Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 6, July 2021 : 5804 - 5814

Research Article

Smart ATM Security System

L.Annie Isabella [a],Aravindharaj P [b], Barath E[c], Barath W[d], Sriganesh K[e],A.Xavier[f]

[a] Assistant Professor, Department of Electrical and Electronics Engineering , [b,c,d,e,f] Students, Department of Electrical and Electronics Engineering
[a,b,c,d,e,f] RMK Engineering College, Chennai. 6Manager,Net-Access India pvt Ltd
[a] lai.eee@rmkec.ac.in, [b] arav17110.ee@rmkec.ac.in,[c] bara17115.ee@rmkec.ac.in,
[d]bara17116.ee@rmkec.ac.in,[e] srile18125.ee@rmkec.ac.in,[f] antxav1978@gmail.com

Abstract

In the current world, the use of ATM to pull out cash has been expanded additionally robbery cases have likewise expanded. We need more secured system which adds second layer of security. In this paper, we are proposing a new technique by using both finger print and RFID for ATM transaction. The transaction will happen in two phases, for the original user, he can swipe/scan his card in ATM, after he scans his fingerprint, then the transaction will begin and he can withdraw his money. For other users the transaction is done by a second person who has RFID card and it will picture the face and send the image of the person through mail. If the card holder responds to the message, the transaction will proceed. If any unauthorized transaction take place user will receive a message. The transaction will take place only if the original user responds. The ultimate aim of this paper is to secure the ATM transactions that is made by the unauthorised person and also notify the transaction to the cardholder for his concern

Keywords

1. Introduction

ATM (Automated Teller Machine) is a machine that helps customers of banks to access their account for making cash transaction without going to bank's branch office. ATMs were introduced in London in 1967 and then 50 years, these machines are introduced worldwide later on.In ATMs cash can be withdrawn in multiple banks for 24*7 and also located in different places. The ATM can be used only the person who knows the PIN Number which is given to access their own individual account. ATMs to reduce lot of time by not allowing person to stand in queue.

The ATM facilities various transaction which can be done in banks such as (cash withdrawal and checking account balance, modern ATMs are used to open a fixed deposit with a bank, recharge mobile, pay income tax, deposit cash, pay the insurance premium, apply for a personal loan, transferring cash, paying the bill, booking railway ticket, etc).Since in india more Atm's are located there are also lot of chances of theft happening in today's scenario.Thus in addition to security officers at the ATM, more security methods are needed.report from RBI says, Fraudsters siphoned off ₹615.39 crore in more than 1.17 lakh cases of credit and debit card frauds in ATMs over last 10 years [2].

Table I. Timeline of an Atm

Period	Development
1988 – 1994 (The starting period)	Cash deposit and cash withdrawal
1995 – 1999 (Initial developments)	Mini statements and balance
2002 – 2007	Fund transfers
2007 onwards	Customized ATM services

There was an investigation directed to evaluate the operational highlights of the ATM and the variables that represent customers‟ ability to utilize ATM. The investigation demonstrated the operational highlights of ATM utilizing lining displaying and model was assessed to decide the elements influencing client use of ATM. Information was gathered from 160 clients of banks with ATM offices .It was understood that there is a high traffic power for ATMs use for most banks in the Municipality. Additionally, higher instructive achievement, number of ATMs per bank, accommodation, security highlights, effectiveness and low transaction charges have critical impact on affecting the utilization of ATM administrations. It is suggested that administration of these banks need to upsurge the number and nature of ATM administrations to expand access and use of ATM. [2]

The fresher age of ATM card is presented for the current ATM machine. Rather than the ATM card, machine can be worked through the RFID tags. These RFID tags shut down the use of many number of ATM cards and gives an office to coordinate it into a solitary card named RFID Safer cards. At the point when the more secure card is embedded in the ATM machine the peruser unit present in the machine, at that point the data about the card holder will be shipped off the worker. Data identified with the client, for example, their record subtleties, photo will be gotten from the worker. In the interim the camera inserted in the machine will catch the picture of the client and it will be contrasted and the picture put away in the worker. Thus the improvement of security will be profited when contrasted with the current ATM machine since it offers both the secret key and biometric limit. In the event that the specific picture matches with the database it demands for the pin number and the transaction preparing will be started. In any case the transaction will be cut off. At the point when the client's picture matches with the database the framework created OTP will be shipped off the client's portable. At that point the client needs to enter the got OTP to proceed with the banking cycle. Subsequently by utilizing this framework ATM card utilization will be totally wiped out and it tends to be finished by the RFID more secure card. Framework breakdown can likewise be kept away from which will make our transaction safer.

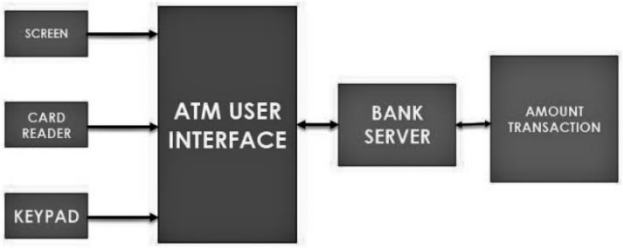
2. The Existing System

The existing ATM supports two types of methods. The firstly it allows the customer to know the cash requested and sends a message with an proof of the amount withdrawn and balance account[3]. The second one is to accept the deposit from the owner and features the credit card payment facilities, and sends a message to the owner about the process details and account information.

The current system of ATM as shown in Fig. 1. The contribution to the ATM is perceived through the information gadgets, for example, card reader and keypad. The card reader is an information gadget that is utilized to peruse information from the card which recognizes the client's card number. The card is either swiped or pressed on the card reader that catches the record data once an association is set up with the magnetic strip on the rear of the ATM card [18].

This data is passed to the host server that utilizes the information to get insights regarding the cardholder. The RFID card is perceived utilizing a Personal Identification Number (PIN). After the PIN is approved, the client can pick any help given by the ATM through the keypad. To guarantee security, each card has an interesting PIN and the PIN is shipped off the host processor in the encoded structure.

Fig. 1: Schematic Diagram of Existing System



Normally, in existing system transaction will be successful once if the user enters the correct pin of that particular card. But there are some drawbacks as server will not identify the user and process the user transaction but that transaction might be done any false user as in online transaction there is lot of security issues. As there is advanced technology that user to hack the user card detail including user pin number.[3],[15].

1. Merits:

- This system just sends a message to the original user as soon as the transaction begin.
- This has much flexibility to such an extent that the client needn't go to the ATM rather any individual who knows the card's PIN can access the card.
- Each card has special PIN.
- Simple
- User friendly.
- Less time for transactions.

2. Demerits:

- Criminals can fit tiny cameras to ATMs that can record account subtleties and PIN that increase the dangers of misrepresentation and theft.
- The user doesn’t get any message about the unauthorized transaction.
- The user doesn’t get information rather than type, location
- Less Secure (only four Digit Password),

3. The Proposed System of the Atm

In this system, wherein normal cards are supplanted with RFID cards that contain the card number of the user. Rather than utilizing the PIN, the fingerprint of the client is checked and his/her additionally card is examined by the RFID scanner and the system hangs tight for the legitimate fingerprint of the relating card. In the event that a substantial fingerprint is perceived by the fingerprint sensor of the ATM the transaction will occur, On the other hand, if an invalid fingerprint is perceived, the transaction will be shut. Despite if the access is allowed or not, the cardholder additionally gets details about the time & location of the access.

This schematic diagram in Fig.2 shows the working of the proposed system. Here the system uses hardware components like RFID scanner and cards, fingerprint sensor, Node MCU, It uses software platforms including Arduino IDE for processing the received input from the sensor and scanners to send messages and firebase.

The fingerprint processing mainly includes two elements namely enrolment and matching. In fingerprint enrolling, every cardholder requires to place the finger twice on the sensor that the system checks the finger images to process and generates a pattern of the finger. The enrolled fingerprint is stored. In matching,

during the ATM access, the user places the finger on the optical sensor after which the system produces a pattern of the finger and compares it with those fingers enrolled in the finger library templates.

[11]The main reason for NodeMCU is used is that it has a built-in WiFi module in it that helps to send the necessary values to the cloud database, in this case, it is the firebase. The MFRC522 module used as the user's card and the corresponding card reader uses electromagnetic fields to transfer data over a short distance. An R307 fingerprint module is used for getting the fingerprint as primary protection for authentication from the original user.

Fig.1.1 FingerPrint Module

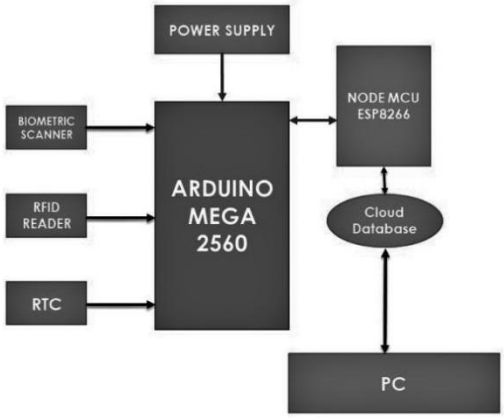
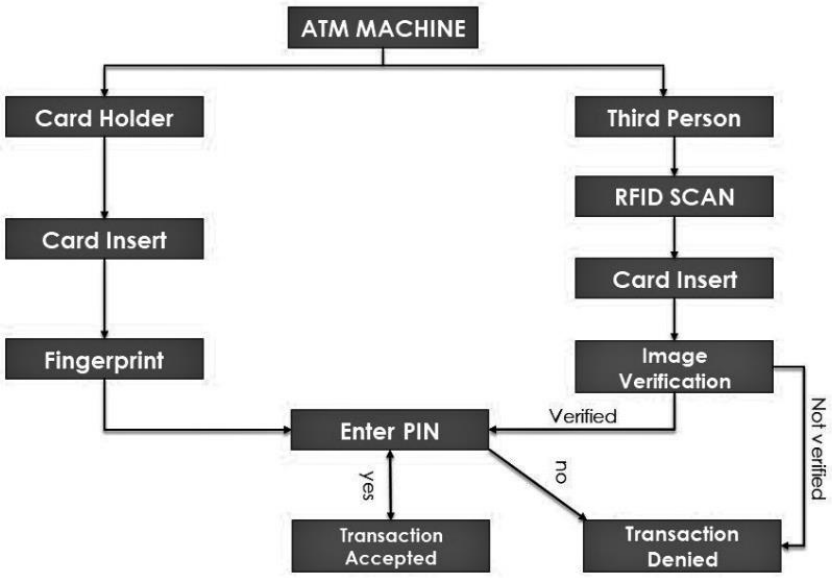


Fig.2: Schematic Diagram of Proposed System.

The schematic diagram contains Arduino, ESP8266 (NODE MCU), biometric sensor, RFID and camera. Biometric sensor and RFID reader are connected to the UART port of Arduino. ESP8266 (NODE MCU) is used to send user detail to the cloud. The biometric sensor gets finger print from users and give it to the controller. The controller will compare the users finger print with the database. If any third person access the ATM machine for money transaction, system will take images of the person and send to the corresponding user.

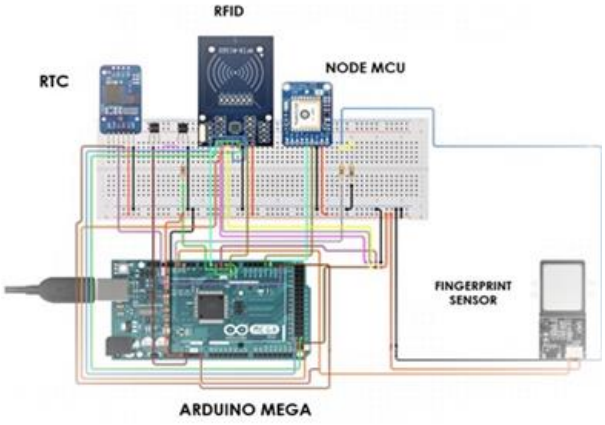
Fig.3 Flow chart of our system.



A) Software Requirements:
1. C Program
2. Arduino compiler
3. Python 3.6
4. HTML
5. Google Firebase

B) Hardware Components:
1. ARDUINO MEGA 2560,
2. ESP8266 (NODE MCU),
3. Power Supply unit
4. Push Button
5. LCD Display(16x1)
6. BIOMETRIC SENSOR (R305)
7. RFID READER,
8. Laptop with Camera.

Fig.4: Model Circuit DiagramFig.5 Circuit Diagram



4. Results And Discussion

We have created a login page for user login as shown in figure 6, also there will be a separate portal for account creation and viewing all the unauthorized transactional data to the user. At the point whenever a transaction happens or any attempt for a transaction is made, there will be separate values get refreshed in the firebase (the dataset utilized).Following this, the respective values for RFID card number, user ID, location of the access, access status, flame, and vibration sensor status are updated in the firebase portal which can be viewed whenever needed. Each header is defined using various RFIDs as separate ATMs.

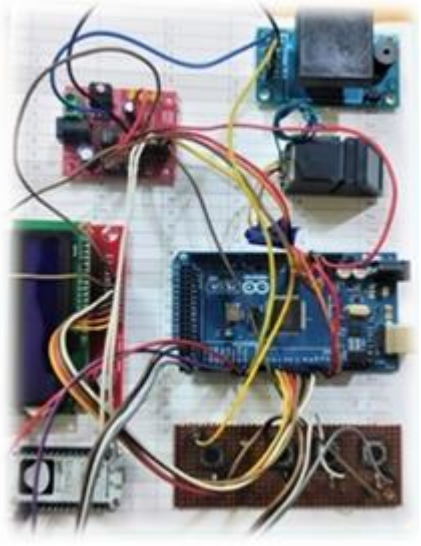


Fig.5 Circuit Diagram

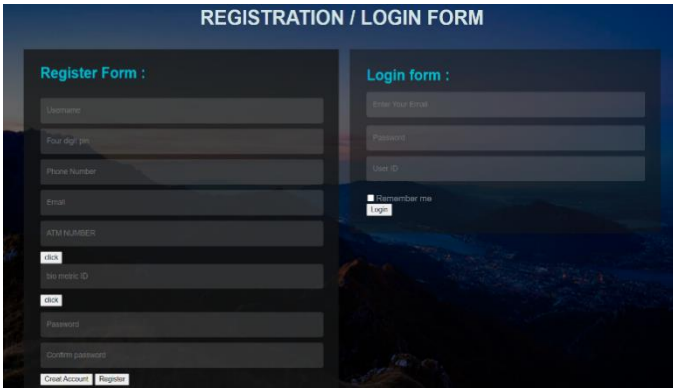


Fig.6: Login Page

There are mainly three possible ways, The main case happens when a original user uses or attempts to access through an invalid card. For this situation, the ATM shows it as an invalid.

The subsequent case happens when the user accesses the system utilizing a legitimate card and give in the comparing substantial fingerprint for the card. For this situation, the access is allowed and the estimations of the RFID card number, area, and time of access are refreshed in the Firebase and they are recovered through the application as shown in fig. 7. From firebase.

Fig.7: Recorded in Firebase

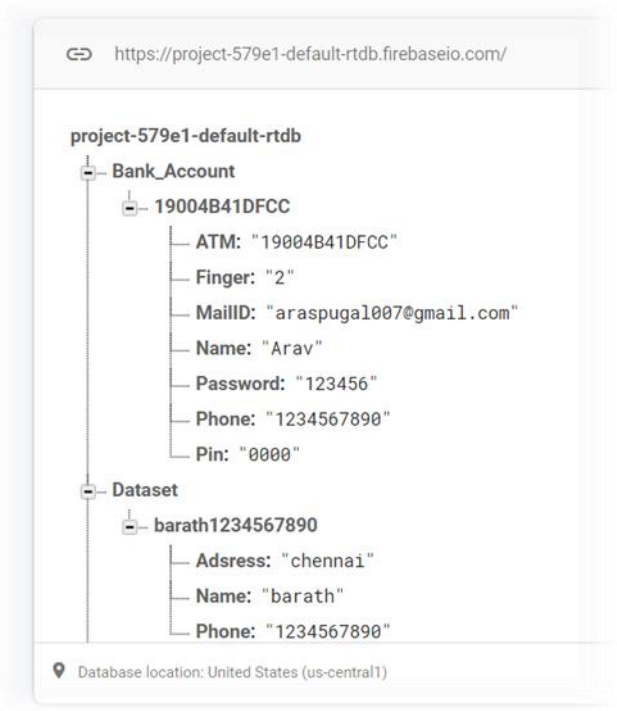


TABLE:2 Comparison of Existing & Proposed System

Existing System	**Proposed System**
Less Secure (only four Digit Password),	Much secure than existing system
Less time for transactions,	Same time as the existing system
Simple and User friendly.	Its also simple and user friendly.
User only receive the message after transaction	User will receive who access the ATM.
Anyone can access the ATM, if PIN is known	It has two level protection
It has high flexibility	Its not as flexible as existing, this paper aims at security.

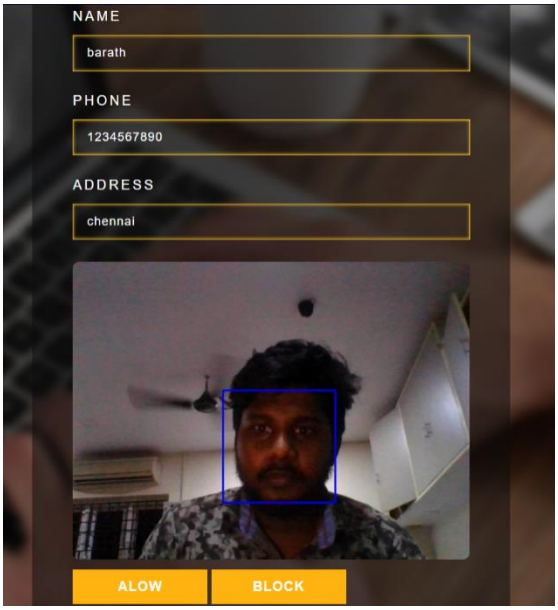
In this case happens when the entrance for the framework is given by a original card yet it is given an invalid mark for the separate card. Transaction isn't allowed for this situation as the system expects the relating unique mark for the card enlisted already. The qualities for the RFID card number, area, and time of transaction are refreshed in the Firebase and are recovered.

A message is sent to the registered mail address of the original user stating that " the your card been tried for access at this location and other details."

Fig.8: Invalid Finger

To keep track of unauthorized transaction in ATMs, the image of the person will be captured using the camera which is present in the ATMs. Here we used python programming for image detection which captures the face of the person and stores it to the database which can recognize the face.

Fig.9 facial data as displayed in the webpage



To carry out this, the "OpenCV" module in python is utilized. We used a classifier which is utilized in the code which uses object identification calculation to recognize objects in a picture or a video as demonstrated in fig 10. At the point when the program is executed, the camera looks for a face with the assistance of the facial highlights utilizing the classifier. When the face is remembered, it is flipped, reshaped and featured. A rectangular box is drawn around the face and is pushed to the data set. The catching of the substance of the client is appeared in Fig.9 These can make ready for an ATM framework to be successful, secure, and effectively available.

As the above table compared the differences between the existing and proposed system. This shows a clear picture that the existing system has much more advantages than the current system.

Some of the parameters are compared with the existing system like flexibility, reliability, time, security, accessibility, etc., are compared. We can clearly find the differences between the above two systems.

Fig.10: Dataset of Image recorded using OpenCV.

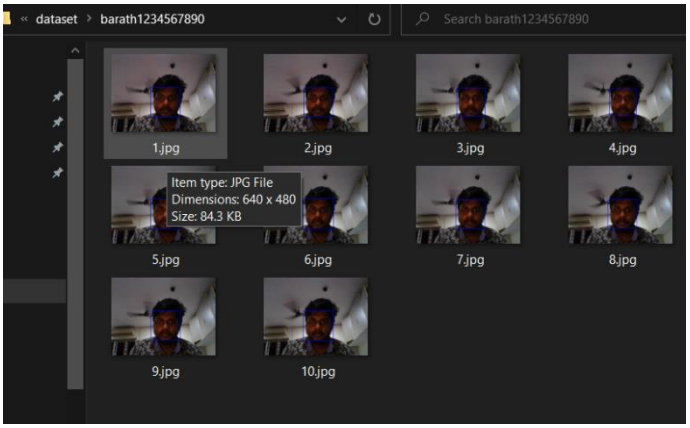
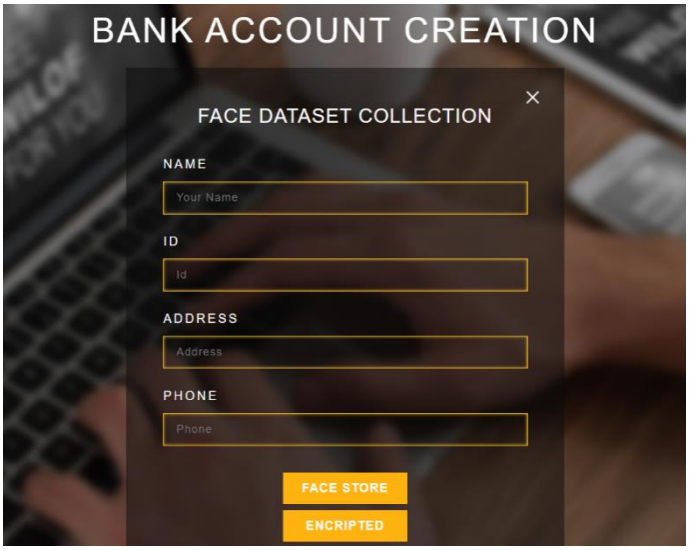
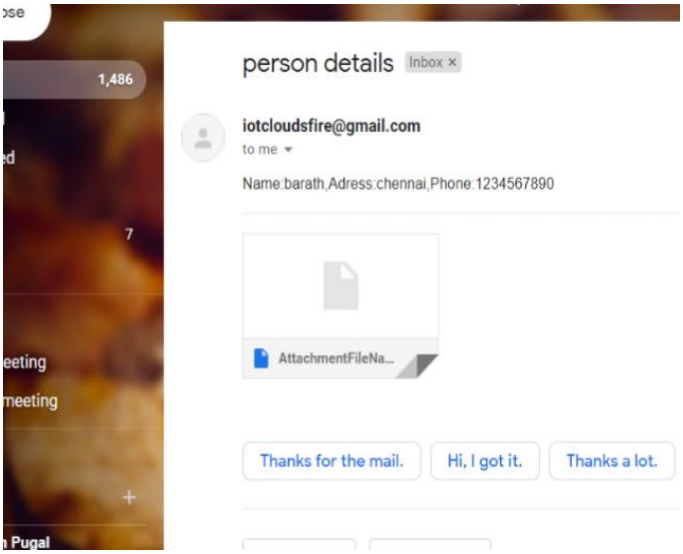


Fig.11: User login portal



Once the RFID is scanned the system checks for PIN and sends the information if unauthorized transaction take place. The message will be in the form of text containing the attachment file of image. Name, Address, Mobile Number, Image of the person who used that RFID card as shown in fig.12.

Fig.12 Mail received from the server.



5. Conclusion

This system uses both RFID as well as fingerprint for security purposes. For multiple bank accounts, different RFIDs can be used. The card which is closest to the proximity of the reader will be considered for operation. It increases the security by notifying messages to the card owners to his register phone number about the data such as location, date, and time, also about the transaction is approved or not. There should be a separate camera which should runs continuously and checks in the ATM that helps in cases of fraud. It will prevent many accidents and theft activities, also adds second layer of protection.

Many researchers in [21] discussed system user identification and authentication and proposed an embedded fingerprint biometric authentication scheme for Automated Teller Machine (ATM) banking systems.

[22] A three tier design structure was demonstrated in the proposed system. The first tier concentrates on the biometric feature from enrollment to matching, the second tier concentrates on the database and face recognition and the third tier concentrates on ATM transactions like balance enquiry and cash withdrawals.

[23] Many analysed the issues and challenges that the existing ATM infrastructure has and the ones faced by ATM users. It was concluded that ATMs have become very important to society that many people are dependent on it. The use of biometrics for authentication on the ATM was proposed.

In addition to sending the user's location of the ATM, the amount withdrawn, the image of the face of the user can also be sent. Since the fraud in fingerprint recognition has increased, to ensure security towards this issue in the proposed system, extra layers of safety measure like facial detection, iris scanner can be added..

References

[1] The Times of India, "Atm Crimes". Available: https://timesofindia.indiatimes.com/topic/Atm-Crimes [Accessed: May 08,2020].

[2] S. Hazra, "Smart ATM Service," 2019 Devices for Integrated Circuit (DevIC), Kalyani, India, 2019, pp. 226- 230.

[3] K. Archana, P. B. Reddy and A. Govardhan, "To enhance the security for ATM with the help of sensor and controllers, "2017 Internation Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 1012-101.

[4] V. M. E. Jacintha, S. J. Rani, J. G. Beula and J. J. Johnsly, "An extensive resolution of ATM security systems," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM),Chennai,2017,pp.934-938,doi: 10.1109/ICONSTEM.2017.8261340.

[5] Rhydo Labz. R30X Series Fingerprint Identification Module User Manual. Available: https://www.rhydolabz.com/documents/finger-print¬module.pdf.

[6] V. Ashokan and Murthy, O. V. R., “Comparative evaluation of classifiers for abnormal event detection in ATMs”, in 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2017, 2018, vol. 2018-January, pp. 1330-1333.

[7] Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani, “ATM Security Using Fingerprint Biometric Identifer: An Investigative Study”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012, pp. 68-72

[8] Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, “Fingerprint Matching”, IEEE Computer Society 2010, pp. 36-44.

[9] N. K. Gyamfi, M. A. Mohammed, K. Nuamah-Gyambra, F. Katsriku and J.-D. Abdulah, "Enhancing the Security Features of Automated Teller Machines (ATMs): A Ghanaian Perspective," International Journal of Applied Science and Technology, vol. 6, no. 1, 2016.

[10] K. Namusa, "Zambia: Cyber Crime Costs Banks U.S.$4 Million," Allafrica, 14 June 2013. http://allafrica.com/stories/201306141287.html

[11] J. Bloomberg, "ATM 'Jackpotting' Attacks Reveal Deeper Problems," 12 02 2018. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2018/02/12/atm-jackpotting-attacks-reveal-deeper-problems/#5b1147ee6fc3. [Accessed 10 04 2018].

[12] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Computing Surveys, to be published. https://doi.org/10.1145/2333112.2333114.

[13] W. E. Burr, D. F. Dodson, and W. T. Polk, Electronic authentica-tion guidelines NIST Special Publication 800-63, Apr. 2006 [Online]. Availa-ble:http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[14] J. Bloomberg, "ATM 'Jackpotting' Attacks Reveal Deeper Problems," 12 02 2018. [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2018/02/12/atm-jackpotting-attacks-reveal-deeper-problems/#5b1147ee6fc3. [Accessed 10 04 2018].

[15] N. K. Gyamfi , M. A. Mohammed , K. Nuamah-Gyambra , . F. Katsriku and J.-D. Abdulah, International Journal of Applied Science and Technology, pp. 102-111, 2016.

[16] F. Twum, K. Nti and M. Asante, "Improving Security Levels In Automatic Teller Machines Using Multifactor Authentication," International Journal of Science and Engineering Applications, pp. 126-134, 2016.

[17] P. Jindal and R. Kumar, "Analysis of Security System for ATM," in 4th International Conference on System Modeling & Advancement in Research Trends (SMART) , Moradabad, 2015.

[18] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, “Multiple password interference in text and click-based graphical passwords,” in Proc. ACM Computer and Communications Securi-ty (CCS’09), Chicago, IL, Nov. 2009. https://doi.org/10.1145/1653662.1653722.

[19] S. Chiasson, P. van Oorschot, and R. Biddle, “A usability study and critique of two password managers,” in Proc. USENIX Security Symp., Vancouver, Canada, Aug. 2006.

[20] D. Davis, F. Monrose, and M. K. Reiter, “On user choice in graph-ical password schemes,” in Proc. USENIX Security Symp., SanDi-ego, CA, Aug. 2004.

[21] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, “A comprehen-sive study of frequency, interference, and training of multiple graphical passwords,” in Proc. Conf. Human Factors in Computing Syst.(CHI’09), Boston, MA, Apr. 2009. https://doi.org/10.1145/1518701.1518837.

[22] Der Chin Chen, “Portable Biometric System of High Sensitivity Absorption Detection”, Biometric Systems, Design and Applications, 201