International Journal of Engineering Innovation & Research
Volume 2, Issue 2, ISSN: 2277 – 5668

Enhancement of Auto Teller Machine Security Using Pressurized/Safe Mode Login Pin2 Security Model

Navneet Sharma, Dr. Vijay Singh Rathore

Abstract - **Auto teller Machine is a revolutionary invention in banking sector. Which perform the financial operations 24X7 without any interaction of banking official outside the bank premises the main object of ATM machines to keep safeguard of money and provide availability of cash very fast, it is very useful and convenient If there is an authorized user operates the machine, but if any unauthorized user it may be an attacker or a thief or robber or any pressurized operation then this type of attacks on machine make the transaction vulnerable from authorized access. To protect the machine with these types of vulnerabilities we need some security system by which we can make the ATM more secure. ATMs offer the advantage of 24-hour access, but this advantage can be undone if customers do not feel secure when using the facilities. Most banks rely on surveillance and security systems to provide round-the-clock protection for ATM users. In this paper we have mentioned a security model which may use to enhance the physical security of ATM from pressurized login attacks or external attacks on ATM and its user.**

Keywords - **Auto Teller Machine, Pressurized Login, Physical Attack, Safe Mode Operations.**

I. Introduction

ATM crime has become a nationwide issue that faces not solely customers, however conjointly bank operators. Security measures at banks will play an essential, conducive role in preventing attacks on customers. In our research findings ATM is more vulnerable from physical attacks .in our research analysis we found that ATM security in existing system is not sufficient. Mostly ATMs are authenticating their users on single PIN, if it is entered correctly by anyone than it allows to making transaction. Now the problem is if the user is not genuine and if user is genuine and making transaction in some external attacker's pressure than this type of security is not sufficient. To prevent the ATM operations with these type of attacks and pressurized login we proposed a new security model, which will prevent the user with direct physical attack on user and prevent from pressurized login and protect the ATM an currency with robbery or tampering with the machine.

In current scenario in India there is a single PIN authentication for ATM user, when we enter the PIN from keypad card reader reads the PIN, verifies it with magnetic strip which is available on ATM card, if the PIN is correct then ATM allows the user to make transaction from the ATM.

II. Existing Security and Working Process of ATM Operations

In the existing security model ATM verifies the user on a 4 digit single PIN verification, if the PIN entered by the user and PIN stored on card or bank database matches than ATM permits to make transactions from it and user can process ATM for various operations i.e. cash withdrawal, mini statement etc. if user enters wrong PIN three times card confiscated by the ATM. This single PIN verification used in existing model in almost all the banks in India.

The working process of ATM card authentication and validation is the first step where user enters the card in ATM and card reader reads the PIN and Account number from the card and reset the PIN count to 0 than user enters the 4 digit PIN with keypad ,if PIN matches with card PIN it permits to process further operations onto the ATM ,if it not matches than it set the pin count with incremented value of 1 and ask to reenter the PIN, if user enters wrong PIN three times card confiscated by the ATM.

III. Limitation with Existing Model

In current scenario all the existing ATM models are working on single PIN verification process. Now in new generation ATMs some biometric verification (finger print, retinal etc.) are implementing for verification. As per vulnerability analysis if our study there is a major vulnerability found with physical attacks or some pressurized withdrawal from ATM where the authorized user is making transactions under the pressure of attackers on gun point or some other pressure of attacker who is standing outside the ATM or with the near the user and demand for the money from him by making transaction from the ATM by saying him to login onto ATM. The limitation with existing system of ATM transaction is that it verifies the user with single PIN verification and user enters the correct PIN under the attackers or criminal's pressure and ATM dispense the money for him as he enter the correct PIN and with existing system user is authorized as per the bank. He may be looted by the attacker and this is the major vulnerability with this system .The limitation with this type of verification is there is no security for this type of fraud which may generated by the attacker. secondly banks says that to inform the police user can enter their PIN in reverse order for this type of attack to bring in notice of police but practically it is not implemented in current system.

IV. Problem with 4 digits Palindrome PIN Numbers

It is a logical problem to begin with the banking industry to be faced with a problem of reengineering the pin number system. There are many combinations of four digit PINs which are palindrome. That is, numbers of the form 1221 or 6666 or 4224 etc. However, these types of numbers cannot be used as reverse numbers for disaster management. Now the problem is remain exist for pressurized logins. Here we have tried to eliminate this type of problem in our proposed security model.

V. Proposed Security Model

As the above mentioned physical vulnerability with pressurized login and transaction and a logical problem with reverse PIN entry scheme provided by the bank for disaster management here we are proposing a new security model which will eliminate this type of problem. In our proposed security model we are using two PINs for same user instead of single PIN .In this case bank will assign two ATM PINs for same account holder. One is the **Normal Mode Login operations**, which will use in normal type transactions and second is for **pressurized login**. In this model we are representing it with **Safe Mode/Pressurized Login** which will use by the user for disaster management in abnormal conditions. Using safe mode login we can prevent the ATM with unauthorized user or pressurized login and safe the genuine user from the attacker in case of physical attack on user. In our proposed security model where in both the PINs are verified by the bank to identify the user if it is a Normal Login user or Pressurized Login user with some attacker. If it is a normal mode login than ATM will process the operation in normal way as it is working .If the user is in pressure from some external attackers or robbers who are creating pressure on the user to make transaction from the ATM for them then the user can use second type of login which is mentioned in our proposed model as Safe Mode PIN. User can use the second PIN (Safe Mode Login) given to the user from the bank and can use it at the time of pressurized login or disaster management.

The process of our proposed model is described in below given flow chart Figure:1, there are two PINs are described one is for normal operation (Normal PIN) and second is pressurized login or safe mode login (Safe Mode PIN). If it is a normal mode PIN than the ATM will work in normal condition but if it is a safe mode PIN entered by the user than user is in some problem or in pressure of external attacker or robber who is pressurizing the user to make transaction from the ATM .in this situation user can use the **Safe Mode PIN** for disaster management and protect his account and himself physically from the attacker. When user enters the Safe Mode PIN than ATM will activate in high alert mode and start the high alert processing on ATM. Steps for safe mode/pressurized login processing are given below:

Step1: It will start the camera 3 and camera 4 both which are hidden cameras, as camera 1 is inside the ATM which records the normal transactions and camera 2 is CCTV camera situated in ATM kiosk works in normal conditions. Camera 3 and 4 will only activate in safe mode transactions. camera 3 is the hidden camera inside the ATM with high resolution night vision effect will activate and start recording of all operation and at the same time display it live in bank control room with high alert signal may be some hazard signals displaying the location and ATM ID etc. and alarm1 will ring at same time in bank control room so banking officials can manage the abnormal situations.

Step 2: Camera 4 which is a hidden camera situated inside the kiosk facing in front of gate with moving camera and covering location of gate and kiosk both will also be activate and start recording of safe mode operation and at the same time display it live in nearest police control room with high alert signal may be some hazard signals displaying the location and ATM ID etc. and alarm2 will ring at same time in police station so that law enforcement officers take the necessary actions in emergency conditions and manage the abnormal situation.

Step 3: to protect the user account from pressurized transactions ATM will process one more thing that is it will create a temporary fake account balance only for displaying the account balance with Rs. 2000. And will process the transaction only for this much of account, so that the actual amount will not be shown and withdrawal only a minimum amount from ATM. It may protect the user for safer side as the attacker will not get angry due to less amount withdrawal and user can protect from him with physical attack at that time. With the help of our proposed security model law enforcement officer can trace the situation on camera and protect the user, ATM and account balance from this type of physical attack manage the disaster at that type of situation.

VI. Implementation of Proposed Security Model

We have implemented the generalized security model which works on two types of PINs (Normal Mode and Safe Mode).This is the generalized model implemented for normal mode and safe mode both login types processing to implement the process and enhance the security of ATM for disaster management which is mentioned in our security model.

To implement the security model we are using an interface designed in C# with SQL server database management system for cared data base and implement a working model with a new safety protocol to protect the pressurized login users and their bank amount with attackers and physical attacks.

VII. Security Model for ATM

Here in figure 1 the interface is defined for ATM processing. In this interface there are two input boxes which will take card number and PIN as an input from the user. Than it verifies the card number and PIN with ATM or bank database for user authentication .if both matches with bank database than it process normal operations and display normal mode as symbolic message in right side displayed action box.

If user enters the card number and safe mode PIN in input box than it will activate the safe mode alert camera 3 and 4 will activate and start the recording and live recording will display on both bank control room and nearest police station where camera connected with wireless connection and at the same time both alarms will ring on both places. Which are indicated in this interface with two separate symbolic boxes police station and control room and two bars symbolic to alarm1 and 2 bank control room and police station both. Safe mode operations in mentioned in figure 3, where the high alert with safe mode operation is symbolically displayed in red color.

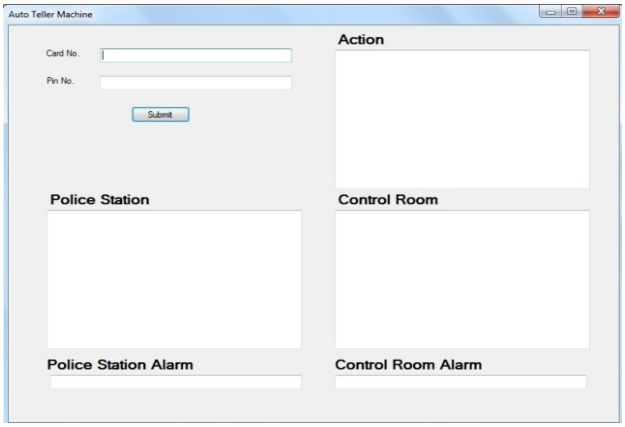


Fig.1. Interfaces for Proposed ATM Security Model

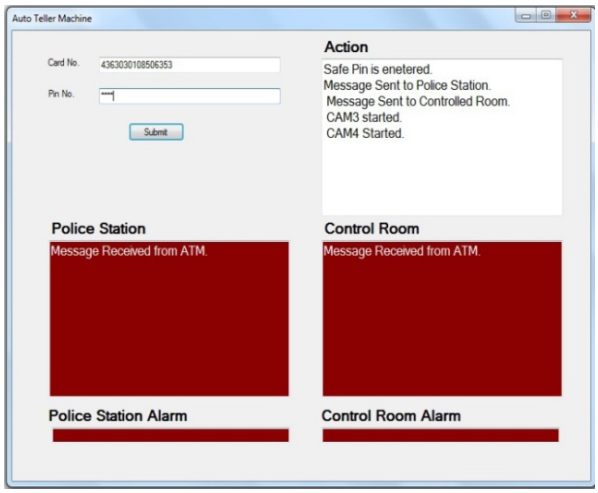


Fig.2. Interface output after using Safe Mode/pressurized PIN and its action

In figure 2 the action displayed after using Safe Mode PIN. This protocol will verify the PIN with Bank Database and start the related actions displayed in interface for Safe Mode Login as symbolic message of action in action box as it is shown in the figure 2.

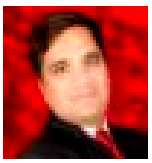
This is a symbolic program implemented for testing the security model and we can further implement it with actual operation with the permission of concern authorities and related bank.

VIII. Conclusion

This research paper is a practical research work based on the research on different vulnerabilities and security issues on Auto Teller machine. Having looked at the research findings in our research study we found that ATMs are more vulnerable from physical attacks and using our proposed security model we have tried to overcome the vulnerability related to physical attacks. It is the invention of this research to make recommendations that we can enhance the security of ATM and its uses through banks with implementation of our proposed security model for ATM and its users security. This should be implemented with ATM system to protect the users and ATM itself with pressurized login and physical attack.

Author's Profile

Navneet Sharma
Research Scholar
Dept. of Computer Science and Engineering
Suresh Gyan Vihar University, Jaipur. Rajasthan , India
E-mail:navneetsharma1977@gmail.com



Dr. Vijay Singh Rathore
(Professor) Director
Shri karni College, Jaipur, Rajasthan, India
E-mail: vijaydiamond@gmail.com