ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

Secure Pin Authentication as a Service for ATM

G.Jayandhi[1], S.Elphin Samuel[2], A.Govardhan[3], A.Logesh[4], A.Vishnukumar[5]

Assistant Professor, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India[1]

UG Student, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India[2]

UG Student, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India[3]

UG Student, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India[4]

UG Student, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India[5]

ABSTRACT: In this paper we present an NFC- and QR-code based hybrid configuration approach for smart sensors which is suitable for smart automated teller machine use cases. The purpose of this paper is to reinforce security of the conventional ATM model. Features like face recognition and One -Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN**.**

KEYWORDS: Automated teller machine, Authentication, Fraud, One Time Password, Security.

I.INTRODUCTION

Automated Teller Machine (ATM) is considered the common e-banking technology adopted by banks all over the world. ATM is a computerized machine that provides customers of banks the facility of accessing their accounts for cash withdrawal and to carry out other financial transactions without the need for a human cashier, clerk or bank teller. It combines a computer terminal, recordkeeping system, and cash vault in one unit, permitting customers to enter a financial firm's bookkeeping system either with plastic card containing a personal identification number (PIN) or by punching a special code number into a computer terminal linked to the financial firm's computerized records 24 hours a day.ATM's has been adopted by banks because they offer considerable benefits to both banks and their depositors. The most exciting experience for customers as well as bankers is that the ATM is replacing all the difficulties of bank transactions such as personal attendance of the customer, banking hour restrictions and paper-based verification. It is quite easy to withdraw money from ATM instantaneously at any time. ATMs allow one to perform multiple banking functions such as withdrawal of cash, making balance enquiries, transferring money from one account to another, paying insurance premium, making small loans and payment of bills.

II.LITERATURE SURVEY

The pin used in ATM is insecure because there may be chances of stealing ATM card and pin number. To overcome this issue unique ATM password generated by the server and the pin is hided in the form QR code this give an additional security. In order to avoid misuse of ATM card additional feature of face recognition is used in this project to overcome the fraudulent use of ATM

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

III. DRAWBACKS OF CONVENTIONAL ATM

Notwithstanding the numerous benefits of ATM systems, security of customer's information has become a huge challenge and source of worry not only on the part of the banking industry but also to the customers. Criminals tamper with the ATM and steal users' credit card and password by illegal means. ATM's eliminate the need for round-the-clock human involvement and tend to be located in places that make them more vulnerable to attack as they are often attractive targets for perpetrators. Activities of card fraudsters have been on the increase, this is as a result of the growth of the number of ATM card holders, e-payment awareness and deployment of ATM cash points. The proliferation of identity theft among ATM users calls for a more reliable method of carrying out the validity of customers' identity. In conventional ATM systems, authentication of users' identity is performed using an ATM card and PIN. This method has some shortfalls as stolen cards can be used by unauthorized users to access customers' account details if the PIN is known to them. This is possible because many ATM users resort to the use of PIN that is simple and can be remembered easily such as birthdays and social security numbers.

IV. PROPOSED SYSTEM

In this proposed system, we are going to implement this paper as ATM based security system using face recognition and QR code based OTP system. The valid person facial image will be stored in the database. If the person is using the ATM card means, the face recognition mechanism it check the person is valid or not. If the person is valid means one request message will be passed to the server. The server will produce a QR code and passed to the ATM machine and ATM machine will hide the OTP in QR Code. The QR Code will be displayed in the machine, and then the user has to scan the QR Code through the QR Scanner APP. Then, the displayed OTP will be passing to the server by the user. Then the user has to click the sent icon in the app. Then the OTP and server produced OTP will get compared if the OTP get matched, and then further process gets started. If the unknown person is using the ATM means the security questions will be asked by the ATM machine, if they say the right answer, the further process will get started or else the warning message will be passed to the user mobile.

The use of password in place of PIN, OTP to verify the validity of customer's identity at two different layers of authentication will provide a robust security. This is because it cannot be lost, stolen, forgotten or forged. An OTP is a pass code that is valid for only one login session or one single transaction. It expires once it is used. The most important advantage addressed by OTP is that it is not vulnerable to replay attack in contrast to static password. The use of two-tier authentication model will undoubtedly improve ATM security by eliminating the rate of card fraud, currency fraud and identity theft thereby restoring the confidence of customers on the use of ATM systems.

V. WHAT ARE FACE RECOGNITION SYSTEMS?

Face recognition is an application that identifies a person from a digital image or a video outline from a video source. One of the behaviours to do this method is by matching chosen facial features from a facial database and the image.

VI. PURPOSE OF USING FACE RECOGNITION AND OTP IN ATM

Face recognition finds its application in many fields such as homeland security, criminal identification, human-computer interaction, privacy security, etc. The face recognition feature prevent the access of account through stolen or fake cards. The card itself is not enough to access account as it requires the person as well for the transaction to proceed. Eigen face based method is used for the face recognition. However, the drawback of using this method is that it can sometimes be spoofed by the means of fake masks or photos of an account holder. To overcome this problem 3D face recognition methods can be used. However, its computation cost is high and requires large storage space which makes it very difficult to store information about a large number of users and 3D masks can also be used to spoof the 3D facial recognition based model. 3D printing is mostly used for such attacks. These drawbacks can be easily overcome by using One -Time passwords (OTP). OTP ensures that the user is authentic by sending the randomly generated 4-digit code to the registered mobile number of the corresponding account holder. In addition, the user will not have to remember PIN. It prevents the fraudulent attacks like:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

A. Eavesdropping:
The ATM card or PIN of a user can be spied upon and can be accessed easily by obtaining the card by faulty means. This can lead to some serious consequences.

B. Spoofing
There is a possibility that, when a user enters the PIN during the transaction process, a hacker fakes as the authorized site and prompts the user to re-enter PIN due to a system error. When a user complies with the instruction the hacker stores the data and uses it for his future peccadilloes intentions. This man-in-the-middle (hacker) attack is futile because new password is temporarily assigned in every new transaction.

C. Brute-force attack
Using the brute force, if we try to crack the current static four digits PIN it can be done in 9999 attempts, thus weakening the security. In our model a 6-digit code is sent to a registered number, thus increasing the security and reducing the chances of cracking the code using brute force.

VII.FACE DETECTION AND RECOGNITION

At this stage a user simply needs to look into the camera installed on ATM. If the user is recognized, then OTP is sent to user's mobile phone. We have seen thefts in ATM like the criminal entering into the room and forcing the user to access his or her account. To overcome this problem we have found a simple solution; if more than one faces are detected by the machine then the account gets temporarily locked. This additional feature is simple yet effective. Therefore, this system ensures that transaction is preceded only when user alone is accessing the machine.
In general, face recognition techniques can be divided into two groups based on the face representation they use

A. Appearance-based
It uses holistic texture features and is applied to either entire face or only to the specific regions in face image. Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminate Analysis (LDA) fall under this category.

B. Feature-based
It uses geometric facial features (mouth, eyes, nose, etc.) and geometric relationships between them.

VIII. OTP WORKING

For implementing OTP, we will make use of GSM modem to send SMS (an OTP) to user's mobile number. The idea to use mobile phones is preferred over e-mail because the people in rural areas have simple phones which can receive text messages but have no internet connections and e-mail facilities. Since mobile phones are ubiquitous, we intend to use mobile phones so that everyone can take the benefit of the new proposed system. The user will receive OTP immediately after passing the face recognition test. Once OTP is received user has to enter the code which is of 4-digit. User gets three chances to enter the code. If the code is entered incorrectly in three consecutive attempts account gets temporarily blocked and notification is sent to registered mobile number. This feature is added in order to restrict the fraudulent means of attacking the account of a user by wearing masks or in rare cases, if unauthorized user's face mistakenly matches authorized user's face.

A. Random Number Generation
Generation of sequence of Pseudo-Random Numbers, (Y_n):
$Y_{n+1} = (a \times Y_n + C) \bmod (m)$
Choices of a (multiplier), C (increment) and m (modulus) are important because random numbers generated will be in sequence if not handled properly.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

B. Proposed Random Number Generation formula

The drawback of the above random number generator is that the sequence has a finite number of integers and the sequence gets repeated over a period of time. Therefore, we have modified the formula by applying the same random number generator formula to 'C' and this value is substituted in the random number generator's increment. So the new random number generator formula will be:

$C = (b \times X_n + d) \bmod (m)$

$X_{n+1} = C$

$Y_{n+1} = (a \times Y_n + C) \bmod (m)$

The random number(Y_{n+1}) generated will be the OTP. The value of 'm' should be a large prime number in order to distinct unrelated numbers. Though the overhead is increased due to computation, but the repetition of a sequence is completely eliminated.

IX. HOW THIS MODEL HELPS TO PREVENT THEFT?

Our proposed system's linear dependency of three phases, i.e card requirement, face recognition and OTP plays a crucial role in preventing theft as explained below:

1. If a thief creates a duplicate card access a user account, the thief's face will not match with user's face.
2. In rare cases, if the thief manages to match the user's face by using masks, then OTP will be sent to the user's registered number, which in turn will alert the user that someone is trying to access the account.
3. Suppose if a user's mobile phone is stolen, the user can deactivate the phone number by contacting the service provider which will prevent OTP to reach the stolen phone which will help to prevent unauthorized access to the account.

To break through these three phases, a thief needs to steal/duplicate cards, then match a user's face and then steal user's phone. Thus passing through this system is only possible if the user is careless to report a stolen/misplaced phone or stolen/misplaced ATM card to deactivate account.

X.QUICK RESPONSE CODE

Due to the size limitations of a QR code's maximum payload, two different modes for transferring configuration data to the mobile device are suggested.

1. The whole configuration payload is stored in the QR code, which allows to store about 2900 bytes of data. We denote this type as *inline* QR code. Inline QR codes do not require the mobile device to have an active network connection, thus, those codes can be distributed, for instance, to a maintenance worker without restrictions
2. If the configuration data is larger than the size limit of 2900 bytes, only an URL pointing to the backend is included in the QR code. The mobile device then needs to fetch the configuration data from the backend using a secure channel (TLS). This type is denoted as *URL* QR code. For the download process, the mobile device needs to have a network connection through which the backend can be reached.

XI. DRAWBACKS

One of the major drawbacks of this model is when the camera does not work properly or damaged. Due to such technical problems the transaction is hindered. However, to solve this problem, we have introduced a 'report' button on the screen during the face recognition phase. This notifies the authority of a bank and the problem can be resolved as soon as possible. In order to prevent unnecessary use of report button, detail of user is provided to the authority to identify the user who has reported the problem.

1. If the user does not receive OTP in short time after the face recognition phase, it can delay the transaction which in turn makes user impatient. To overcome this situation a 'resend OTP' button will be provided which will resend OTP.
2. The major drawback of this system is that if a particular network service is down, then it becomes impossible for the user to receive OTP.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

XII. FUTURE SCOPE

Facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The defects in face recognition technique like the inability to detect face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition reduces, it can be used instead of face recognition.

XIII. RESULT AND DISCUSSION

In the fig 1, it shows that authorized person is using the ATM and QR code is displayed on the screen

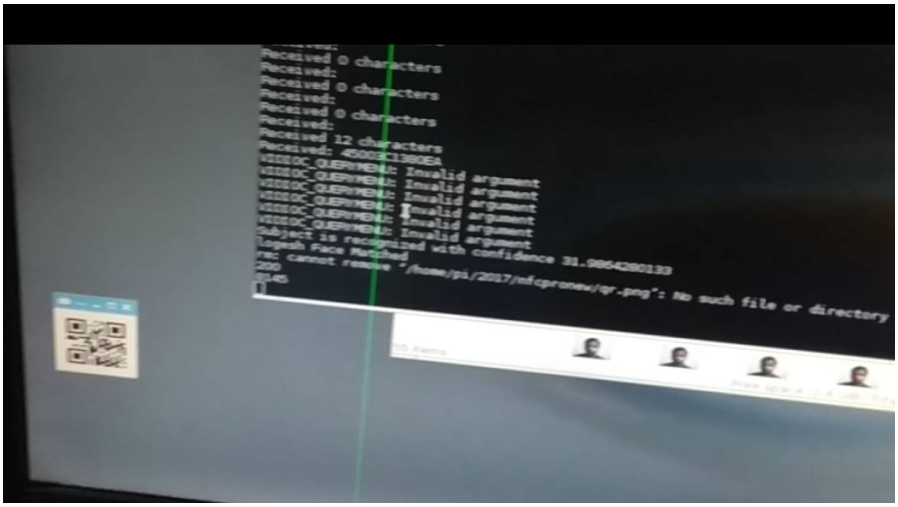

Fig. 1 Authorized person using ATM

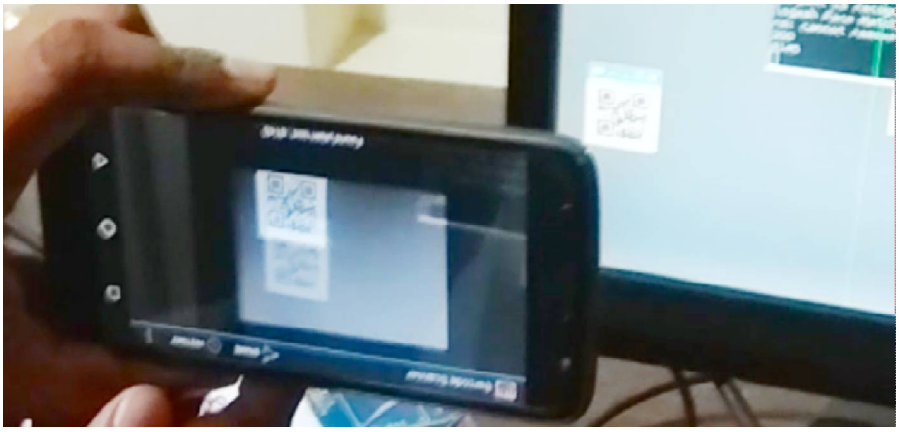

Fig. 2 Scanning the QR code

In the fig 2, it shows that scanning the QR code by using mobile app, then OTP is displayed on the mobile.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

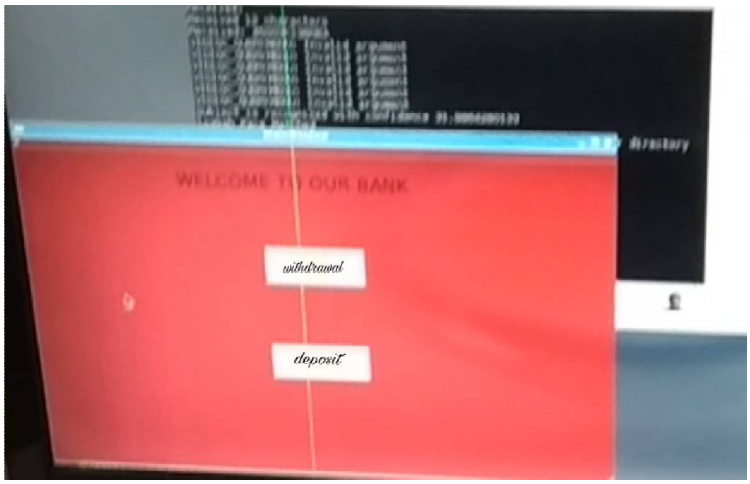

Fig .3 ATM window

In Fig 3, shows that the ATM screen which means that the OTP gets matched and further process like withdrawal orr deposit of cash can be performed.

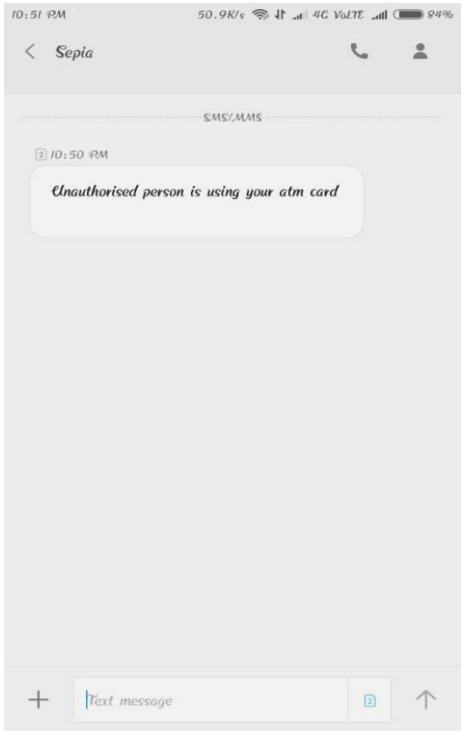

Fig .4 Warning message

In Fig 4 shows the warning message sent by server to the registered mobile number that your ATM card is used by someone.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 3, March 2018

XIV.CONCLUSION

This project is still under development. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms. According to the statistics PCA based face recognition is very accurate, requires less computation time and less storage space as trainee images are stored in the form of their projections on a reduced basis. After the completion of the project we will collect the quantitative aspects of the model and compare it with the qualitative results for further proof.

REFERENCES

[1] G. Meijer, K. Makinwa, and M. Pertijs, Smart Sensor Systems: Emerging Technologies and Applications. John Wiley & Sons, 2014.
[2] D. Lucke, C. Constantinescu, and E. Westk¨mper, "Smart Factory – A Step towards the Next Generation of Manufacturing," in Manufacturing Systems and Technologies for the New Frontier. Springer, 2008, pp. 115–118.
[3] C. Lesjak, T. Ruprechter, H. Bock, J. Haid, and E. Brenner, "Facilitating a Secured Status Data Acquisition from Industrial Equipment via NFC," Journal of Internet Technology and Secured Transactions (JITST), 2014.
[4] R. Harper, Inside the Smart Home. Springer Science & Business Media, 2006.
[5] H. Zhang, "Bring your own encryption: balancing security with practi- cality," Network Security, vol. 2015, no. 1, pp. 18–20, 2015.
[6] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC)," in Workshop on RFID security, 2006, pp. 12–14.
[7] D. L´ pez-de Ipi˜ a, J. I. Vazquez, and I. Jamardo, "Touch Computing: on Simplifying Human to Environment Interaction through NFC Technology," 1as Jornadas Cient´ficas sobre RFID, vol. 21, 2007.
[8] G. Van Damme, K. Wouters, and B. Preneel, "Practical Experiences with NFC Security on mobile Phones," Proceedings of the RFIDSec, vol. 9, 2009.
[9] J. Ondrus and Y. Pigneur, "An Assessment of NFC for Future Mobile Payment Systems," in Management of Mobile Business, 2007. ICMB 2007. International Conference on the. IEEE, 2007.
[10] V. Coskun, B. Ozdenizci, and K. Ok, "A Survey on Near Field Communication (NFC) Technology," Wireless personal communications, vol. 71, no. 3, pp. 2259–2294, 2013.
[11] "Cryptographic Extraction and Key Derivation: The HKDF Scheme," in *Annual Cryptology Conference*. Springer, 2010, pp. 631– 648.
[12] D. Mellado, E. Fernandez´-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer standards & interfaces*, vol. 29, no. 2, pp. 244–253, 2007.