CHAPTER –5

ENHANCING SECURITY

FEATURES OF ATM

5.1 SECURITY FEATURES OF ATM

The Automated teller machines have gained popularity worldwide and been accepted as easy and dependable mode for conducting financial transactions, but its creditability is being eroded due to vulnerability it is facing. Automated teller machines are put at places frequented by large number during day time, business hour and or evening hours. but the places may become an isolated/deserted place with advancement of night, Automated teller machine not only face physical risk to its security but also Automated teller machine the users face the security risks and therefore problem has to be tackled though new inventions of technology, technology which has to functional without any human presence at the place of installations of the Automated teller machine by having arrangement to activate the signals at bank and police stations if there is danger inside the Automated teller machine.

Another problem widely and increasingly faced by user of Automated teller machine is vulnerability of four digit pass word or PIN number of ATM card for financial transaction. There is need for password mechanism for the transactions by Automated teller machine to be strengthened. There can be combination of digital password or PIN number with biometric parameters of the users, matter has already been dealt in this project. In this chapter we shall deal with security of Automated teller machine by installations of different alarm system within
Automated teller machine housing and strengthening of pass word or PIN from the existing functional system working of present day Automated teller machine in order to the keep benefit of Automated teller machine intact to continue with the gains of financial operations 24X7 without any interaction of banking official outside the bank premises and without considerations of banking hour or strikes in the bank. Since the Automated teller machine working outside the bank on 24X7 basis and delivers the direct currency for transactions, so it has become very useful and convenient except when authorized user operating the Automated teller machine is attacked, an attacker or a thief or robber or user brings an ATM card holder into Automated teller machine housing and pressurizes the card holder to make transactions and hand over the money withdrawn to the attacker. Another ways of common defrauding through Automated teller machine as has been explained the preceding chapter is obtaining ATM card in any way or including creation of a cloned or duplicate ATM card and withdrawing money after having access over the PIN of ATM card.

To protect the machine with these types of vulnerabilities, we need to install some security system so that the Automated teller machine becomes more secure and the user making transactions over Automated teller machine feels sense of security. Automated teller machines offer the advantage of 24-hour access, but this advantage shall not remain intact if customers do not feel secure when using the facilities. Many banks outside India rely on surveillance and security systems to provide round-the-clock protection for Automated teller machines users by installing some type of alarm mechanism. The Automated teller machine surveillance system can use a thermal sensor, humidity sensor, and video camera recording the activity in Automated teller machines premises. In existing system there are so many security features and so many arrangements are available which are discussed in previous chapters but still there are some vulnerabilities exists in Automated teller machine and it need new securities for high security system.
On study of the Automated teller machines security in previous chapters we found that Automated teller machines are more vulnerable from physical attacks than by any unauthorized transactions by gaining access of users’ account and process the transaction from his/her account by ram raiding, skimming, shoulder surfing, safe card cloning, trapping etc al well physical vulnerabilities viz cutting, bombing, any attacker waiting inside or outside an Automated teller machines housing. As the Automated teller machine are mostly installed outside the bank premises and activate alarm in case thin human presence hour attacks or robbery or pressurized login are high in considerations.

To prevent the Automated teller machine operations with 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 Automated teller machine a currency with robbery or tampering with the machine.

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

5.2 EXISTING SECURITY AND WORKING PROCESS OF ATM:

Here we are explaining the working process of ATM card authentication and validation process has illustrated at flow chart figure 5.1 in this chapter. In this flow chart the step by step working of PIN validation mentioned in well explanatory. The first step is user enters the card in Automated teller machine and card reader reads the PIN and Account number from the ATM card and reset the PIN count to 0 then user enters the 4 digit PIN with keypad. On matching of PIN with card with PIN entered through key, it permits to process further operations from Automated teller machine. If the entered PIN do not match than it sets the pin count with incremented value of 1 and ask to re-enter the PIN, on entering wrong PIN three times card gets confiscated by the Automated teller machine and/or the account is blocked.
In this existing security model Automated teller machines 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 then only Automated teller machine permits to make transactions for its user and user can process Automated teller machine for various operations i.e. cash withdrawal, mini statement etc. Some client using ATM card may not confident be PIN number for having forgotten PIN number, fraud may have acquired the knowledge individual digits comprises the PIN but not exact sequence of digits in PIN number and enters wrong PIN thrice in continuation, ATM card gets confiscated by the Automated teller machines wherein ATM card is inserted and incase wherein ATM cards is required to be swiped account related account is blocked or rendered dormant. The single PIN verification is used in existing model in almost all the banks in India.

**CHART OF PIN VERIFICATION**

![Flow chart of pin validation process](image)

*Figure 5.1 flow chart of pin validation process*
LIMITATION WITH EXISTING MODEL OF ATMs:

In current scenario all the existing Automated teller machines models in India are working on single PIN verification process. Now in new generation Automated teller machines authentications are carried by some biometric parameters viz finger print, retinal etc. for implementing verification of the user are still to be introduced in India. Though biometric authentications are far more safe than digital Automated teller machines’ ATM card reader as authentications is carried out by physical parameter of the user i.e. biometric of the user, but even this safeguard of vulnerability analysis is inadequate as our study indicate when vulnerability is physical attacks or some pressurized withdrawal from Automated teller machine i.e. forced is used to make transactions under the pressure by attackers knife point, gun point or some other pressure of attacker who is standing outside the Automated teller machines or with the near the user and demand for the money from him by making transaction from the Automated teller machine by demanding that he must have to login onto Automated teller machines. The limitation with existing system of Automated teller machines 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 withdraw the money from Automated teller machines for criminal by entering the correct PIN. He may be looted by the attacker and this is the major vulnerability with this system. Secondly banks says that user in order to inform the police user should 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.

5.3 PROBLEM WITH 4 DIGITS PALINDROME PIN NUMBERS:

It is 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 manner to avoid disaster. Now the problem is remain without being
solved for pressurized logins. Here we have tried to eliminate these types of problem in our proposed security model.

**STRENGTHENING OF PASS WORD**

The ATM cards are used not only for transactions at Automated teller machines but also at POS (point of sale) either by swiping of card through a card reader device and connected to the bank network or through e-network. E-network transactions or e-business have the system of strengthened pass words. The strengthening of pass word can be caused by having pass words consisting of more than four characters. Characters mean it may be numerical digits, or alphabets or specific symbols. Since these characters are options of more than mere numerical digits, the pass words are strengthened and in order to strengthen additionally, pass words must consists of mixed characters i.e. if numerical are used at least one of the character should be alphabet or vice versa. In recent strengthening of pass word for e-network, many banking/financial institutions have mandatory that one at least one of the character must be special symbol. This system can also be adopted in Automated teller machine technology to strengthen the pass word. The adoption shall require modification of Key pad of the Automated teller machine to have alphabets and special characters in addition to numerical digits only.

Another process of strengthening already developed to strengthen the pass word is One Time Password known as OTP, this has strengthened system also on four characters which is being used by the present Automated teller machine as 4 digit passwords.

**5.4 OTP-ONE TIME PASS WORD:**

One time pass word has been developed by Gemplus on the EAP-SIM authentication protocol and is in practice since 2004 by reassigning to work with a team of Verisign on a new authentication method: OTP or One Time Password. At this time, the existing one time password was a token from RSA that was using a clock to synchronize the passwords. The lab of
Versign came with a very simple but one should say very smart concept. The OTP that we may be using with your bank or Google was born. This is this algorithm and authentication method, describe in the following articles. In this article, a complete code of the OTP generator has been presented. It is very similar to the Javacard Applet used since 2004 when concept OTP started with the Versign labs.

THE ONE TIME PASSWORD GENERATOR

The OTP is based on the very popular algorithm HMAC SHA. The HMAC SHA is an algorithm generally used to perform authentication by challenge response. It is not an encryption algorithm but a hashing algorithm that transforms a set of bytes to another set of bytes. This algorithm is not reversible which means that you cannot use the result to go back to the source.

A HMAC SHA uses a key to transform an input array of bytes. The key is the secret that must never be accessible to a hacker and the input is the challenge. This means that OTP is a challenge response authentication. The secret key must be 20 bytes at least; the challenge is usually a counter of 8 bytes which leaves quite some time before the value is exhausted.

The algorithm takes the 20 bytes key and the 8 bytes counter to create a 8 digits number. This means that there will obviously be duplicates during the life time of the OTP generator but this doesn’t matter as no duplicate can occur consecutively and an OTP is only valid for a couple of minutes.

THE OTP’S VERY STRONG AUTHENTICATION METHOD:

There are few reasons why this is a very strong method.

The key is 20 digits

A password is a couple counter/password, only valid once and a very short time
The algorithm that generates each password is not reversible

With an OTP token, the key is hardware protected

If the OTP is received on your phone, the key always stays at the server

Those few characteristics make the OTP a strong authentication protocol. The weakness in an authentication is usually the human factor. It is difficult to remember many complex passwords, so users often use the same one all across the internet and not really a strong one. With an OTP, one doesn’t have to remember a password, the most you would have to remember would be PIN code (4 to 8 digits) if the OTP token is PIN protected. In the case of an OTP sent by a mobile phone, it is protected by mobile phone security. A PIN is short but you can’t generally try it more than 3 times before the token is locked.

The weakness of an OTP if there is one, is the media used to generate or receive the OTP. If the user loses it, then the authentication could be compromised. A possible solution would be to protect this device with a biometric credential, making it virtually totally safe.

THE CODE OF THE OTP GENERATOR FOLLOWS:

```csharp
public class OTP
{

    public const int SECRET_LENGTH = 20;

    private const string
        MSG_SECRETLENGTH = "Secret must be at least 20 bytes",
        MSG_COUNTER_MINVALUE = "Counter min value is 1";

    public OTP()
    {
    
```
private static int[] dd = new int[10] { 0, 2, 4, 6, 8, 1, 3, 5, 7, 9 }; 
private byte[] secretKey = new byte[SECRET_LENGTH] 
{ 
    0x30, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x39, 
    0x3A, 0x3B, 0x3C, 0x3D, 0x3E, 0x3F, 0x40, 0x41, 0x42, 0x43 
};
private ulong counter = 0x0000000000000001; 
private static int checksum(int Code_Digits) 
{ 
    int d1 = (Code_Digits/1000000) % 10; 
    int d2 = (Code_Digits/100000) % 10;  
    int d3 = (Code_Digits/100000) % 10; 
    int d4 = (Code_Digits/10000) % 10; 
    int d5 = (Code_Digits/1000) % 10; 
    int d6 = (Code_Digits/100) % 10; 
    int d7 = Code_Digits % 10; 
    return (10 - ((dd[d1]+d2+dd[d3]+d4+dd[d5]+d6+dd[d7]) % 10)) % 10; 
} 

///<summary>
/// Formats the OTP. This is the OTP algorithm.

/// </summary>

/// <param name="hmac">HMAC value</param>

/// <returns>8 digits OTP</returns>

private static string FormatOTP(byte[] hmac)
{
    int offset = hmac[19] & 0xf;
    int bin_code = (hmac[offset] & 0x7f) << 24
        | (hmac[offset + 1] & 0xff) << 16
        | (hmac[offset + 2] & 0xff) << 8
        | (hmac[offset + 3] & 0xff);
    int Code_Digits = bin_code % 10000000;
    int csum = checksum(Code_Digits);
    int OTP = Code_Digits * 10 + csum;
    return string.Format("{0:d08}", OTP);
}

public byte[] CounterArray
{
    get
    {
        // Code here
    }
}
return BitConverter.GetBytes(counter);

public byte[] Secret
{
    set
    {
        if (value.Length < SECRET_LENGTH)
        {
            throw new Exception(MSG_SECRETLENGTH);
        }
        secretKey = value;
    }
}
}  

///<summary>  
/// Gets the current OTP value  
///</summary>  

///<returns>8 digits OTP</returns>  

public string GetCurrentOTP()  
{
    HmacSha1 hmacSha1 = new HmacSha1();
    hmacSha1.Init(secretKey);
    hmacSha1.Update(CounterArray);
    byte[] hmac_result = hmacSha1.Final();
    return FormatOTP(hmac_result);  
}

///<summary>  
/// Gets the next OTP value  
///</summary>  

///<returns>8 digits OTP</returns>  

public string GetNextOTP()  
{
    // increment the counter
The attached code also contains an implementation of the HMAC SHA algorithm. It is of course possible to use the standard hmacsha of the NET Framework but the code I provide in fact used a demo in a prototype of smart card that was running a .NET CLR. At the time I wrote this code, the cryptography namespace was not yet implemented by the card.
THE OTP SERVER AND AUTHENTICATION PROTOCOL:

Usually there are 2 ways to perform an authentication with an OTP and describes the real case of an authentication to an online banking site and is explicit with something. You cannot use what I’m going to describe in this post to hack into a banking site! On the contrary after reading this you should understand why using an OTP as a second factor authentication is extremely secure.

The OTP by itself is already very secure for at least the 2 following reasons:

It can’t be played twice

One can’t go back to the source.

The second characteristic is very important in term of security. An OTP depends on 2 parameters:

A secret key

A counter

Even if a hacker intercepts millions of OTP the algorithm is not reversible which means that even if you know the key you can’t go back to the counter that was used to generate the OTP. So without the key and the counter, it is virtually impossible even with millions of OTP to find a pattern to guess the key and the current counter value.

Like many security protocols, the strength of the OTP is given by the quality of the cryptography algorithm used, in this case HMACSHA1 which is a proven challenge response algorithm. Another HMAC algorithm can be used in place of HMACSHA as encryption algorithms have to become stronger when CPU power is increasing. This can be done by increasing the size of the key or by redesigning the algorithm itself.
OTP are usually used to perform authentication or to verify a transaction with a credit card. In the case of a transaction an OTP is sent to the mobile phone of the user, for an authentication if is possible to use either a secure token or to request an OTP to be send to the user phone.

**USING AN OTP SENT TO A PHONE:**

This is usually the authentication method used when a transaction is verified with an OTP. The bank system sends the user an OTP and the user then have few minutes to enter this OTP. This mechanism doesn’t need any synchronization process as the OTP is originally generated by the server and send to a third party device. The server expects that user to type the correct OTP within generally 2 minutes. If user fails to do it, user can just ask a new OTP and then enter it within the given time. When a system supports both authentication methods, it means that the back-end has 2 different keys and counters; one pair for the OTP token and one pair for the OTP transmitted by SMS.

**OTP TOKEN:**

The original product works on when implemented in one of the first versions of the OTP in a Javacard was using an OTP token with a screen or a mobile phone with a card applet to generate the OTP. In this model both the server and the authentication token have to generate an OTP that must be synchronized. The process is the following: The user generates an OTP with his token, type it and press OK. The server receives the OTP generated by the token, it increments the counter and generates a new OTP. This is where there is a possible synchronization issue.

**SYNCHRONIZATION ISSUES:**

If the user enters the correct OTP, then the server when it increments the counter and calculate the OTP, the authentication will be successful. Now there could be few scenarios that could lead to a desynchronization of the server counter and the authentication mechanism won’t
work. In some cases it could be possible to resynchronize automatically the counter but in some cases the user would have to resynchronize the server counter using a specific procedure.

Few scenarios of desynchronization could arise:

The user accidentally press the generate button of his token and doesn’t perform an authentication.

In this case the counter of the token would be ahead of the server counter by few steps.

The user enters an OTP without generating it from the token. In this case the counter of the server would be ahead of the token counter.

The user generates an OTP with the token but types a wrong OTP.

If the OTP given by the user doesn’t match the one of the server, the server can try to auto-resynchronize itself by trying few counters around the expected counter. In our server we would use 10 values around the nominal counter value. If the synchronization cannot be done, the server would retain the current counter value in order not desynchronize the server further.

However the server would have to implement a strategy to inform that the server and token are totally desynchronized and a manual synchronization must be performed.

5.5 PROPOSED TWO PIN MODEL:

Another option may be to adopt a two PIN System. 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. To implement this model banks shall have to take the permission from Reserve Bank.
In our proposal, the purposed security model should have two sets PINs for same user instead of single PIN i.e. bank will have to assign two ATM PINs for same user. 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 Automated teller machine to allow unauthorized user or pressurized login and safe the genuine user from the attacker in case of physical attack on user. Here we are mentioning the flow chart of Automated teller machine process bellow with new 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 user with some attacker. If it is a normal mode login then Automated teller machine 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 Automated teller machine for them then the user can use second type of login which is mentioned in our proposal is 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 for banks to take appropriate security steps once Safe Mode PIN has been used on an Automated teller machine.
Enhancing Security Features of ATM

START

Wait

Card inserted?

Yes → Read PIN & A/C no from card

No → Reset PIN count to 0

Input PIN from user

Use PIN & card PIN match?

Yes → Proceed to customer services

No → Reset PIN in safe mode

No → Maximum PIN count?

Yes → Confiscate the card

No → Activate cam3 Recording ON live to BCK and cam 4 Recording ON live to MFS, Ring All (BCE), Ring All2(MFS) Alarm2(MFS), set TempAcc Bal=2000
Figure 5.2 flow chart with safe mode login process
The process of our proposed model is described in below given flow chart Figure: 5.2 in addition to above given flow chart figure 5.1 there was a single PIN verification to identify or verify the user. Now in figure 5.2 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 then the Automated teller machine should function in normal pattern but as mentioned in figure 5.2 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 Automated teller machine. In this situation user can use the Safe Mode PIN for disaster management and protect his account and him physically from the attacker. When user enters the Safe Mode PIN than Automated teller machine will activate in high alert mode and start the high alert processing on Automated teller machine. Steps are given below:

**Step 1:** It will start the camera 3 and camera 4 both which are hidden cameras, as camera 1 is inside the Automated teller machine which records the normal transactions and camera 2 is CCTV camera situated in Automated teller machine kiosk works in normal conditions. Camera 3 and 4 will only activate in safe mode transactions. Camera 3 is the hidden camera inside the Automated teller machine 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 Automated teller machine identity i.e. its number and location etc. and alarm 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 Automated teller machine identity 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 Automated teller machine will process one more thing that is it will create a temporary fake account balance only for displaying the account balance with such a petty amount so that transaction cannot be made or if made is negligible amount. And will process the transaction only for this much of account and the actual amount will not be displayed on display screen of Automated teller machine. 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, Automated teller machine and account balance from this type of physical attack manage the disaster at that type of situation.

5.6 IMPLEMENTATION OF PROPOSED SECURITY MODEL:

As per the above mentioned flowchart we have implemented the working security model which works as per the steps mentioned in flow chart and algorithm both to identify the process of both type of logins (Normal Mode and Safe Mode). This is the simulator model implemented for normal mode and safe mode both login types processing to implement the process and enhance the security of Automated teller machine 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.
Here in Figure 5.3 the interface is defined for Automated teller machine processing. In this interface there are two input boxes which will take card number and PIN as an input from the user, then it verifies the ATM card number and PIN of the ATM card with Automated teller machine 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 5.4, where the high alert with safe mode operation is symbolically displayed in red color.
In Figure 5.4 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 5.4.

This is a symbolic program to be implemented for testing the security model and we can further implement it with actual operation with the permission of Reserve bank of India and concerned bank.

**DOES REVERSE ENTRTY OF PIN WORK:**

News had been circulating on the Internet in September 2006 that by making reverse entry on an Automated teller machine, alarms is raised at the bank and the nearest police station about transactions being carried out by a client under forced conditions. The Credit Card Accountability Responsibility and Disclosure Act of 2009 compelled the Federal Trade Commission to provide an analysis of any technology, either then currently available or under development, which would allow a distressed Automated teller machine user to send an electronic alert to a law
enforcement agency. The following statements were made in the FTC’s April 2010 report in response to that requirement:

FTC staff learned that emergency-PIN technologies have never been deployed at any Automated teller machines. The respondent banks reported that none of their Automated teller machines currently have installed, or have ever been installed, an emergency-PIN system of any sort. The leading Automated teller machine manufacturer Diebold confirms that, to its knowledge, no Automated teller machines have or have had an emergency-PIN system.

Ergo, there aren’t and haven’t ever been “reverse PIN” technologies despite Internet circulated claims dating to September 2006 that anyone being robbed at an ATM simply had to enter his or her PIN in reverse to summon help. Moreover, said that FTC report: The available information do suggest that emergency-PIN and alarm button devices: (1) may not halt or deter crimes to any significant extent; (2) may in some instances increase the danger to customers who are targeted by offenders and also lead to some false alarms (although the exact magnitude of these potential effects cannot be determined); and (3) may impose substantial implementation costs, although no formally derived cost estimates of implementing these technologies are currently available. There has been a reported instance, where ATM card user waited after escaping his captors on foot, the man who was carjacked by the Boston Marathon bombing suspects was forced at gunpoint to withdraw money from an Automated teller machine, having possessed the knowledge and presence of mind to enter his PIN in reverse, some believe, the machine would have automatically notified the police that he was doing so under duress and officers would have been dispatched. It seems that it is simply not true and pure bunk to recite your PIN backward. Such bad idea has become an urban legend worthy of a Snopes.com debunking is nowhere near as truth, however, the fact is that American Congress and multiple state legislatures have actually considered making it law.