International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218632

Survey On Biometric Based ATMs

Anukul Muley[1], Akash Bendre[1], Priti Maheshwari[1], Shanmukh Kumbhar[1], Prof. Bhagyashree Dhakulkar[2]

[1]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Maharashtra, India

[2]Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Maharashtra, India

Article Info
Volume 8, Issue 6
Page Number : 292-297

Publication Issue
November-December-2021

Article History
Accepted : 20 Nov 2021
Published : 05 Dec 2021

ABSTRACT

Nowadays Automated Teller Machines (ATMs) are widely used by people. People are dependent upon ATMs to conveniently meet their day-to-day needs. As it is an important factor there comes security. ATMs are electronic machines that are operated by customers to deposit or withdraw cash from banks. It is observed that the number of crimes related to ATMs is increased hence there is a need to provide better security to ATM machines. There are different technologies that are used to provide security to ATM machine which includes – RFID technology, fingerprint, face recognition, iris scan, OTP, reference number, random keypad, etc. In a traditional ATM system card and PIN numbers are used for authentication, where security plays a big concern, such as losing cards, stolen pin numbers, card cloning, shoulder surfing, fake keyboard, skimming, etc. In order to overcome these issues, this paper discusses various systems where ATM cards and pins are replaced by biometrics and how they made ATMs more secure.

Keywords : Facial Recognition, Iris, Fingerprint, OTP, PIN.

I. INTRODUCTION

Automated Teller Machines (ATMs) have become an essential part of our life. It plays a vital role in our daily transactions. An ATM is an electronic banking machine that allows customers to complete basic transactions without going to the bank. Anyone with just a credit card or debit card can access cash at ATMs any time with just a few simple steps. The first ATMs appeared in 1967 on the street in Enfield, London at a branch of Barclays Bank, and now they have grown in number to over 2 million worldwide.

When the banking sector introduced ATMs the usage of credit and debit cards has increased throughout the world. Banks had reduced their infrastructure costs by introducing Automatic Teller Machine (ATM) and Internet websites by which the customer's transactions will be carried out effortlessly and in an easy way.

ATM is a digital machine mainly used for gaining access to various banking services anywhere without the assist of any financial institution staff. The users mostly prefer ATMs for all physical transaction purposes, like money withdrawal and money deposit without going to the bank. In ATMs, the user experience has become a very important aspect to be provided by the banks. But this can additionally cause growth in robbery and assaults in ATM and online banking by numerous fraudulent methods. However, the technological improvement within the banking area gives more suitable protection to keep away from fraudulent activities.

Traditional ATMs only offer security through a pin and card, which is prone to various attacks like card skimming, card cloning, card shimming, Eavesdropping, etc. ATM skimming is a way of doing payment card fraud in which the fraudsters try to steal PINs and other important information by rigging machine with hidden recording device.

Card shimming is an attack in which a very small device with a microprocessor and flash memory inside is inserted into the card reader or ATM to capture user data. The data leaked via this method is then sold on the Internet or used in cloning the magnetic strip cards.

In an Eavesdropping attack, a small hole is being made in the ATM device or access gained to the top box of the ATM device through which electronic links are then attached directly to the card reader which helps them to capture card and PIN details.

These problems gave rise to biometric-based ATMs. Biometrics are unique for every user, further making the ATMs more impenetrable. In this paper, we will be discussing some biometric-based ATMs implemented using fingerprint scans, iris scans, facial recognition and how they improved the security of ATMs and some of their shortcomings.

II. LITERATURE REVIEW

[1] Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar (2018). In this paper, the authors had proposed the concept of Fingershield ATM, a biometric identification in the form of the fingerprint is implemented along with ATM which is integrated with smart card and database server. Despite the fact that user has to go through additional authentication time for fingerprint verification, the security was much improved and guaranteed by their system. Firstly, a smartcard is inserted into the reader, the program will ask for PIN from the user through the keypad. On successful PIN authentication, the program will then prompt fingerprint input. After successful fingerprint authentication, the user will proceed further or authentication will fail.

[2] Indranil Banerjee, Sjivangam Mookherjee, Sayantan Saha, Souradeep Ganguli, Subham Kundu, Debduhita Chakravarti (2019). In this paper, the authors had proposed a double layer security check. Firstly, the user inserts the RFID card after that user gives a fingerprint which is verified if there is a mismatch a message is sent to the user. If it's a match, the system further goes on with the level-2 security check i.e., the IRIS scanner. IRIS is the only part of our body that doesn't change from birth till our death. Iris scan is one of the most secured biometric systems it further increases the level of security along with the fingerprint and RFID card that acts as the secondary security check.

[3] Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu (2020). This paper represents the security of ATMs using facial recognition. The authors had used an RFID reader instead of an ATM card reader to identify the account details of the user. CCTV is used to recognize the face

using haar cascade and local binary pattern and if the face will match to the database, then after entering the pin, the transaction will proceed otherwise the system will send the link to the account holder it will show the snap of the person who is currently using his card and also enables three options for the user to choose one option – 'it's me', 'accept', 'decline'. If the user clicks on it's me then it will allow updating the image of an account holder and if an account holder clicks on accept then the system will allow the transaction and if the user clicks on the decline, it will terminate the transaction.

[4] Darwin Nesakumar A, T Suresh, Nivedha T, K Nivedha, Priyadharshini G, P Mugilan (2020). In this paper, the author had proposed a system using facial recognition and fingerprint. After inserting an ATM card and entering a pin, the card reader collects the details stored in the card and after capturing the face and fingerprint system will compare with the database, if all the information is matched then it will allow for transaction otherwise it will send a one-time password along with the suspect's image to the account holder's mail and after entering the correct OTP system will allow the transaction.

[5] Shivani Shukla, Anjali Helonde, Sonam Raut, Shubhkirti Salode, Jitesh Zade (2018). In this paper, the author had proposed a security text-based word and graphical password for the transaction system which uses facial recognition for detection of the face in the second stage. As soon as the user has entered the system, the user will land on the Random keypad page. If the user is not registered then the user can click on the registration link which will on the same page. After clicking on the registration link, the registration form will be opened which includes fields like user name, account number, date of birth, address, contact number, and gender. Once the form is submitted, the user will be registered with the system. If the user is already registered then the user can enter the pin using a random keypad where the numbers would be a random sequence. After entering the PIN, it will proceed for facial recognition. If the match is found then the user can perform their operations like balance inquiry, pin change, withdrawal. This system overcomes the shoulder surfing attack.

[6] Prakash Chandra Mondal, Rupam Deb, and Md. Nasim Adnan (2017). The author proposed a system that uses behavioral biometrics for authentication with more security. In this system, authentication is performed using three steps which include online handwriting signature verification, chip-based card, and PIN verification. This method does not involve the need for further enhancement like using physical biometrics (fingerprint, face images, etc).

[7] Rasib Khan, Ragib Hasan, and Jinfeng Xu (2015). In this paper, the authors had proposed the system in which Secure PIN Authentication as a service (SEPIA) is used for authentication of the PIN for ATMs which uses cloud-connected personal mobile and wearable devices. The process gets started when the user interacts with the screen and this initiates a request message to the ATM server. As a response, a QR code is generated on the screen and this QR code can be scanned using wearable devices like Google glass from which the user's details can be retrieved and verified. After the verification, the user needs to enter the PIN received via phone number. After the authentication, the user can perform the transaction.

[8] Sweedle Machado, Prajyoti D'silva, Snehal D'mello, Supriya Solaskar and Priya Chaudhary (2018). In this paper, the author had proposed a system that uses a fuzzy vault system for the security of ATM pins and passwords using a user's fingerprint data. It involves encryption and decryption. In the encryption process, the minutiae points get extracted from the fingerprint which is encoded using a pin password. While obtaining the user's account the data encoded is deciphered using the same fingerprint

impression to retrieve the pins and the passwords. The main benefit of this system is securing ATM passwords and pin with fingerprint data.

[9] Adrian Fernandes (2020). In this paper, the authors had proposed biometric protection to overcome the PIN Number problem. A fingerprint scanner is used for authenticating the users where the user's fingerprint will authenticate it and further proceed for bank transactions. The user will enter an ATM card into the machine then the machine will ask for a fingerprint to verify the user. Here Fingerprint verification is done by the data stored in the Aadhar server. Therefore, fingerprint data is retrieved through the Aadhar server based on the Aadhar card in which the user's bank account. After the biometric check user will proceed with the transaction process. If the user makes three consecutive attempts with an error the user account will be blocked.

[10] Dimaunahan, Ericson D.; Ballado, Alejandro H.; Cruz, Febus Reidj G, Dela Cruz, Jennifer (2017). In this paper, the author proposed voice identification along with fingerprint authentication as a solution to existing automated teller machine security for visually impaired users. By using fingerprint authentication and voice recognition to perform ATM transactions, adds two tiers of security, and also provided ease of use of the system for people with visual impairments. They have used vector quantized mel frequency cepstrum coefficients and discrete wavelete transform extraction of the voice parameters for speech recognition to identify the user. To identify the unknown voice, the system checks out the extracted features of the unknown speech and then compares them to the stored extracted features. The process of feature extraction is done by using the mel frequency cepstrum coefficients and discrete wavelet transform and the feature matching is being modelled using the vector quantization.

[11] R.D.Salagar, Akshata Patil (2014). In this paper, iris recognition is discussed by using MATLAB software. Here, firstly input of eye images is uploaded from the database, and further region of interest segmentation and localization of iris using canny edge detection is performed successfully. Here, the use of canny edge detection provides good localization and detection, and further normalization of the iris is performed using the Gabor filter and feature vectors are extracted using Local Binary Pattern (LBP) and classification is performed using Learning Vector Quantization (LVQ). Here, matching is performed using hamming distance which is specifically done by comparing the user iris with the iris database images which will be added at the time of account opening in the bank. Afterward, once the authenticity of the user iris is successfully verified, the user is allowed to carry out further transactions using voice-based commands by speaking into a microphone where the microphone capture sound waves and further generates electrical impulses and then the sound card converts the voice signal into a digital signal. Hence, this proposed system not only ensures security but also gives easy accessibility to people with visual impairments.

III.CONCLUSION

In these times, every individual uses an ATM machine for withdrawal and transferring cash. In the past few decades, the fraudulent activities related to ATMs had increased gradually. The existing ATM systems racked up so many hackers and fraud towards fraudulent activities such as shoulder surfing, card skimming, etc. This paper studied the existing problem and the loopholes which came into existence because of the insecure ATM systems. In order to get rid of this biometric-based ATMs were introduced. Biometric-based ATMs have enhanced the security of ATMs. Further, they have added multiple authentication steps along with biometrics to make the system impregnable.

IV. REFERENCES

[1]. Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar (2018). “Fingershield ATM – ATM Security System using Fingerprint Authentication”, International Symposium on Electronics and Smart Devices (ISESD) 2018.

[2]. Indranil Banerjee, Sjivangam Mookherjee, Sayantan Saha,Souradeep Ganguli,Subham Kundu,Debduhita Chakravarti (2019). “Advanced ATM System Using Iris Scanner”, International Conference on Opto-Electronics and Applied Optics (Optronix) 2019.

[3]. Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu I (2020). “Securing ATM Transactions using Face Recognition”, International Journal of Advanced Trends in Computer Science and Engineering, March-April 2020.

[4]. Darwin Nesakumar A, T Suresh, Nivedha T, K Nivedha, Priyadharshini G, P Mugilan (2020). “Smart ATM Security Using Face Recognition”, European Journal of Molecular & Clinical Medicine, April 2020.

[5]. Shivani Shukla, Anjali Helonde, Sonam Raut, Shubhkirti Salode, Jitesh Zade (2018). “Random Keypad and Face Recognition Authentication Mechanism”, International Research Journal of Engineering and Technology (IRJET), March 2018.

[6]. Prakash Chandra Mondal, Rupam Deb, and Md. Nasim Adnan (2017). “On Reinforcing Automatic Teller Machine (ATM) Transaction Authentication Security Process by Imposing Behavioral Biometrics”, 4th International Conference on Advances in Electrical Engineering (ICAEE), 2017.

[7]. Rasib Khan, Ragib Hasan, and Jinfeng Xu (2015). “SEPIA- Secure PIN Authentication as a service for ATM using Mobile and wearable devices”,3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering ,2015.

[8]. Sweedle Machado, Prajyoti D’silva, Snehal D’mello, Supriya Solaskar and Priya Chaudhary (2018). “Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System”, IEEE 2018.

[9]. Adrian Fernandes (2020). “Biometric ATM”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) 2020.

[10]. Dimaunahan, Ericson D, Ballado, Alejandro H, Cruz, Febus Reidj G, Dela Cruz, Jennifer C. (2017). “MFCC and VQ Voice Recognition Based ATM Security for the Visually Disabled”, IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM),2017.

[11]. R.D.Salagar, Akshata Patil (2014). “Voice Enabled ATM Machine With Iris Recognition For Authentication”, 3rd IRF International Conference 10th May-2014.

Cite this article as :

Anukul Muley, Akash Bendre, Priti Maheshwari, Shanmukh Kumbhar, Prof. Bhagyashree Dhakulkar, "Survey On Biometric Based ATMs", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 6, pp. 292-297, November-December 2021. Available at doi : https://doi.org/10.32628/IJSRST218632
Journal URL : https://ijsrst.com/IJSRST218632