JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING
ISSN: 0975 – 6760 | NOV 16 TO OCT 17 | Volume 4, Issue 2

SECUREING ATM TRANSACTION

[1] A.KHATPE [2] A.BHOSALE [3] A.KAMBLE [4] A.DESHMUKH

[1,2,3,4] Department of computer engineering,
Shri Chhatrapati Shivajiraje College of Engineering, Pune university,
Dhangawadi , Maharashtra, India.

[1] **Apk21395@gmail.com** [2] **bhosaleakshay.595@gmail.com** [3] **amol2184@gmail.com**
[4] **deshmukhanics@gmail.com**

ABSTRACT: *ATM contains multiple amount of cash and process sensitive customer data to perform cash transactions and banking operations. ATM become very important part of banking sector all over the world. As banks compete by opening more and more ATM's every year, the security of ATM becomes very important issue. In real time ATM the user authenticated only by four digit personal identification number (PIN) which can compromised easily. But now a days criminals mainly focused on physical attacks to gain access to cash inside an ATM's safe. They capture customer data on the magnetic stripe of an ATM card with skimming devices during insertion of cash or capture customer data. So to understand the risk that arise by attack we conducted risks assessment of ATM platform that is running in real banking. Our project proposes a secured ATM system using One Time Password (OTP) on mobile to improved security. Usual ATM systems do not contain the OTP feature for money withdrawal. System generates and sends a onetime password to the registered mobile number to that particular user. The password is generated and sends to the user mobile phone. This password is use to conduct next transaction. Using this concept if attacker clone the users card, he cannot use it because users pin is regenerated every time and send it to users phone number. So that attacker cannot gain access to users account. we can also use the concept of biometrics system in which we scan the user finger print and authenticate users identity using his finger print.*

***KEY WORDS** : Fingerprint, PIN, OTP, security, biometric, ATM.*

INTRODUCTION:

Banking technology is rapidly developing technology that change the way of banking activities. In banking technology ATM has some advantages and disadvantages on banking sector. With the help of ATM a customer is able to perform different banking transactions like cash withdrawals, paying phone and electricity bill, money transfer. ATM allows user to easily and fast to access their bank account and to perform financial operations. Personal identification number (PIN) or password is one of the important aspect in ATM security system. To prevent the unauthorized access to customer account the PIN is commonly used. It is computerised machine design to make transactions on cash without help of any human interaction and it allows to perform basic financial operations like mini statement, balance enquiry, withdrawal and fast cash transfer. The PIN is only way to authenticate the user in existing system. By using ATM scamming devices and video cameras these four digit pin can be easily compramised. Contain of magnetic tape can be read by the scamming devices and capture pin refer fig 1. Such a devices are card reader, video cameras and digital pads refer fig 2.

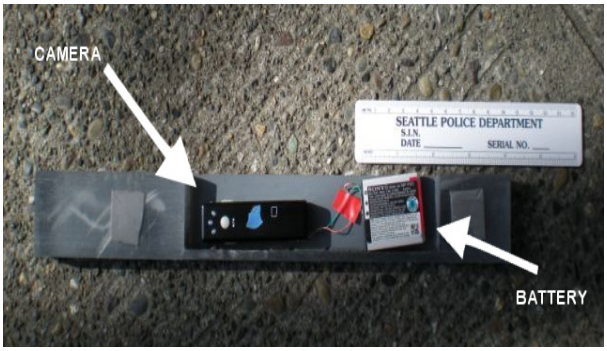

Fig 1: Camera

PIN can also access by shoulder surfing. By using this method attacker can obtain card information and create duplicate card easily. In this situation user is aware of card scamming and he/she face a financial risk and totally depend on the bank to block the card.

fig 2: Digital pads

SECURITY METHODS :

In this paper we provides the two methods for securing ATN transactions.

a. One Time Password (OTP)
b. Biometrics

a. One Time Password (OTP):

OTP concept is already used in online transactions. Usually ATM systems do not contain the OTP feature for money withdrawal. Our project proposes a secured ATM system using One Time Password (OTP) on mobile to improved security. in banking system when user create his account he register his personal mobile no. In the banking system when user create his account he register his personal mobile number. Banking system generates and sends a one time password to the registered mobile number to that particular user. The password is generated and sends to the user mobile phone. This password is use to make next transaction. Using this concept if attacker clone the users card, he cannot use it because users pin is regenerated every time and send it to users phone number. So that attacker cannot gain access to users ATM or account. In this system first password is provided by the bank with ATM card and when user used his ATM first time his password is change and system generate new password and send to user's mobile number, the new generated password used for next transaction. Every time when user use ATM card even only for balance enquiry system generate new password every time. System generate a 4 digit pin number in which one place digit randomly make blank instead of blank we use underscore(_) to known which place is blank for eg. _234, 1_34, 12_4, 123_ . The bank provide one fix number to customer and that number is permanent and only known to the customer. When the system regenerate password and send to customer, this password contains the one blank place on that blank place customer use that fix permanent number to gain the access to ATM. In some cases if user phone and ATM stoled by the attacker, then also attacker cannot use it because attacker cannot know the fix or permanent number of new generated pin's blank place. Some times in ruler areas if users phone is out of coverage area and he/she cannot get the new generated password then also he/she can make the two transactions, as he/she has one previous password already and bank provide emergency pin for one time use in emergency cases.

Advantages of OTP system

1. Better security than normal pin
2.Requried less cost to implementation
3.Strong and automatic password change
4.Can be reset once compromise

Disadvantages of OTP system

1.Single point of failure – multiples redundancy levels are needed.

b. Biometrics:

Biometrics can be defined as a measurable physiological and behavioural and behavioural characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioural characteristic. It is ameasure of an individual's unique physical or behavioural characteristics to recognize or authenticate its identity. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioural characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

Fingerprint Biometrics:

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. In the world today, fingerprint is one of the essentialvariables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used forcontrolling access to highly secured places like offices, equipment rooms, control centers and so on.

following reasons to the wide use and acceptability of fingerprints for enforcing or controlling security:

a. Fingerprints have a wide variation since no two people have identical prints.
b. There is high degree of consistency in fingerprints. A person's fingerprints may change in scale but not in relative appearance, which is not the case in other biometrics.
c. Fingerprints are left each time the finger contacts a surface.
d. Availability of small and inexpensive fingerprint capture devices.
e. Availability of fast computing hardware.
f. Availability of high recognition rate and speed devices that meet the needs of many applications
g. The explosive growth of network and Internet transactions
h. The heightened awareness of the need for ease-of-use as an essential component of reliable security.

The banking sector stores the customers finger print in database and set the finger print biometrics scanner on ATM machines. When customer want to perform ATM transaction after card swapping he/she can authenticate his finger print using scanner and then make transaction.

Advantages of Biometrics:

1. High level security
2.Cannot be forgotten or lost
3.Reduce operational cost

Disadvantages of Biometrics:

1. More costly.
2. Required more time to implement.
3.System are not 100% accurate.
4.Require additional hardware.
5. Cannot be reset once compromised.

Conclusion:

We have discussed various aspect of ATM security that is card clone and currency fraud. In this paper we proposed two different methods of securing ATM transaction that is OTP one time password and Biometrics for finger print reorganisation.

REFERENCES:

DrWeb, “Trojan.Skimer.18 infects ATMs,” DoctorWeb.[Online].Available:http://news.drweb.com/?i=4167&c=5&lng=en&p=0 [retrieved: 08, 2015].

S. Chafai, "Bank Fraud & ATM Security," InfoSecInstitute, 2012. [Online]. Available: http://resources.infosecinstitute.com/bank-fraud-atm-security/ [retrieved: 08, 2015].

F. A. Adesuyi, A. A. Solomon, Y. D. Robert, and O.I. Alabi, "A Survey of ATM Security Implementationwithin the Nigerian Banking Environment," J. Internet Bank. Commer., vol. 18, no. 1, 2013, pp. 1–16

Wikipedia the free encyclopaedia, "Biometrics", Downloaded March 20,2012 from http://en.wikipedia.org/wiki/Biometrics.

S.S, Das and J. Debbarma, "Designing a Biometric Strategy(Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System", International Journal of Information and CommunicationTechnology Research, vol.1, no. 5, pp.197-203, 2011.

Kjell.J. Hole, Veblorn Moen, Andre N. Klingsheim ,and Knut M. Tande , "Lessons from the Norwegian ATM system," IEEE Security and Privacy," vol. 5,no. 6, pp.25–31, 2007.

Lei Zhang, JiangchuanLiu ,Hongbo Jiang and YongGuan, "SensTrack: Energy-Efficient location Trackingwith Smartphone Sensors," IEEE Sensors Journal , vol.
13, no. 10, pp. 3375–3784, 2013.