure the money saved in the bank and if we are not considering the physical attacks.

1. User enters the card to machine.
2. Card Reader reads the information on the magnetic strip on the card and sends the information to the bank server. If the card information is valid according to the bank, the ATM will ask for PIN.
3. User will enter PIN to the ATM machine.
4. If PIN entered by User is correct according to server, User will be allowed further to access for transactions.
5. This is process will only be applicable for one time, i.e. if user want to withdraw more money than he/she have to repeat the process again.

But there are problems and vulnerabilities in the present system.

1. It is possible that the machine is tempered and read wrong information as correct information.
2. It is also possible that the magnetic strips hold legitimate information but that card is duplicated.
3. PIN can be hacked by any means like shoulder surfing, mutual friends, family friends etc.
4. After PIN is correct there is no one who can catch attacker to steal money from bank. It is just like stealing from cupboard.

Current ATM system is not the safest system for the most important asset of human being i.e. Money. There is a need of some new system which is easy to adapt and more secure

b. Objective

The main objective of this project is to provide more security to the ATM system by using most trusted and easy way that is One Time Password (OTP) and Biometric System.

1. When user wants to use OTP of the ATM System, the OTP should be produced at that time only with current time and user's available data in the present database system and OTP should be delivered on registered mobile of the user.
2. If user selects biometric option on the screen, system should get biometric pattern information from stored database and should match the information with current scanned fingerprint.

Other Objective of this project is to introduce user friendly system for those people who are less familiar with newer technologies, with very few changes in the current system. That is accomplished by using current technologies/devices like Mobile, SMS, and ATM GUI etc.

Perspective of Proposed System

Given in the diagram is block diagram in Figure 3 is of the proposed system.

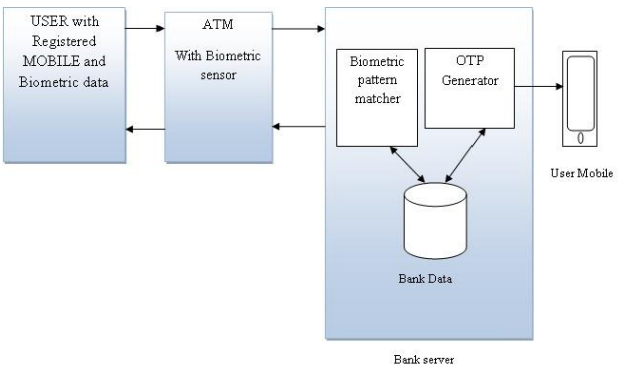


Figure 1. Block Diagram of securing ATM with OTP and Biometric

First block denotes user who is accessing the ATM machine (i.e. user). At the time of opening account the bank system will ask about mobile registration of the mobile number of the user with biometric information (say fingerprint). This information will be stored in the bank database for further reference. When User goes to any ATM machine he/she has to swipe card to machine after that machine and bank server

 ISSN: 2321-8169
2041 - 2044

will check validation and authentication of that card, if card and its information is correct machine will ask the PIN of the user. That card detail and PIN will be verified on the banking system. If PIN entered by the user is correct then the user will undergo another/proposed steps.

After verification of the card owner and PIN, bank system will ask user to select one option among two that is One Time Password or Biometric. If user selects OTP, system will access the user details from database and generate the OTP (by using SHA-1[5][6] algorithm and proposed OTP extract method) that will be further send to the mobile number of the user. When user gets OTP code on mobile he/she has to enter that code on the screen in same way as PIN. But here circumstantial problem arises for example dead battery of mobile, no network coverage or delayed SMS delivery. To deal with problems like this, user will be having another option as Biometric which is as effective as OTP in terms of securing any system. If entered OTP is correct then ATM system will allow access to user for transaction.

When user selects Biometric option on screen, system will check and fetch information about that particular account on which card information is stored in the database, after PIN is successfully entered by user, user has to place his/her finger on dedicated scanner on ATM machine. That scanner will scan a fingerprint image of the user and that image will be matched with the database images. If a pattern of fingerprints matches then user is a legitimate user and access will be granted. If user fingerprint and database fingerprint does not match then ATM machine will show home screen and will ask to repeat swiping card procedure again.

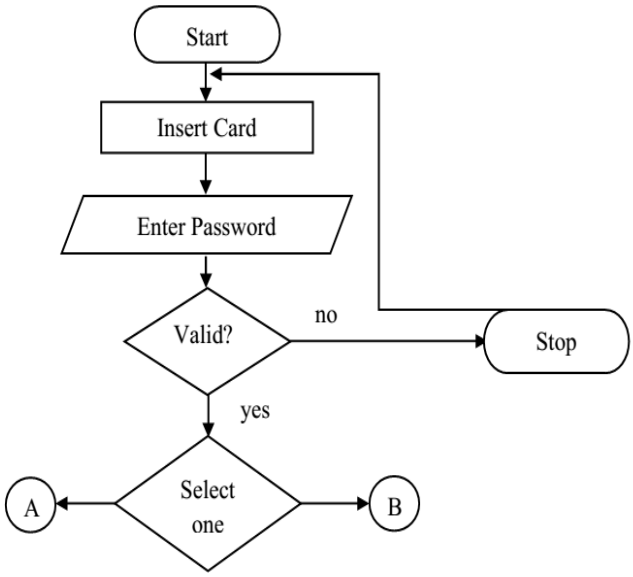
Design and implementation constraints

This project needs some changes in current design of ATM system that are listed below.

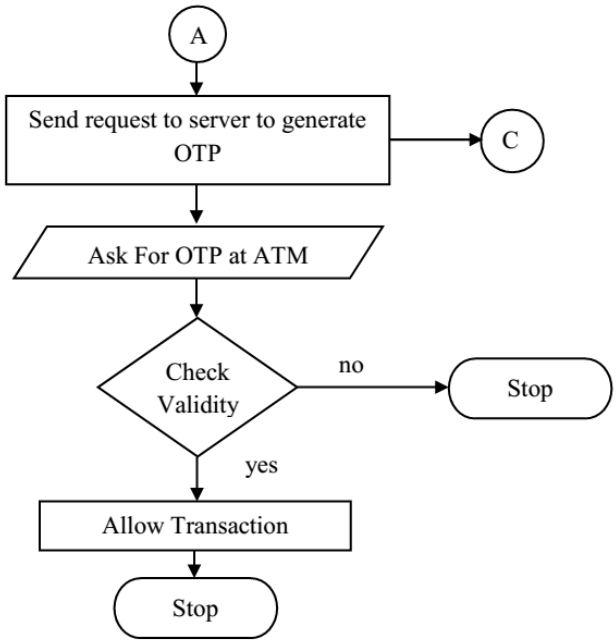
1. Mobile number of the user should be present in the system which is necessary for this particular project.
2. Database of biometric system should be maintained.
3. While opening an account bank should get fingerprint information of the user.
4. One biometric (fingerprint scanner) should be attached on ATM machine so that it can scan current fingerprint at the time of authentication.
5. Bank should have a fast and trusted SMS gateway to deliver OTP on customer's mobile number.
6. New System should be explained to customer so that while accessing ATM he/she should not face any difficulties or problems.

Flow chart of the proposed system:

Flow chart 1: User Enters into ATM and Selects one option among OTP or Fingerprint after Entering ATM PIN.

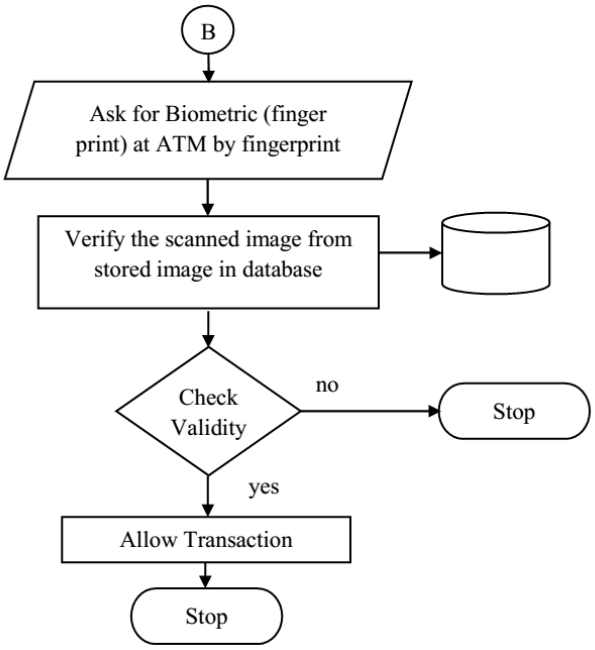


Flow chart 2: If user selects OTP option on screen.

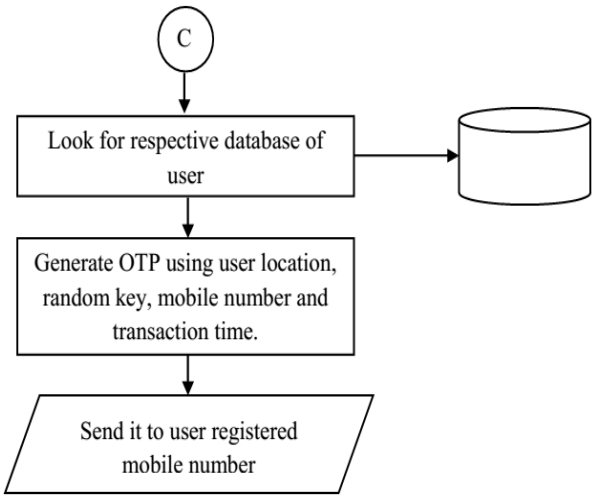


Flow chart 3: If user selects Biometric option on ATM screen.

 ISSN: 2321-8169
2041 - 2044



Flow chart 4: When user selects OTP, flow chart of OTP generation and sending on mobile number regisred on that record.



IV. Conclusion and Future Work

This project is developed on the basis of more need of security in ATM banking system. Now-a-day's ATM is getting less secure with emerging ways to hack/crack ATM PIN or ATM card. Use of OTP and Biometric is best and easy way to deal with these security threats. This project is using SHA-1 algorithm to generate OTP with more randomness provided in proposed system after generation of SHA-1 hash string. That OTP will be sending on registered mobile number of the user. And that OTP will be used to access ATM transactions. If User wants to use Fingerprint system, he/she can select that option on the screen and can get access. If he/she is legitimate user of ATM.

Another important point in proposed system is that it demands lesser changes to the present system of Bank and ATM. That means lesser overhead will be required to change the whole system with enhanced security. Changes in Hardware part will be required that is one fingerprint scanner is required to be attached to ATM machines. This project will needs to explained to end user, to educate the user to use this system.

In future work this project can use enhanced and more accurate equipments with better algorithms. More efficient biometric methods can be used like iris scanner, voice recognition etc.Latest algorithms like SHA-3 can be used to generate OTPs.

References

[1] European atmsecurity [Online]. Available: https://www.european-atm-security.eu/atm-industry. [Accessed: 12 Nov 2014].
[2] Kristin s. Fuglerud and Oystein dale "Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client" IEEE J. Security & Privacy,Volume: 9, Issue: 2, Pages 27-34, March-April 2011.
[3] N. Haller, C. Metz, P. Nesser, One-Time Password System, RFC 2289, February 1998.
[4] Aastha Bhargava, Priya Jain "Biometric; an Effective Shield in Today's Scenario" RGPV International Conference on Cloud, Big Data and Trust 2013, Nov 13-15.
[5] Secure Hash Standard (SHS), FIBS PUB180-4, March 2012.
[6] D. Eastlake, P. Jones. A US Secure Hash Algorithm 1 (SHA1), RFC 3174, September 2001.