

Secure ATM Activities and Pin Recovery by Fingerprint Recognition

Manishkumar

ABSTRACT

Automated Teller Machine i.e. ATM is a device through which one can do banking activities even when there is no human teller, through ATMs banking activities are made easy one can do transaction any time, transactions of ATM are made available 24*7. The user recognition in an ATM machine is done by inserting ATM card in machine and entering the authenticated ATM pin received by the person from Bank, if the entered pin is correct money is withdrawn or the transaction is done if the pin is incorrect then again it is asked by the machine to enter the pin this step is repeated for three times if after this three try a person is still not able to enter the correct pin then the card gets block because of security reasons and the person now have to go to the bank for card activation and have to perform all the norm of banks which is quite time taking and complex, therefore there is a need for fingerprint recognition as everyone have unique fingerprint so there is no such chance of fraud. In this paper fingerprint recognition is being used for reactivation of ATM card in ATM center.

Keywords:- ATM, SURF algorithm.

1. INTRODUCTION

In automatic teller machine transaction pin based authentication is applied, as for security purpose it is very important but there exists problems like shoulder – surfing attacks, duplicate cards, pin sharing therefore many works have been done and researches are going on to develop transactions without using cards. These development includes the use of personal devices like cell phone to perform money transactions. Observation attack i.e. shoulder surfing attack is the most common problem or threat of ATM authentication and its rapidly increasing year after year the attacker just had the observation of the personal entry of the verified user and thus can perform fraud operations, the attacker might be standing in a queue just after the real or authenticated person and notice all the detail of the person and perform the attack, fixing of cameras for pin noticing etc can be done a little bit of carelessness can make a person lose all his earnings not only this there are many other problems also like duplicate card use, terminal faking etc which makes user security a bit difficult.

To get users card information one can also attach card skimming device to it. As the users slide their card in ATM slots the card information is taken in the skimming device this device is fit in the atm slot. Thus transfer of money through mobile phones by having a pin is a bit secure in comparison to this ATM transactions, although if a person is unable to put correct pin even after three attempts in ATM machine then the card is blocked by reactivating it takes time and effort.

2. OBJECTIVES

As already discussed in the introduction that the use of ATM card is a bit unsecure because if anyone gets to know the card details or pin then that person is able to take out all the earning of the authenticated ATM user, and there are many fraud people in this world whom are just waiting to do such kind of tasks by performing shoulder surfing or duplicate card methods etc. Even there is a problem that if the verified person is not able to memorize his/her ATM pin then that person gets only three attempts for his operation if after three attempts also the person is unable to enter the correct code then the card gets blocked and the person have to perform bank norms to get the

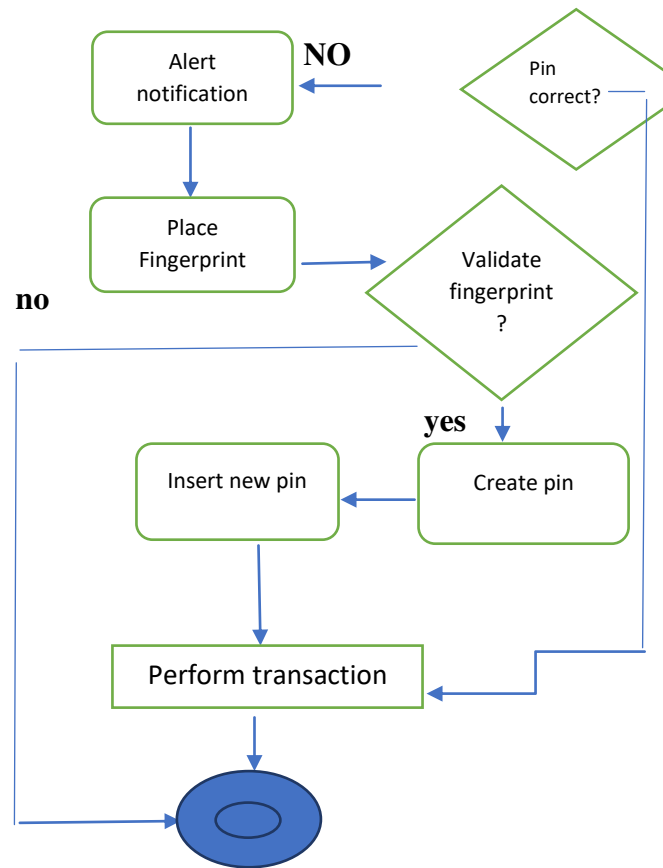
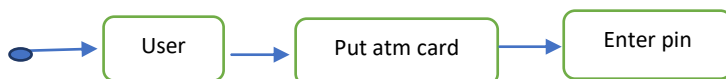
card reactivated back which requires time and effort. So, the objective here are following:

- Reactivating the ATM card of authenticated user by fingerprint recognition, at the ATM center itself.
- If the card is being misused the verified user will get notification about it.
- Avoiding the user to perform the norms of Bank for ATM card reactivation.

3. Methodology

Fingerprint recognition is the basis of identification of the ATM user and this is the proposed method here, as after entering incorrect pin of the ATM card continuously for three times the ATM card gets blocked and now the authenticated person have to perform all the norms of bank for its reactivation and these process demands time and attention so here if a user enters an incorrect pin for more than three times then a alert notification is send to the registered mobile number of the authenticated user and also a display box will be opened with a message saying “Kindly give your fingerprint to reset your password as more than three attempts have been made for your transaction”. The person gives his/her fingerprint and if the fingerprint matches from that of the authenticated persons fingerprint then the a pin reset dialog box will appear in the ATM window and the person will be able to reset the password and complete the transaction with the new pin created by him/her.

Diagram 1 represents the proposed model.



4. Fingerprint Verification algorithm.

Insert: Fingerprint picture.

Output: Keypoint detection.

1. Inserted picture is transformed to greyscale picture and afterwards to binary picture.
2. A framework picture is acquired.
3. Keypoints of fingerprint is identified by Harris corner detection algorithm and SURF algorithm is used.

4. Fingerprints are matched using key points.

5. Results

The proposed model gave a overview of difficulties or problems faced by a user when their atm card gets blocked , security issues are also there. Thus the provided model is able to deal with the security issue as it sends the authenticated user a alert message regarding the

incorrect pin entered after the provided three attempts, also its been shown that a real time biometric verification can be implemented in ATM center, such that the user can get a new ATM pin without performing any norms of Banks which are way too time taking and tedious.

6.Future Scope

If ATM cards are being misused bank should block the card after getting notified from the authenticated user, more security can be provided in ATM machine. Customer issue services can be enhanced, people should be taught more about how to use ATM machine. Machine should be made more easy to use.

7. Conclusion

Using ATM cards by PIN- based authentication entry is a bit less secure and attack prone like observation attack can be done, duplicate ATM cards can be made etc . So, there is a need for transactions through Mobile phones , that is online transactions also doing transaction

through ATM card and forgetting the pin and entering wrong pin for more than three times block the card and afterwards one have to perform all the works to reactivate it so, here it can be done just by matching the fingerprint , if it matches one can get there new pin and perform the desired transaction also a alert message is being sent to the authenticated person after three false try. Thus making the transaction more secure and personal.

8.References

1. [G. Stanley, Card less financial transaction April 21, 2014,US Patent App.14/588,257.]
2. [Sai Venupradhap , Sivakumar, Gajjala Ashok, Design and Implementation of Security based ATM theft Monitoring System, International journal of Engineering Inventions, Vol 3,2013]
- 3.[N.sethi, A.Gera , A revived survey of various credit card fraud detection techniques, International journal of computer science and Mobile computing,Vol.3,no.4,pp.780-791,April-2014]