International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Smart ATM Security Using Mobile Messaging

Deepak G. Deshekar

Department of Master of Computer Application
Panvel, Navi Mumbai, India
deepak.deshekar@gmail.com

Abstract -

Authentication may be a essential a part of any trustworthy computer system that ensures that, solely people will log on to the system .Here ATM Security has forever been one amongst the foremost outstanding problems. ATM machines typically authenticates by victimization ATM card and personal identification number to perform transactions In recent days completely different access management ways are planned to secure the ATM dealings from unauthorized access.

This papers gift the planning of ATM system which will improve the authentication of client where as victimization ATM. Here is feasible situation that associate degree individual's ATM card falling into wrong hands by knowing personal identification number.

This paper describes method of implementing2way authentication. The primary one is traditional PIN verification methodology. If the Arcanum is correct then it goes to the second step of authentication (i.e.,) two way authentication methodology. in this if the approved person replied YES through their mobile, then corresponding dealing stakes place. Otherwise card can will block.

I.INTRODUCTION

ATM's haven't solely modified the banking Perspective of the planet, however a general perspective as well. An automatic teller machine (ATM) could processes telecommunication device that gives the purchasers is ready to conduct several banking service like money withdrawal, deposit, and check book printing and cash transfer in different accounts in very public house while not interaction with bank workers.

Being a machine, it's vital that it authenticates the user when he/she applies for access to ATM Services. this is often typically done by the insertion of associate degree ATM card that contains a singular card variety and security data like a PIN number that is exclusive to each user.

The two way method authentications are several in use for money withdrawal in ATM. A number of the 2 way method authentication are using mobile as medium to involve second step of authentication. By using mobile Authentication Approval is second step

II. How Do ATMs Work?

ATM is communicating with central host processor by Internet Service supplier include a gateway where all ATM networks offered to user. Here ATM machine connected to the central host processor by telephone line or traditional phone line using modem. Once client desire to perform dealing offer PIN and ATM card. ATM machine forward to central host processor where as ATM request to the customer bank. If client request a money central host processor initiates electronic fund transfer from client bank to the ATM central host processor account. Once transfer compete to central host processor, it send approval code to ATM to dispense money.

But the authentication of ATM throughout transaction are unsecure as a result of with facilitate of just like original cards by replicas of ATM machine cards slot with integer magnetic reader. The reader

capture data embedded in the magnetic strip and store it. By placing small wireless cameras in ATM center to track the PIN to cash withdrawal. To beat this, I proposed using two way authentications using mobile messaging.

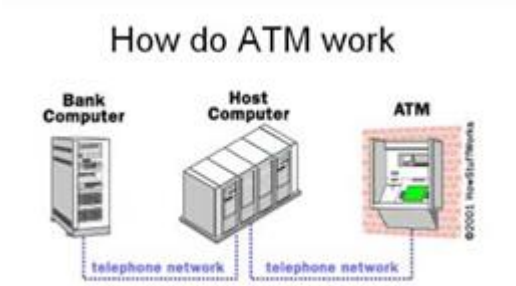

Figure 1:-Working of ATM(ref [01])

III. LITERATURE SURVEY

The idea behind to develop ATM was to back work of bank. In present ATM system to perform ATM transaction we must enter card and PIN details to verify authentication.

In case of losing ATM card/ forget ATM card chance to perform fraud rant ATM transaction. In present days this type of technology is not sufficient to secure ATM transaction form intruders.

I. Current Method To Secure The ATM Transaction :-

1. Personal Identification Number(PIN Number):-

The account holder will be given the ATM card and private PIN (Personal Identification Number) or password. PIN number or password is an important aspect in ATM system, which is commonly used to secure and protect financial information of customers. PIN number need to be remembered by the card owner and it should not be shared with others to prevent unauthorized access.

Drawback Of Personal Identification Number(PIN Number):-

1. **Shoulder surfing:-**

Shoulder surfing is an very big attack on the ATM transaction. Shoulder Surfing involves a fraudster looking over your shoulders to observe you enter your PIN to conduct a transaction. Once PIN has been compromised, your investments are no longer safe ,and then this fake user can easily access the legitimate person account by using the pin number and then this fake person steal money from their accounts.

Figure 2:-Shoulder surfing

2. Password Guessing:- ATM PIN number is an 4 digit .There for an attacker can easily guess the PIN number. The attacker can try number of pattern(ig. birthdates, bike number).If any password match then attacker can easily steal the money in account .

2. UNIMODAL BIOMETRICS IN ATM SYSTEM

The term “biometrics” comes from the Greek words “bio” (life) and “metrics” (to measure). Statistics refers to automatic system that uses measurable physiological characteristics or behavior altruist to acknowledge the identity or manifest the claimed identity of a private.

Biometric systems supported dingle supply of data are referred to as unmoral system. In smart card, the fingerprint templates are encoded into a smart card memory, to identify a person, his/her fingerprints are compared against the digital templates stored in the

card memory. Identity management system is to find the individual's identity.

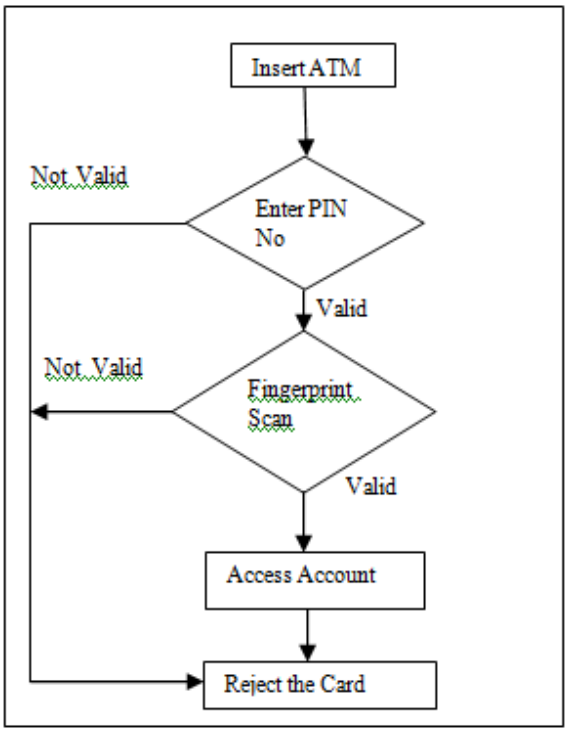

Figure 3: System Flow Diagram for ATM using Unit Model Biometrics

Biometric characteristic as long as it satisfies the following requirements **[2]:**

1. Universality- one and all ought to possess the biometric characteristic.
2. Distinctiveness- Any2personsought to be sufficiently totally different in terms of the characteristic.
3. Permanence- The characteristic caught to be sufficiently invariant over a amount of your time.
4. Collectability- The biometric characteristic caught to be measurable with some sensing device.
5. Performance- Refers to the extent of accuracy and speed of recognition of the system, the resources needed to realize the specified recognition level, like wise because the operational and environmental factors that have an effect on the accuracy and speed
6. Resistance/ Circumvention- Refers to the degree of issue needed to defeat or bypass the system/

Limitations Of UNIMODAL BIOMETRICS

1. **Noise in sensed data**- The accuracy playa serious role in recognition of biometry. The accuracy of the biometric systemic extremely sensitive to the standard of the biometric input and also the noise gift within the information can lead to a big reduction within the accuracy.
   a. E.g. the fingerprints on a person can get damaged and also, it changes with age.
2. **Lack of individuality**- Feature extracted from completely different people could also be similar. This lack of individualism will increase the False settle for Rate (FAR) of a biometric system.
3. **Intra-class variations**- The data acquired for verification won't match to the information used for generating guide throughout enrollment. as an example the face biometric is capture dander Neath completely different angle. Massive intra-class variations increase the False Reject Rate (FRR) of a biometric system.
4. **Inter-class variations**- It happens primarily between twins. It refers to the overlap of feature are as similar to multiple people. Massive inter-class variations increase the False Acceptance Rate (FAR) of a biometric system.
5. **Spoofing**- A biometric system could also be circumvented by presenting afflux biometric attribute to the detector
6.

IV. Attack on ATM:-

1. Steal Cards:-The simplest way for a criminal to get card data is to steal someone's card. To get the PIN, the thief might shoulder surf or guess a weak password, such as a birth date.

2.ATM Malware:-Malware that intercepts card and PIN data at the ATM, allowing the criminals to copy this to create counterfeit cards.(ref [4])

V. The Existing System:-

The existing ATM system ATM authenticates transactions via the card-based and PIN-based system. Therefore it grant access to bank customer to several services such as cash withdrawal and deposits, account to account to account transfer, balance enquiry and utility bill payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a PIN is match, the system authenticates the user and grants access to all the services available via the ATM. If there is a PIN is mismatch then the user authentication process fails and the user is given two more chances to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM..

Therefore in existing system chance of fraud rant transaction. If any one know the PIN number of an ATM then this fake person can easily access the all services available via the ATM.

The below Data Flow Diagram depicted the existing working of ATM system .Entry of a correct PIN is adequate to authenticate a user to the bank system and thereafter grant access to the system for withdrawal as depicted in Figure

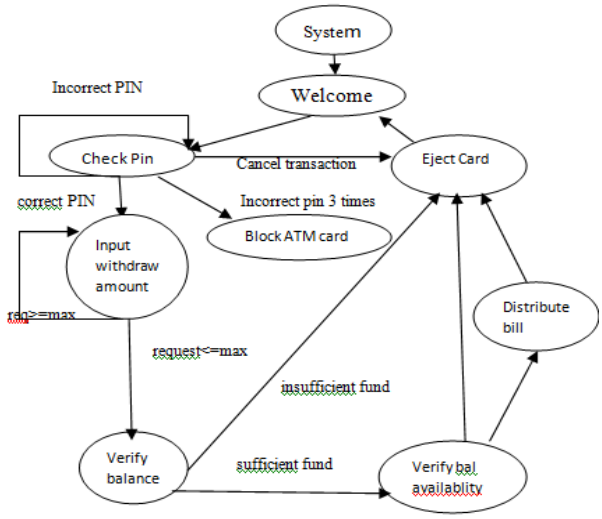

Figure 4:- Data Flow Diagram of Existing Working Of ATM System

VI. The Proposed System:-

In this Existing system we analyzed what are the problem people faced in the ATM transaction.
Multifactor Authentication (MFA) methodology provides additional complexity to the user.
In the existing system more chance for illegal Transaction in the ATM. Fake people can easily withdraw or transfer the amount.

This research will helps to overcome the problem of complexity and provides easiest way to secure the ATM card. Whenever ATM card is inserted into the ATM card slot, the system requires PIN to authenticate the user. If PIN gets verified, it sends authentication message to the user's mobile which is register in the bank. If the user replied to make a transaction, then transaction takes place. And if user reply to terminate it switches ON the buzzer and block the ATM card gives detail about fraud to the banking security authority. The proposed system uses GSM modem for sending authentication message from ATM to the user and getting Reply Message Option from user to ATM. If the authorized person

sends Reply Message YES then transaction takes place and if it sends NO then transaction occur is terminated. In proposed new feature get added for blocking the ATM card, if you miss your ATM card then you can block your ATM temporary or permanently.

The below Data Flow Diagram depicted the proposed working of ATM system. Proposed system which is an enhancement of the existing system. The entry of an accurate PIN is insufficient to certify to the bank system.. This is as a result of a further level has been incorporated for the authentication method which requires the customer to send reply message from pre-registered mobile device via

SMS gateway to the ATM system. If customer send Yes then transaction take place, if it send No then transaction is terminate and if it sent Block then it will Block the ATM ca

Figure 05:- Transition Diagram for the Proposed System

VII. The Algorithms

The algorithms for the proposed system are described below.

START
STEP 1: Insert card into the ATM Machine
STEP 2: Enter PIN
STEP 3: If PIN is Valid GOTO STEP 7 ELSE
STEP 4: Verify if Incorrect PIN has been entered trice
STEP 5: If incorrect PIN entered trice GOTO STEP 6
ELSE GOTO STEP 2
STEP 6: Block and Retain ATM card GOTO STEP 20
STEP 7: Input withdrawal amount
STEP 8: If withdrawal amount > maximum allowed
GOTO STEP 7
STEP 9: Verify account balance
STEP 10: If balance is sufficient GOTO STEP 11
ELSE GOTO STEP 20
STEP 11: Send Reply Message (Yes,No,Block)
STEP 12:If Reply Message is YES then GOTO step 17
STEP 13 If Reply Message is NO then GOTO step 15
STEP 14: If Reply Message is BLOCK then GOTO step 16
STEP 15: Terminate transaction GOTO STEP 20 .
STEP 16: Block ATM card
STEP 17: Verify balance availability
STEP 18: If sufficient balance GOTO
STEP 19 ELSE GOTO STEP 21
STEP 19: Disburse balance
STEP 20: Eject Cards
STOP

VIII.CONCLUSION:

The adoption of the ATM as an electronic banking channel has positively impacted the banking industry worldwide because it is very effective and convenient for bank customers. The advent of ATM fraud has however been a menace for many banks all over the world and many banks now aim to eradicate fraud costs to the bank. The planned system will offer sensible and viable solution that addresses the Requirements of the regulatory authority of the banks. The adopted technology of the proposed system is also cheaper to deploy than the biometric

authentication technique because it utilizes the components of the existing system. The chance given for hackers to make use of fake biometrics to act as an authorized user is strictly avoided, which makes the ATM Transaction more secure. In general, it will positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions.

The proposed second level authentication mechanism for ATMs will increase customer satisfaction and also give customers the peace of mind they need considering the high level of security applied to their accounts. Finally, it will limit the financial risks of customers given that they most times take the responsibility for financial loss via ATM rather than being allowed to pass on the risk to the banks.
In the future, we will implement the proposed system using the second-level authentication model discussed in this paper.

IX. References

[1]https://www.elprocus.com/automatic-teller-machine-types-working-advantages/

[2]http://atmoperation2010.blogspot.in/2009/12/automated-teller-machine-atm.html

[3]http://www.circuitstoday.com/working-of-automatic-teller-machine-atm

[4]http://www.ncr.com/company/blogs/financial/six-types-of-atm-attacks-and-fraud