© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

ATM Transaction Security Using Biometrics

S. Balaji
Sri Sairam Engineering College, Tambaram Chennai, Tamil Nadu India

ABSTRACT

For the traditional ATM terminal customer recognition systems rely only on bank cards, passwords, and such identity verification methods which measures are not perfect and functions are too single. For solving the bugs of traditional of ones, we design a new method to access ATM without cards and passwords. This system includes the verification of the account holder using their mobile number, face recognition and security questions.

Keywords : Automatic Teller Machine (ATM) Mobile, Face Recognition.

I. INTRODUCTION

With the development of computer network technology and e-commerce, the self-service banking system has got extensive popularization with the characteristic offering high quality 24hrs service for customer. Nowadays, using the ATM (automatic teller machine) which provides customers with the convenient banknote trading is very common. A lot of criminals tamper with the atm terminal and steal user's card and password by illegal means. Once user's bankcard is lost and password is stolen, the criminal will draw all cash within a shortest time, which will bring enormous financial losses to customer. Traditional atm systems authenticate generally by using the atm card and the password, the method has some defects. Using atm card and password cannot verify the client's identity exactly. In recent years the algorithm that the face recognition continuously updated which has offered new verification means for us, the original password authentication method combined with the bio-metric identification technology verify the clients identity better and achieve the purpose that use of ATM machine improve the safety effectively.

II. METHODS AND MATERIAL

A. Existing System

In case of cash withdrawal, one has to go to ATM center for making the transactions. The very first step for the transaction is to swipe the card in the ATM machine. Existing ATMs typically provide instructions on an ATM display screen that are read by a user to provide for an interactive operation of the ATM. Having read the display screen instructions a user is able to use and operate the ATM via data and information entered on a keypad.

We have to be very particular in typing our 4-digit pin number in a correct manner. Then one has to select for the required transactions displayed on the screen.

Today's existing ATM system has only one security factor i.e. 4- digit PIN validation. According to Cambridge researchers, they have documented a worrying PIN cracking technique against the hardware security modules commonly used by bank ATM. It is possible to crack the PIN in an average of 15 guesses. According to the survey the average debit card fraud amount was $5.55 Billion in 2012.

Major problems faced by the user while accessing the cards:

1) Skimming Attack

ATM skimming is like identity theft for debit cards. Thieves use hidden electronics such as portable small card readers to steal the personal information stored on your card such as card number and record your PIN number to access earned cash in the account. Skimming device can retain information from 200 ATM cards before using it. When one slides the card into the ATM, it is unwitting sliding through the counterfeit reader, which scans and stores all the information on the magnetic strip. To gain full access to the bank account on an ATM, the thieves still need the PIN number. They use tiny spy cameras to get a clear view of the keypad and record all the ATM's
PIN action.

2) Card Trapping

Card trapping is a major attack in ATM. This attack occurs when the person inserts the card in ATM; the card is physically captured by inserting a strip of metal or sleeve of metal or plastic called loop. When the card is inserted, the loop holds the card then the cardholder type the PIN and request for his funds. When the card is retained, it asks for PIN again. The retyped PIN is ensured by the fraudster. Once the person believes that the machine has retained the card and leave to make enquiries. The fraudster then removes the card from the ATM device and makes use of it.

3) PIN Cracking

ATM PIN is the primary security against ATM fraud. For cracking the PIN, the program is written in such a way that tries the PIN for particular account and this requires average of 5000 transactions to discover each PIN. Also hackers have only three guesses to match against 10,000 PINS. The decimalization tables used to translate between a card PIN and the hexadecimal value of a PIN generated when the hardware security module checks the validity of a number. The attack works not by going after the PIN number directly but by manipulating the contents of the decimalization table in order to gain clues.

4) ATM Malware

The person, who is having the key of ATM, inserts the malware into system and inserts the control card into machine's card reader to trigger the malware which contains all recent transaction information from primary memory.

B. Proposed System

The foremost aim of this way of banking is proposed or designed to outsmart fraudsters and withstand physical and logical attacks. This way of banking using mobile phones is mainly concerned with security and anti-theft solutions. ATM banking security and protection of its data has been of great concern and a subject of research over the years. It is observed that the user has to carry the card all the time for the transaction. And also due to convenience of remembering the key (PIN), user uses short keys (4 Digits) which in turn increases the vulnerability of the data. At the time of registration to the network, a person's mobile number is registered and face is scanned and phase features of the image are generated. Therefore a local binary code of sixty four byte is extracted of this matrix and is transmitted to the server. These features are stored in the server database.

1) One Time Password

At the time of transaction, instead of swiping the cards, mobile phones are initially used so that every ATM machine should have a number which can be used as toll-free. This number differs from each and every machine at each and every time. One has to give a missed call to this toll-free number. As soon as the mobile number is received, the server checks the number with the database and it alerts the person with the onetime password (OTP). It is not necessary for the person to have the OTP in memory. This password varies every time whenever the toll free is dialed. The concern after entering the OTP, the details of the person is then displayed on the screen along with the transaction. The user then selects the transaction according to the need.

2) Face Recognition

The very next step is the face recognition. Face detection is an important aspect for biometrics, video surveillance and human computer interaction. The image of the user's face is registered in database. During transaction, the camera fixed in the ATM captures the image and matches it with the image in the database. To implement this, a multi-GPU implementation of the Viola-Jones face detection algorithm that meets the performance of the fastest known FPGA implementation. The GPU design offers far lower development costs, but the FPGA implementation consumes less power. We use Viola- Jones Face Detection algorithm. At a high level, the algorithm scans an image with a window looking for features of a human face. If enough of these features are found, then this particular window of the image is said to be a face. In order to account for different size faces, the window is scaled and the process is repeated. Each window scale progresses through the algorithm independently of the other scales. To reduce the number of features each window needs to check, each window is passed through stages. Early stages have fewer features to check and are easier to pass whereas later stages have more features and are more rigorous. At each stage, the calculations of features for that stage are accumulated and, if this accumulated value does not pass the threshold, the stage is failed and this window is considered not a face. This allows windows that look nothing like a face to not be overly scrutinized. To more thoroughly understand the algorithm, some specifics need to be defined including features, a special representation of the image known as the Integral Image, and a stage cascade.

Feature classifiers are used to detect particular features of a face. Windows are continuously scanned for features, with the number of features depending on the particular stage the window is in. The features are represented as rectangles. To compute the value of a feature, computation of the sum of all pixels contained in each of the rectangles making up the feature is done. Once calculated, each sum is multiplied by the corresponding rectangle's weight and the result is accumulated for all the rectangles in the feature. If the accumulated value meets a threshold constraint, then the feature has been found in the window under consideration. The weights and sizes of the rectangles for each feature are obtained and verified. After face recognition verification, the user is able to make the required transactions.

Once this face recognition fails (i.e.) the image does not match with the specified person's face, the alarm signal inside the ATM center sounds and the ATM door closes automatically as the false person (or) the fraudster is being trapped inside the atm center and recognition of face being carried out which is monitored by the LCD inside the ATM sends the signal to the higher authorities.

3) Security Question

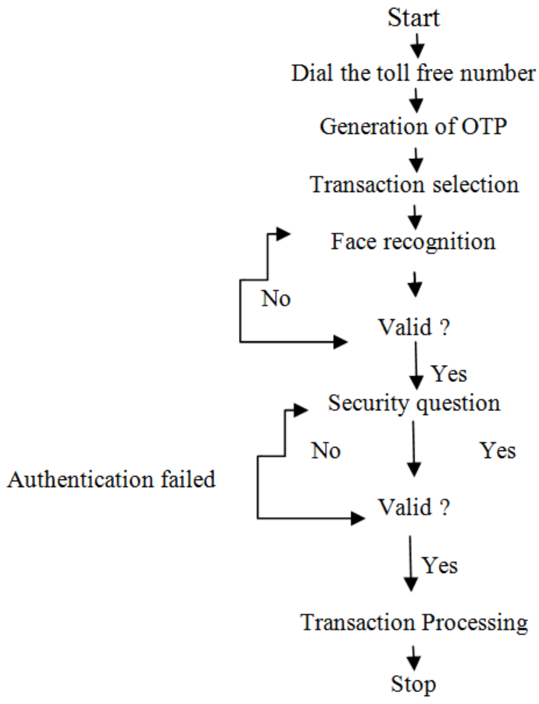
Once the face recognition is successful, the user enters the sum of money to be transacted. Then the ATM displays a security question, this is mainly to overcome any defect in the face recognition process. The security question along with the answer is stored priorily in the database. The user types the answer for answer is encrypted and sends to the server for validation purpose. At the server side encrypted answer is decrypt and match with the server side database. If the answer is validated, the user at last makes the transaction efficiently.

III. RESULTS AND DISCUSSION

Advantages of Proposed System

1. Securable access without ATM card.
2. Face recognition cannot be easily hacked because of its unique identification.

Flowchart



IV. CONCLUSION

Network Security includes basic securities to protect the information from unauthorized access and loss. ATM access is not more secure using 4 digits PIN. This paper proposed the new approach for existing ATM system for providing more security using face recognition which plays an important role because these are unique and not easily hackable.

V. REFERENCES

[1] Pooja Mali Shruti Salunke Rajashri Mane Pooja Khatavkar "Multilevel ATM Security Based On Two Factor Bio-Metrics" International Journal of Engineering Research & Technology (Ijert)

[2] L. Acasandrei and A. Barriga IMSE-CNM-CSIC, Seville, Spain IMSE-CNM-CSIC/University of Seville, Seville, Spain "FPGA implementation of an embedded face detection system based on LEON3" http://elrond.informatik.tufreiberg.de/papers/WorldComp2012/IPC2434.pdf

[3] "Work of ATM skimming", http://www.howstuffworks.com/atm-skimming.htm