Design and Implementation of Multilayer Security for ATM Machines

Anjalin Joy, Caren Babu

Abstract*: *Automated teller machine (ATM) nowadays are a favourite spot for attackers as they are available everywhere and are much easier to rob. Generally, ATM attacks can be either physical ATM attacks or ATM-related fraud attacks. In this paper the idea of an ATM system with multilayer security is proposed with the help of internet of things (IoT), fingerprint identification and face recognition to increase the security of ATM. The physical ATM counter attacks can be identified by using specific sensors to detect changes in vibration and temperature in the ATM counter. To prevent ATM related fraud attacks the proposed system has additional security features like fingerprint identification and face recognition along with ATM number verification. The convolutional neural network (CNN) and machine learning based face recognition is used in this work which is quite reliable. Failures in any of the above steps cancel the transactions and so the proposed system provides multi layer security which makes it impossible for the attackers to break the ATM security. The proposed system will help to increase the security of the ATM and provide safe and secure ATM transactions.

Keywords*: *ATM, Card Verification, Convolutional Neural Network (CNN), Faces Recognition, Fingerprint Verification, Password Verification And Security.

I. INTRODUCTION

Automated teller machines (ATM) are one of the easily available sources to do cash withdrawals and access their bank details without going to bank. In the traditional ATM, transactions are authorized based on the authentication of their ATM card and personal identification number (PIN). Since the incidence of ATM thefts by duplicating cards and identifying PIN [7]-[9] are increasing worldwide, transactions using card and PIN are not safe and secure. In order to increase the ATM security many new technologies like face recognition fingerprint identification, global system for mobile communication (GSM) technology and internet of things (IoT) techniques have been used alone or combining with the traditional card and PIN.

The technologies which are commonly used to increase ATM security like face recognition [1]-[3], fingerprint identification, smartphone, GSM technology, IoT etc alone cannot provide a safe and secure transactions. The security using smartphone will not be efficient if smartphone is not working. The existing face recognition techniques have less accuracy compared to other techniques. The fingerprint techniques may fail if fingerprint is not identified correctly. There is a chance of card duplication in some cases when cards are used and result in fraud transactions. The PIN can be identified by video cameras installed by frauds and may steal money with duplicate cards. The technologies discussed above alone are not able to provide security against both physical ATM attacks and fraud transactions.

This paper proposes a new ATM security method which provides security against both physical ATM attacks and fraud transactions [5]. Physical attacks can be prevented by adding IoT based techniques which include the use of sensors to detect changes in temperature and humidity. The electronic thefts are prevented by addition of face recognition and fingerprint authentication along with traditional card and PIN. The GSM technology is also used to send alert short message service (SMS) if any changes in temperature or humidity occur in ATM counter during physical attacks. The transaction details are also informed to the customer by SMS send to the registered phone number. The ATM security is enhanced by addition of fingerprint verification, face recognition, IoT methods, GSM technology [4] along with card and PIN to provide safe and secure ATM transactions.

The prime purpose of an ATM security system is increase protection against physical and electronic theft. New technology has been implemented in the proposed system to overcome this problem. To prevent physical attacks, the changes in the temperature, humidity or vibration in the ATM that can be assessed by using IoT technique [6]. To prevent fraud attacks additional security features like fingerprint identification and face recognition along with card and PIN verification is used. The proposed system will be useful to prevent the unauthorized use of ATM cards and ATM attacks. The main objective of this paper is to provide maximum layer of ATM security [10] by reducing security issues in ATM counter and machine. This paper also aims to introduce the technological advancement in banking fields. The proposed system makes sure that even if one layer of security is compromised the other will prevent the attack, and making it nearly impossible for the attackers to break the ATM security.

II. PROPOSED SYSTEM

The paper proposes the idea of an ATM system with multilayer security that provides protection against both physical ATM counter attacks and ATM related fraud attacks. The components used and connection between individual components in

Manuscript received on June 14, 2021.
Revised Manuscript received on June 19, 2021.
Manuscript published on July 30, 2021.
* Correspondence Author

Anjalin Joy*, Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology, Kodakara (Kerala), India. Email: anjalinjoy007@gmail.com

Dr. Caren Babu, Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology, Kodakara (Kerala), India. Email: carenbabu1@gmail.com

Retrieval Number: 100.1/ijrte.B61120710221
DOI: 10.35940/ijrte.B6112.0710221
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

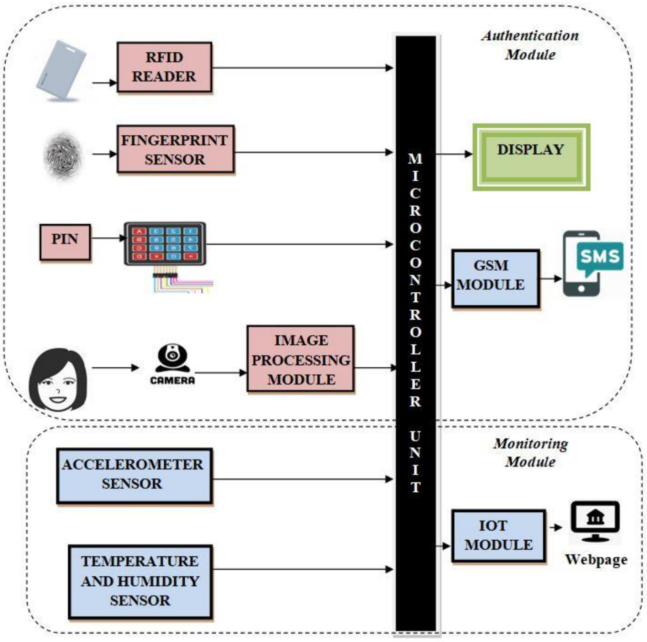

Fig. 1. Block diagram of the proposed system

The proposed system are described in Fig. 1. The working of the proposed system is described under authentication and monitoring sections which help to prevent ATM related fraud attacks and physical attacks respectively. The components used to provide security in authentication module include RFID reader, fingerprint sensor, keypad, camera, GSM module, LCD display and microcontroller. The components used in monitoring module are DHT11 sensor, accelerometer [15] and IoT module. The RFID reader is used to read the card and after card verification the ada-fruit fingerprint sensors detect the authorized users fingerprint. The 4x4 keypad is used to enter the authorized PIN. The camera in the system is used to capture live videos for face recognition. DHT11 sensors are used to detect changes in temperature and humidity. The vibrations in ATM are detected by using accelerometer sensor. The ESP 8266 IoT module helps to show the real time values of changes in vibrations [15], temperature and humidity in the admin's webpage. The GSM module is used to send alert SMS when changes in vibration and temperature cross the threshold. The microcontroller [14] used is ATmega2560 to which the Arduino program is built. The display used in this system is 16x2 LCD display.

The proposed system provides protection against both physical ATM counter attacks and ATM related fraud attacks.

A. *Protection against Physical ATM Counter Attacks*

In the proposed system the physical ATM counter attacks can be detected by using specific sensors that detects changes in temperature, humidity or vibration in the ATM counter.

- *Vibration Sensor:* The changes in vibration of the system during physical attacks are detected by accelerometer or MEMS sensor. The accelerometer sensor have threshold limits set in three directions (x,y and z). If threshold limit is crossed in any one of the three directions, the system considers it as an emergency. In emergency situation alert SMS will be sent to the authorized number of authority and emergency alert is shown in their monitoring webpage.
- *Temperature and Humidity Sensor:* The temperature and humidity status are detected using DHT11 sensor. The DHT11 sensor shows the real time temperature and humidity in the authority's webpage. If the value of temperature crosses the threshold, an SMS will be send to the authority. The resultant changes in the temperature, humidity or vibration in the ATM counter can be assessed by using IoT technique from the main security chamber. Authority can identify the status of the ATM machine from webpage.

B. *Protection against ATM Related Fraud Attacks*

In the proposed paper ATM related fraud attacks the proposed system protect customer transactions with additional security features which include fingerprint identification [11]-[12] and face recognition along with card and PIN verification.

- *Card Verification:* The first stage is the card verification of the customer using RFID reader. RFID reader detects the 12 digit number in the card. If this number is matched with the number stored in the system authorization is allowed to second stage.
- *Fingerprint Verification:* In second stage customer will place his finger in the fingerprint sensor and it will be matched against pre-recorded fingerprint data. The fingerprint sensor used in this system is ada-fruit sensor. The fingerprint [13] identification stage consists of enrolment and matching as shown in Fig. 2. In finger enrolment the fingerprint of a user is taken with the help of a sensor and the pattern generated will be stored in the database. In matching when the user places his finger in the sensor, authorization is granted only if it matches with the fingerprint pattern stored in the database. If fingerprint is matched the system will allow proceeding to the third stage.

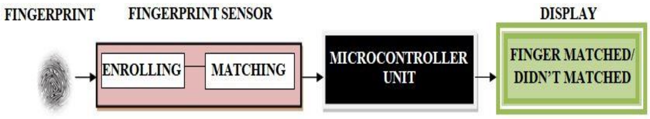

Fig. 2. Fingerprint verification stage

- *PIN Verification:* In second stage customer will place his finger in the fingerprint sensor and it will be matched against pre-recorded fingerprint data. In third stage the customer is asked to enter the four digits PIN from the keypad. The 4x4 keypad is used to enter the PIN by the user for PIN verification. The keypad consists of four columns and four rows. There are switches between the rows and columns. When the key is pressed a connection is established between rows and columns where the switch is inserted The 8 pins of keypad connected to the 8 GPIO pins of ATmega 2560 unit. If correct PIN is entered authorization is allowed to the final stage.
- *Face Recognition:* In the face recognition stage the user's live images will be captured using the ATM camera. The software used for face recognition is Anaconda and it was done in spider IDE.

Retrieval Number: 100.1/ijrte.B61120710221
DOI: 10.35940/ijrte.B6112.0710221
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

The libraries used in face recognition are sci-kit learn and Open cv. The face recognition stage is divided into data collection, face detection and feature extraction, algorithm training and face recognition. The Fig. 3 shows face detection of the authorized user. The live image frame of the user is captured with camera. The image is grabbed and resized into proper image dimension and converted into a blob. The CNN [2] based face detector is used to extract the probability and filter the week detections from the converted image. This also ensures that the dimensions and blob conversions of the image are accurate. The output image is cropped and with the help of a CNN based face embedding or extracting model feature extraction is done and extracted features are stored in the form of embedding vectors (128 numbers). In the classification stage the data of the authorized user is compared with the extracted features of the captured live image. The trained model of the authorized user is created with the help of the data sets collected previously. In the data collection the data's are collected and stored in a directory. Here we take around 500 images and stored in a directory. Face detection and feature extraction was done from the collected data by using a pretrained CNN model and stored in a file. The CNN model used in this system is FaceNet. A model is built with the help of the extracted feature and a machine learning algorithm. The machine learning algorithm used in the system is support vector machine (SVM) classifier. The trained model is also stored in a new file. The trained model is compared with the extracted features of the captured image stored as embedding vectors and predicts probability classes of the user. If features matches face recognition stage is completed and the user will be allowed to complete transaction. In between any of these steps if the identification fails, then the customer will be prevented from doing the transaction.

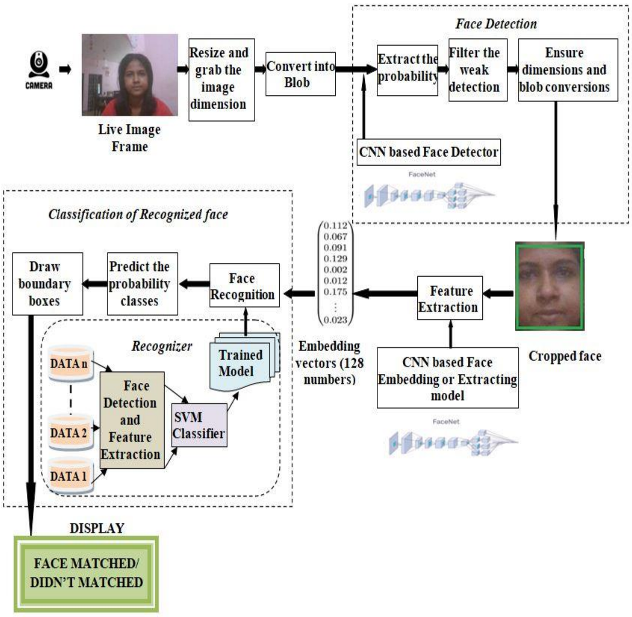
Face Detection
CAMERA
Live Image Frame
Resize and grab the image dimension
Convert into Blob
Extract the probability
Filter the weak detection
Ensure dimensions and blob conversions
CNN based Face Detector
FaceNet
Classification of Recognized face
Draw boundary boxes
Predict the probability classes
Face Recognition
0.112
0.067
0.091
0.129
0.002
0.012
0.175
⋮
0.023
Feature Extraction
Cropped face
Recognizer
DATA n
DATA 2
DATA 1
Face Detection and Feature Extraction
SVM Classifier
Trained Model
Embedding vectors (128 numbers)
CNN based Face Embedding or Extracting model
FaceNet
DISPLAY
FACE MATCHED/ DIDN'T MATCHED

Fig. 3. Face detection model

After completion of authorization process the user will be allowed to access the bank menu and continue with desired transactions. The options displayed in the menu are balance enquiry and amount withdrawal. If user chooses option 1 balance enquiry menu is displayed and if he chooses option 2 amount withdrawal menu is displayed. So this will make sure that only the customer with registered face and fingerprint data along with the correct ATM card information will be allowed to proceed with the transaction. The proposed system makes sure that even if one layer of security is compromised the other will prevent the attack, and making it nearly impossible for the attackers to break the ATM security.

III. RESULTS AND DISCUSSION

The results of the proposed system are shown in Fig. 4. Authentication section will be included in user's side and the monitoring part will be done in administration section. The accelerometer sensor detects changes in the vibration of the system. The accelerometer sensors have threshold limits set in three directions (x, y and z). The threshold limits set in various axis's are: x axis (310-370), y axis (310-370) and z axis (380-440). If the threshold limit in any one of the three axis is crossed, an alert SMS will be sent using GSM module to the authorized admin and emergency alert will be displayed in the webpage. The temperature and humidity changes are detected using DHT11 sensor. The normal temperature limit set in the ATM counter is 34^{0}c.The sensor detect and displays the current temperature and humidity value of the counter using IoT module in the admin's webpage. The sensor also sent an alert SMS using GSM module to the authorized admin.

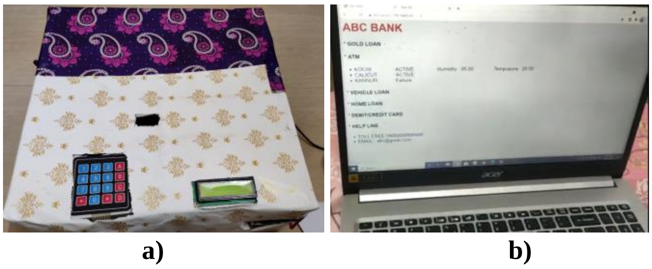

Fig. 4. Multilayered security system: a) User side and b) Admin side.

In card verification stage the 12 digit number of RFID card is detected by the RFID reader. If this number is matched with the number stored in the system, the display shows as "Card Access Granted" and if not displays as "Card Access not granted". In fingerprint verification the finger of the user is kept at Adafruit sensor. When the finger is kept for verification, a 10 second delay is set by the system. If the sensor doesn't match within 10 second, the display shows "Timeout". If it matches within 10 second the display shows as "Finger matched" and if it is not an authorized user the display shows as "Finger didn't Matched". The 4x4 keypad is used to enter the PIN by the user for PIN verification. A four digit number is set as PIN.

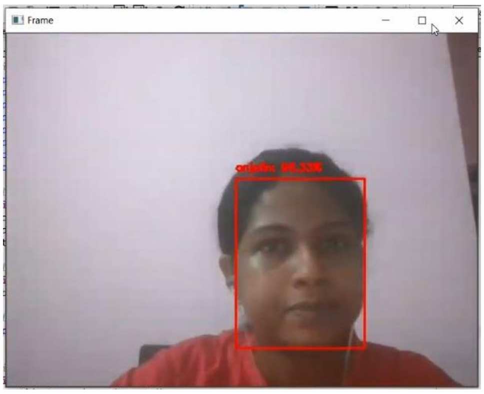

Fig. 5 Matching result

Table- I: Summary of results

	Methods Used	**Results Obtained**
Monitoring Section	Vibration Sensor	Alert SMS sent when threshold crossed. Emergency alert displayed in the webpage.
	Temperature and Humidity Sensor	If temperature more than 34^{0}c alert SMS sent.
Authentication Section	Card Verification	If authenticated, displays “Card Access Granted”. If unauthorized, displays “Card Access not granted”.
	Fingerprint Verification	If authenticated, displays “Finger matched”. If unauthorized displays “Finger didn’t Matched”.
	PIN Verification	If authenticated displays “Password Correct”. If unauthorized displays “Password Incorrect”.
	Face Recognition	If authenticated displays “Face matched”. If unauthorized displays “Face didn’t Matched”.

When the correct PIN is entered the display shows as “Password Correct” and if wrong the system displays as “Password Incorrect”. In the face recognition stage the user’s live images will be captured using the ATM camera. If the live image captured matches with the model built in the system, the display shows as “Face matched” and if not it is displayed as “Face didn’t Matched”. The matching result of the proposed face recognition system is shown in fig. 5. In the traditional systems technologies used for face recognition are usually haar cascade classifier [3]. But in proposed system we implemented combination of FaceNet and support vector classifier which is more accurate in face recognition. So by combining card verification, fingerprint verification, PIN verification, face recognition and IoT techniques, a multilayered ATM security is implemented. The proposed system makes sure that even if one layer of security is compromised the other will prevent the attack, and making it nearly impossible for the attackers to break the ATM security. The summary of the results obtained by various methods of ATM security are shown in Table- I.

IV. CONCLUSION

An ATM is an extension of the facilities provided by the banks allowing customers to access banking facilities without going to the bank. So ATMs are convenient to the customers for basic transactions and perform quick self-service transactions such as deposits, cash withdrawals, bill payments, and transfers between accounts. But ATMs are target for fraud, robberies, physical attacks, electronic thefts and other security problems. The proposed system provides multilayer security preventing both physical attacks and ATM related frauds by the addition of fingerprint verification, face recognition, IoT method along with card and PIN. So the new system will make sure that only the customer with registered face and fingerprint data along with the correct ATM card information will be allowed to proceed with the transaction. Addition of IoT techniques and GSM technology will also help to prevent attacks of the ATM counter. The proposed system makes sure that even if one layer of security is compromised the other will prevent the attack, and making it nearly impossible for the attackers to break the ATM security. This paper will help to increase the security of the ATM counters worldwide and provide safe and secure transactions for the customers.

REFERENCES

1. A. Joy, C. Babu and D. A. Chandy, "Enhanced Security Mechanism for ATM Machines," *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2021, pp. 302-306, doi: 10.1109/ICACCS51430.2021.9441861.
2. A. S. Winoto, M. Kristianus and C. Premachandra, "Small and Slim Deep Convolutional Neural Network for Mobile Device", *IEEE Access*, vol. 8, pp. 125210-125222, 2020, doi: 10.1109/ACCESS.2020.3005161.
3. S. Hazra, "Smart ATM Service," *2019 Devices for Integrated Circuit (DevIC)*, 2019, pp. 226-230, doi: 10.1109/DEVIC.2019.8783820.
4. B. M. Nelligani, N. V. U. Reddy and N. Awasti, "Smart ATM security system using FPR, GSM, GPS," *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, pp. 1-5, doi: 10.1109/INVENTIVE.2016.7830093.
5. O. H. Embarak, "A two-steps prevention model of ATM frauds communications," *2018 Fifth HCT Information Technology Trends (ITT)*, 2018, pp. 306-311, doi: 10.1109/CTIT.2018.8649551.
6. V. Jacintha, J. Nagarajan, K. T. Yogesh, S. Tamilarasu and S. Yuvaraj, "An IOT Based ATM Surveillance System," *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2017, pp. 1-6, doi: 10.1109/ICCIC.2017.8524485.
7. C. Wang, X. Guo, Y. Chen, Y. Wang and B. Liu, "Personal PIN Leakage from Wearable Devices," in *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 646-660, 1 March 2018, doi: 10.1109/TMC.2017.2737533.
8. S. Sankhwar and D. Pandey, "A Safeguard against ATM Fraud," *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, 2016, pp. 701-705, doi: 10.1109/IACC.2016.135.
9. R. Gusain, H. Jain and S. Pratap, "Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2018, pp. 1-5, doi: 10.1109/IoT-SIU.2018.8519850.

10. Maiti, S., Vaishnav, M., Ingale, L. and Suryawanshi, P., 2016. ATM robbery prevention using advance security. *Int Res J Eng Technol (IRJET)*, *3*(02), pp.2395-0056.
11. Oko, S. and Oruh, J., 2012. Enhanced ATM security system using biometrics. *International Journal of Computer Science Issues (IJCSI)*, *9*(5), p.352.
12. Das, S. and Debbarma, J., 2011. Designing a biometric strategy (fingerprint) measure for enhancing atm security in indian e-banking system. *International Journal of Information and Communication Technology Research*, *1*(5).
13. Nawaya, J.J., Jemimah, N. and Oye, N.D., 2019. Designing a Biometric (Finger) Using Multispectral Imaging Biometric Authentication Measures for Enhancing ATM Security in Nigeria.
14. Balwir, S.P., Katole, K.R., Thakare, R.D., Panchbudhe, N.S. and Balwir, P.K., 2014. Secured ATM Transaction System Using Micro-Controller. *International Journal of Advanced Research in computer science and software engineering*, *4*(4).
15. Ajaykumar, M. and Kumar, N.B., 2013. Anti-theft ATM machine using vibration detection sensor. *international journal of advanced research in computer science and software engineering*, *3*(12).

AUTHORS PROFILE

Anjalin Joy, received her B. Tech degree in Computer Science and Engineering from Calicut University, India in 2012. She is an M Tech student in Embedded Systems at Sahrdaya College of Engineering and Technology, Kodakara under KTU.

Dr.Caren Babu, received her B. Tech degree in Electronics and Communication Engineering from Calicut University, India in 2010 and her M.E degree in Communication Systems, from Anna University, India in 2012. She completed her Ph.D. degree in Electronics and Communication Engineering from Karunya Institute of Technology and Sciences, Coimbatore, India in 2020. She is working as Assistant Professor with the Electronics and Communication Engineering Department, Sahrdaya College of Engineering and Technology, Kerala, India. Her research interests include image processing, compression and medical image analysis. She is a life member of ISTE.