International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

Multifactor Authentication for ATM Security System

[1]Suseenthiraraj.S.V, [2]Vijay Swaminath.R

[1,2][Student], B.tech, Department of Computer Science and Engineering,
B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai-600048,India
[1]suseenraj@gmail.com, [2]swaminath.vijay@gmail.com

Abstract: To accomplish most types of banking and non-financial operations ATM machines are heavily been used by people. Nowadays, cash withdrawl can be done by any person who has the card and the pin number. So to have secured transactions under account holder's knowledge, we use Fingerprint Scanners and Facial Recognition for authentication.We have a fingerprint and face Id encryption in the database of an individual in order to ensure safety. So, If one enters the phone number as their Login ID, then the facial recognition gets triggered and captures the face ID of the cardholder and it starts inspecting with the database whether it is matching or not. It also starts recognizing the fingerprint and verifies the identity for authentication. If their fingerprint is not matching with the original account holder, the ATM system denies access for withdrawal. If the account holder gets into their ATM system, It identifies the face first then verifies fingerprint and matches it with its database, if validated, It will directly allow users to perform all banking processes from ATM if not it denies the access.

Keywords: ATM; Fingerprint scanner; Facial recognition; Security.

1. INTRODUCTION

The Automated Teller Machine (ATM) is a machine that uses an automated technique that permits the customers to perform all sorts of economic transactions such as cash withdrawal, cash deposit, balance inquiry, Mini Statement and so on irrespective of time and location without the assistance of a bank representative. Despite a marginal increase, in digital payments still, the economy is dominated by cash transactions compared to digital payments and it is observed that the number of crimes related to ATM has been increased hence there is a necessity to provide enhances security to the ATM machine. According to the traditional ATM system in order to access it, customers must hold a debit/credit card along with the respective PIN number but this limits the security. New ideas and implementation such as GSM-based security in the form of OTP or introduction of card-less withdrawal by generating unique keys and knowing the account number enhances the security but only up to some extent. Since the OTP's aren't completely safe in case you lose your mobile phone transactions cannot be performed and it's difficult for the customer to remember the account number, the unique key combined with OTP for a single transaction creates a hassle. Bio-metric features can be a solution to this kind of problem. Among all biometric features, fingerprint and facial recognition are proven to be the most effective and easy to implement systems across multiple ATM machines. Both the finger print the face recognition cannot be duplicated as these are the unique features that can be faked. There is no worry about losing the ATM card and no need to carry the ATM card with you always. Now a days finger print and the face id serves as a better encryption standars in order to keep the transaction much more safer. The user who access the atm card will find it easy and secure.This is the most promising technology in electronic money transactions. The expansion in electronic transactions caused a larger demand for ultrafast and precise user identification as well as authentication. Incidentally, our proposed system is based on a multifactor authentication of biometrics that includes Fingerprint scanning and facial recognition for precise identification and authentication of legitimate customers during an ATM transaction. Since it is highly impossible to crack down duplication of these biometric features like fingerprint and Face ID, to solve the authentication problem, this proposal can be a better solution.

2. RELATED WORKS

The current paper depicts about deign for developing the security system of ATM by way of a unified private server to monitor every ATM's in and around the city.

Information regarding Security is bagged with the use of a various number of sensors as well as switches [1]. The information is then administered also moved to the main server to the latter analysis presentation of data. Data received from the sensors are directed endlessly at present for building a complete database. This Machine also executes analysis of statistical vulnerability with the use of data established on a number of sensors from dissimilar ATMs. Then it allocates a quotient of vulnerability for every ATM. hence supporting the main system to identify security gaps in a single Atm. The current system tries to find an effective measure for preventing risks linked with the ATMs.

To offer a trustworthy security solution to the people, the concept of a smart ATM is based on the Embedded Linux platform is submitted in this paper. The execution of a face-based detection system in an ATM under the Linux platform is implemented[2] A raspberry pi in a size of a credit card which also has OpenCV software mainly used for every image processing operation. The system initially captures the human face and check whether the face detected is proper or not. If the face detected is improper, it warns the user to adjust themselves accordingly to obtain a clear face. Still, if the problem exists the system will lock the door of the ATM cabin inevitably for security purposes. Once the door is locked, the system will generate a 3 digit OTP code. This code is sent to the watchman's registered mobile number via SMS using the GSM module present, which is connected to a raspberry pi. This generated OTP will be entered by the watchman to unlock the door.

[3]The current research reports about the latest ideas regarding ATM Security systems. The ultimate aim of this paper was recognizing the Enhanced ATM smart security system that was designed with the help of an embedded system and urbanized technologies. In this structure, the RFID card was being utilized instead of an ATM card. To know about the presence of the cardholders and for switching on fans and lights IR sensors are utilized. In case of the ATM being meddled an SMS is pushed towards two important points through GSM. If the cash box is robbed, GPS has been employed for tracing the location. Identification is done through fingerprint as well as for finding the authorized bank personnel. Thence this proposed method was considered to be a high-level secured system for Automated Teller Machines.

Technologies transform at a rapid pace focusing on reliability and ease of use and so do the security issues. Taking into account the current PIN security system of the ATM end up making customers vulnerable to attackers and less secured for authentication purposes, which paved way for a new biometric system coupled with ATM PIN instead of a single PIN only authentication which is easy to steal or guess. Biometrics are added advantage with the existing technology, to improvise the security in order to reduce ATM frauds but on the flip side, it has several issues which include sensor durability and time consumption [4]. The introduction of this new system arises after a severe analysis based on the need for the biometric processes even for lower denominations and in case of a card loss/misuse. So we implement biometrics combined with minimal constraints while performing transactions using ATM involving biometrics to improvise the performance of the system and to solve the defined issues. This proposal is separated into two parts. The first part deals with the sensor's performance issue which is solved by adding a limit on to the cash withdrawal and number of transactions. so only if a person needs to withdraw a huge amount or to perform multiple transactions by withdrawing small amounts, continuously, it shall be necessary to present biometrics. On the other hand, if one needs to withdraw a negligible amount and does fewer transactions and perform nonfinancial transactions such as balance inquiry, a mini statement and a PIN change a biometric presentation are not mandatory. This saves time and maintains the sensor performance. In the next part, this paper speaks about allowing the customer to access the system every time and check the performance of the biometrics and find a new way to improvise the efficiency of the system.

In every organization, Security has been a vital subject in the present day. Because of many types of an outbreak on the communication network, transmitting information from one person to others creates a lot of difficulties [5]. In addition to these outbreaks on communication systems, there are also attacks happening for physical access medium. Physical access comprises authentication, as well as verification and access control. By installing a skimming device on a swipe machine an attacker can able to read the information of the magnetic stripe of a credit or debit card. The current paper provides a suggestion for safeguarding electronic data capture machine's transaction by augmenting biometrics along with a customary PIN. Thence, In the research proposal, the biometric technique with a fingerprint is embedded through PIN (personal identification number) to legalize the users as well as to improve the safety of fund transfer through EDC.

Currently, Individuals utilize a pin number as a security quotient in ATMs, that substituted the system which

involved the signature-based method [6]. The security-based on the pin was the easiest level for security. pin number was a special number that performs encryption as well as decryption during the transaction. Fraudulent activists can retrieve our PIN number in so many ways. So, biometric authentication can be used instead of the usual Pin number authentication as a solution. Fingerprint, retina and some others can be used as an input to the biometric security. These days, systems are utilized for comparing an intake picture with the picture stored in a database and once they get authenticated, the money can be withdrawn by the user. The cash will be withdrawn if the similarity between the data matches, and so this system will totally replace the PIN number system by the Biometric system. Thence, the security in the transactions is enhanced to a larger extent.

Dealing with distinct fingerprints confronts the rise in usage of the automated fingerprint recognition system. Quality control is needed to assist the fingerprint details for verification. Personal identification methods are often depending on fingerprint verification; also it performs a major role in forensic applications such as criminal investigations, terrorist identification, and National security issues[7]. Fingerprint identification algorithms like Fast Fourier Transform, Minutiae Extraction needs a lot of evaluation which makes the process absurd. The overall system performance is based on the fingerprint quality, but the quality of fingerprints differs by the user's age, thus it is necessary to interpret fingerprints of various age groups.

[8]In the present circumstances, the world is being changed by the process by which the banking and transactions take place, the attestation, verification, and confirmation of a user is extremely significant. Corroboration and validation have been the segment to concern regarding the security and secrecy of the customers. In the fast-evolving environment, it does not so ease to sustain honesty and verification of the users. At present, there is a great deal of threat of losing the cash and find when we lost our Automated Teller Machine (ATM) PIN. We don't even know whether it is hacked or not if so our entire money can be lost. To avoid all the cheats, we require an unerring security explication that we could utilize together with the presently accessible devices. The current technology available can be integrated with the bio-metric proofing system. We could utilize palm scanning, thumbprints, iris-scan together with the PIN verification and corroboration. Voice recognition can also be used. Integration of these technologies can assist in minimizing the ATM cheats and the financial transactions can be enhanced by other security measures.

This paper uses an Advanced Encryption Standard (AES) to provide an extremely secured ATM banking system. This suggested system offers dual-level security. A 4-digit long passkey from the client side along with the biometric verification is taken into account primarily. The fingerprint of the user is used in order to implement the biometric verification [9]. An optimized power effective AES processor is used to provide a secure communication link with the user system to the bank server. In this encryption process, the 4-digit long passkey is considered to be the symmetric key and the image of the fingerprint is considered to be the data for the encryption process. In order to obtain a less energy exhausting ATM system, an optimized AES algorithm is suggested. This system uses cryptography techniques and bio-metrics combined in order to provide personal identification to enhance the security level. The structure of the power effective AES processor is simulated in Quartus-II software. The simulation outcome guarantees functional capability.

From Biometric System, a recognition done using Fingerprint was researched to more extent of time as well as it shows a greater part of prominent hope to a real-time application. Conversely, due to tough distortions among dissimilar impressions of the same finger from a hand in real life, The recognition of fingerprint is still an existing problem. toning multiple fingerprints may be an unsuccessful attempt because of several bases as well as it depends on an approach that was utilized to match[10]. Electronic voting machine (EVM) is an easier to use electronic device which is utilized for recording votes instead of ballot paper counting from the ballot boxes that are frequently used as a traditional system of voting. Due to identifiers of Biometrics which may not be simply mislaid, copied, or transported, which were measured high dependable to recognize a person when compared to a conventional token or else methods based on knowledge. From this proposal, Researchers were keen on differentiating three fingerprint toning procedures through performing an election with the use of EVM. With regards to the result in stipulations for accuracy toning, toning time interval, an efficient algorithm was invented to fresh EVM. Some matching methodologies which were used are miniature matching, Ratio-based matching for distance and matching based direct matching. The author conducts an evaluation for the FVC-2000 dataset as well as the conclusions are noted through the conduction of an election by utilizing these toning procedures. Thence, an ultimate toning procedure was established to novel EVM.

Bio-metrics depended verification deliver several benefits over another verification approaches, this will replace the password depended verification and token depended on verification. The important part form Bio-metrics is from the cash machine system, Passport, Online banking, E-Commerce [11]. The development in digital transactions have been grown enormously; It has a higher requirement for quick and precise customer recognition and verification. In a sharing system like the cash machine system, security is an important subject. The security levels have developed on the basis of offering a PIN (Personal Identification Number) to chip Card to Bio-metrics. Despite the security have been developed, simultaneously false operations have matured to the same level. In order to vanquish the hacking operations, the suggested work is improved to give security to the biometric pattern and to strengthen the security in the cash machine system with poly-biometrics, poly-modal bio-metrics, and Two-tier security. Bio-metrics together with cryptography is utilized to encode the pattern that is kept in the database. Biometric crypto-system design specifically the fuzzy vault and the fuzzy commitment is employed to safeguard the pattern that is retrieved from the bio-metrics.

This development to an electronic transaction has caused a superior plea to quick as well as perfect identification of user and verification. Personal Identification Number is used to access codes for buildings, bank accounts and computer systems for identification as well as clearance in security. Regular procedures to identify such as Identity cards else a number for social security or else a passkey were not all organized dependable [12]. The Embedded Fingerprint Authentication based on Fingerprint scheme to Automated Teller Machines banking organizations were presented briefly in the paper. From the method, Biometric based fingerprint practice was fused to an ATM for authentication of a person to security level up-gradation.

Table 1. Key Findings and Interpretation

S NO	PAPER PUBLICATION	JOURNAL /EDITION	FEATURES	INTERPRETATION
1	Centralized Server Based ATM Security System with Statistical Vulnerability Prediction Capability	IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2017.	The system focuses on the Hardware security of the ATM by connecting all ATM to a central private server to monitor the activities of the ATM center.	A centralized server is not safe since it's prone to hack a decentralized server can be used
2	Face Detection based ATM Security System using Embedded Linux Platform	2nd International Conference for Convergence in Technology (I2CT),2017.	The system speaks about the identification of a moving object (a person) inside the ATM room using a face recognition algorithm but it doesn't work as an authentication or identification tool for performing banking operations.	Haar cascade proves to be the best algorithm for Face recognition
3	Smart ATM Security System Using FPR, GSM, GPS	International Conference on Inventive Computation Technologies (ICICT), pp. 26-27, Aug 2016.	An infrared sensor is utilized to recognize the card owner and fingerprint to identify and validate the customer. GSM module is used to send SMS between two addresses and GPS service aids to detect the place of cash withdrawal.	Fingerprint feature can be enhanced for better security

4	A Constraint-based Biometric Scheme on ATM and Swiping Machine	International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),2016.	Proposal of a new method to solve the overuse of fingerprint sensor issue by allowing some transaction under certain conditions to undergo biometric authentication and not every transaction.	ATM System security is deficient since every transaction doesn't require biometric authentication
5	Secure Swipe Machine with Help of Biometric Security	International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp.1056-1061.	An Embedded fingerprint feature with the PIN has been introduced in it. Its design is more secure for swipe card transactions by smearing Bio-Metric features like fingerprint identification along with OTP.	OTP isn't hackproof hence fingerprint sensor has to be used wisely to improvise protection.
6	A Novel Method to Enhance the Security of ATM using Biometrics	International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2015.	This model depicts, pin number is completely replaced with a biometric system like Electronic-fingerprint, IRIS and so on.	IRIS sensor is too expensive and tedious for users to use in day to day life
7	To Enhance the Biometric Image using Binarization	International Journal Of Engineering And Computer Science ISSN:2319-7242 Vol. 3 Iss. 6 June 2014 Page No. 6561-6565.	Enhancement of fingerprint by binarization, extraction, segmentation, and matching by implementing various algorithms and techniques.	The fingerprint authentication can be enhanced and the proper algorithm can be used and mentioned
8	Biometrics to Control ATM Scams: A Study	International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2014.	Multiple methods of authentication which includes most advanced methods of iris scanning and palm scanning.	Multiple methods can consume more time and palm scanning may not be accurate all time
9	Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor	International Journal of Information and Computer Science, Vol. 2 Iss. 4, May 2013.	Advanced Encryption standards used and two-level authentication is done.	The symmetric encryption key used is not accurate all the time and may not be feasible
10	A Comparative Study on Fingerprint Matching Algorithms for EVM	Journal of Computer Sciences and Applications, Vol. 1, No. 4, 55-60, 2013.	Various fingerprint algorithms and techniques are compared and tested.	Minutiae-based matching can be used as its best in terms of accuracy and speed
11	Enhance the Security in the ATM System with Multimodal	International Journal of Advanced Research in Computer Science and	Integration of multiple biometrics including the face, fingerprint and iris	Time-consuming process and has higher false-positive rates

	Biometrics and Two-Tier Security	Software Engineering Vol. 3, Iss. 10, Oct 2013.	recognition along with OTP based two-tier security.	
12	ATM Security Using Fingerprint Biometric Identifier: An Investigative Study	(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012.	The study states that the Fingerprint biometric technique is extremely safe and impossible to impersonate compared to traditional PIN or password system.	The fingerprint module used can be strengthened by adding other biometric features.

3. PROPOSED SYSTEM

The system proposed has a unique way of an approach in which the customer does not require a debit card to perform a financial transaction instead it happens through biometric authentication. At first, one does not require to carry a debit card to an ATM rather they could proceed with a cardless method to perform every banking operation. An individual must know their phone number which is linked with their bank account and they can perform operations in ATM further.

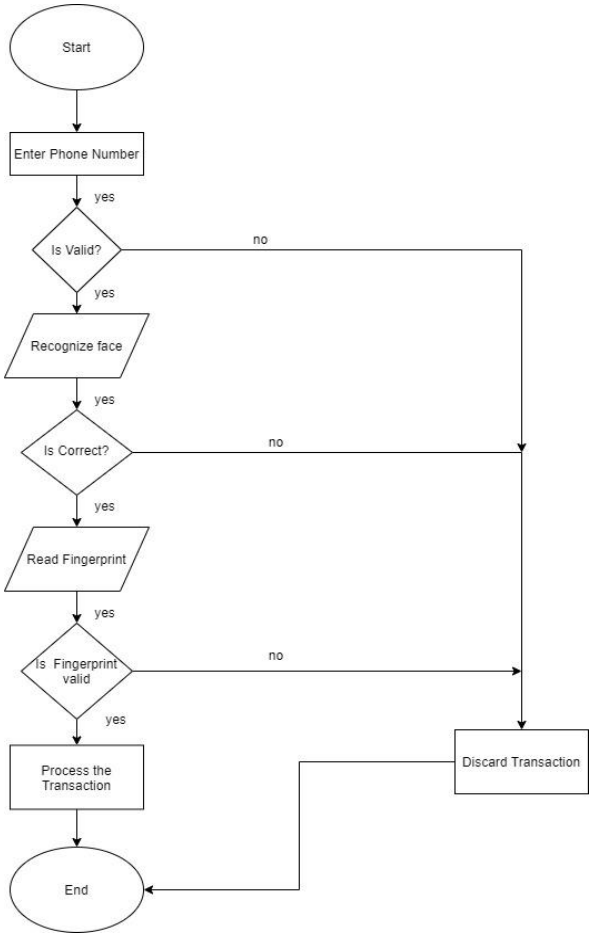

Figure 1. Authentication process in ATM

After entering the credentials, the facial recognition gets provoked and captures the face of the cardholder and it starts examining by utilizing the Haar cascade algorithm to analyze the face captured with the database, to verify whether it gets verified or not. If the system finds an unauthorized user then it denies access for that customer. When the initial part of verification found to be precise then it moves to the following stage of authentication by initiating the recognition of the fingerprint and verifies the identity and strengthens the process of authentication. If an individual's fingerprint does not match with the original account holder, then the ATM system denies access for withdrawal. An account holder who clears both verification stages will directly be allowed to perform all banking processes from ATM.

4. PROPOSED RESULTS

To provide a secure ATM system we deploy biometrics into the system in the form of Fingerprint scanning, facial recognition, Iris scanning, ear, and hand geometry.

Table 2. Characteristics of Biometrics

Biometric Technology	**Accuracy**	**Cost**	**Device Require**	**Social acceptability**
ADN	High	High	Test equipment	Low
Iris Recognition	High	High	Camera	Medium-low
Retinal Scan	High	High	Camera	low
Facial Recognition	Medium-low	Medium	Camera	High
Voice Recognition	Medium	Medium	Microphone	High
Hand Geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature Recognition	Low	Medium	Optic pen	high

Source: http://biometrics.pbworks.com/

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

Among these biometrics, Fingerprint scanning and facial recognition are said to have more adaptability and accuracy which helps the process easier and hassle-free for customers to perform the banking operations by deploying with less expensive components into an ATM system.

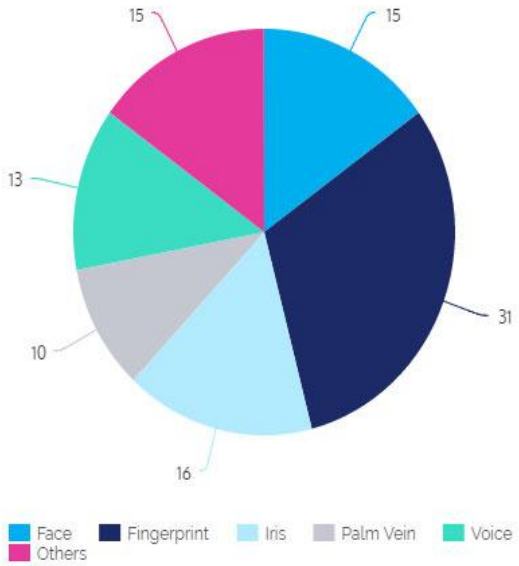

Figure 2. Biometrics rate of Adaption
Source:http://biometrics.pbworks.com/

Integration of face recognition with fingerprint leads way to a better biometric solution when compared with the other biometrics such as iris recognition since it has a low adaptability rate and also it is more expensive than the combination of face and fingerprint scanners to get implemented in an ATM system.

5. CONCLUSION

An increasing rate of electronic transactions surges the need for a secure and reliable transfer system. Currently used PIN-based ATM security system is highly vulnerable to theft, in order to reduce the identity theft rate we are deploying a biometric-based authentication system in this application. Facial recognition, Fingerprint scanning and iris recognition are declared to be the best among other biometric systems with respect to the error rate and response time. Due to a higher setup cost, the iris scanner system is not feasible. Hence by implementing a multifactor authentication system containing Fingerprint and Face ID recognition the security feature is enhanced and making it very hard for hackers to manipulate the customer's identity. This allows customers to perform all banking transactions in the ATM without panic and hassle-free.

REFERENCES

[1] T. Guru Sarath, "Centralized Server Based ATM Security System with Statistical Vulnerability Prediction Capability," IEEE International Conference on Consumer Electronics-Asia [ICCE-Asia], 2017, pp.61-66.

[2] Jignesh J. Patoliya, and Miral M. Desai, "Face detection based ATM security system using embedded Linux platform", 2nd International Conference for Convergence in Technology [ICCT], 2017, pp. 74-78.

[3] Bharati M Nelligani, Dr. N V Uma Reddy, and Mr.NithinAwasti, "Smart ATM Security System Using FPR, GSM, GPS", International Conference on Inventive Computation Technologies [ICICT], Aug. 2016, pp.26-27.

[4] Sweta Singh, Akhilesh Singh, and Rakesh Kumar, "A Constraint-based Biometric Scheme on ATM and Swiping Machine," International Conference on Computational Techniques in Information and Communication Technologies [ICCTICT], 2016.

[5] Akhilesh Singh, Sweta Singh, and Rakesh Kumar," Secure Swipe Machine with Help of Biometric Security," International Conference on Electrical, Electronics, and Optimization Techniques [ICEEOT], 2016, pp.1056-1061.

[6] G. Renee Jebaline, and S. Gomathi, "A Novel Method to Enhance the Security of ATM using Biometrics," International Conference on Circuit, Power and Computing Technologies [ICCPCT], 2015.

[7] Harpreet Kaur, and Aashima Bansal, "To Enhance the Biometric Image using Binarization," International Journal Of Engineering And Computer Science [IJECS], Jun. 2014, Vol. 3, No. 6, pp. 6561-6565.

[8] Ahmad Tasnim Siddiqui, "Biometrics to Control ATM Scams: A Study", International Conference on Circuit, Power and Computing Technologies [ICCPCT],2014.

[9] Fakir Sharif Hossian and Ali Nawaz Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor International Journal of Information and Computer Science Vol. 2 Iss. 4, May. 2013.

[10] D. Ashok Kumar and T. Ummal Sariba Begum A Comparative Study on Fingerprint Matching Algorithms for EVM Journal of Computer Sciences and Applications, 2013, Vol. 1, No. 4, pp. 55-60.

[11] Kande Archana and Dr.A Govardhan Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security International Journal of Advanced Research in Computer Science and Software Engineering Vol. 3, Iss. 10, Oct. 2013.

[12] Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study", International Journal of Advanced Computer Science and Applications [IJACSA], Vol. 3, No.4, 2012.

[13] http:/biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies/

[14] https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

