



A Survey on ATM Security Using OTP and Voice Recognition

Jayanthi M, Jannet Emimal M

Abstract: An Automated Teller Machine (ATM) is a cash dispensing terminal that allows patrons to conduct financial operations without requiring human assistance, including flows, forfeitures, deposits to be made, and balance inquiries. The security of ATM remains a significant concern, with card skimming, phishing, and unauthorized access being prevalent threats [1]. A wide range of technologies, such as PIN, OTP, biometric, RFID, etc., are used to secure ATM machines. This study presents a survey of various ATM security mechanisms, these technologies have several downsides. The combination of OTP and voice recognition technology appears to be superior and more secure than other technologies when compared to other technologies used for ATM security [2]. The integration of these two authentication methods provides a robust defense against various types of attacks, including card cloning, identity theft, and shoulder surfing. The system's usability and user acceptance are also evaluated, showing a positive response from participants. This research contributes to the development of secure and reliable ATM systems, protecting users' financial information and preventing fraudulent activities

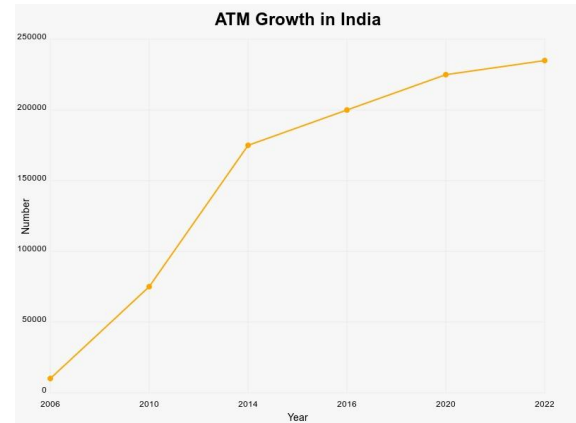
Keywords: ATM Security, Voice Recognition, One-Time Password (OTP), Multimodal Authentication.

Abbreviations:

ATM: Automated Teller Machine
OTP: One-Time Password
PIN: Personal Identification Number
CVV: Card Verification Value
USB: Universal Serial Bus
IoT: Internet of Things

I. INTRODUCTION

The financial services sector is one of the most significant aspects of a person's daily existence. As banking facilities expanded more quickly, people used it to support their economic endeavors [6]. An automated teller machine, or ATM, is one of the facilities that the bank offers its clients [7]. The ATM Introduced in the year of 1960s. With over 3.5 million ATMs worldwide, these machines have become an essential part of modern banking, offering convenience, speed, and security [8]. In Fig.1 demonstrates the expansion of ATMs in India, where a steady rise is shown between 2005 and 2022 [4].



[Fig.1: ATM Growth in India [8]]

Since crimes committed at ATMs are becoming a major problem, ATM security is becoming an essential concern that needs to be solved. A hacker can quickly take out all of the money once the customer's card has been stolen and their PIN is known [9]. The attackers are more skilled at employing various applications and techniques to breach the ATM system [5]. Therefore, there are several ways to offer security for money withdrawals in order to prevent ATM-related frauds [10]. This study also demonstrates the various approaches that different scholars have taken to address these issues, such as biometrics, PIN generation, and OTP. Despite the fact, OTP with voice recognition is more accurate and user-friendly than the others [11].

II. ATTACKS ON ATM

A. Card Skimming

It is a financial crime occurs when criminals connect equipment to ATMs or card readers in order to obtain private data, such as PINs, CVVs, expiration dates, and card numbers [12]. Skimmers can be external, internal, or overlay, and hidden cameras, glue or tape remnants, and sloppy or uneven card readers are all indicators of manipulation [13]. They instantly deduct the cash from our account after acquiring the details.

B. ATM Jackpotting

It is a sophisticated cybercrime where hackers gain unauthorized access to an ATM's internal computer, allowing them to dispense large amounts of cash without using a card or PIN. Usually targeting free standing ATMs in remote locations, thieves take advantage of flaws in ATM software or utilize malware to take over the device [14]. The hacker can empty the ATM's vault by issuing commands to dispense cash once they have gained access [15]. This type of attack, sometimes referred to as "logical attacks," can cause banks and other financial

Manuscript received on 21 November 2024 | First Revised Manuscript received on 18 February 2025 | Second Revised Manuscript received on 18 March 2025 | Manuscript Accepted on 15 April 2025 | Manuscript published on 30 April 2025.

*Correspondence Author(s)

Jayanthi M*, Assistant Professor, Department of Computer Science and Engineering, KIT-Kalaigarkarananidhi Institute of Technology, Coimbatore (Tamil Nadu), India. Email ID: jayanthikit2020@gmail.com

Jannet Emimal M, Student, Department of Computer Science and Engineering, KIT-Kalaigarkarananidhi Institute of Technology, Coimbatore (Tamil Nadu), India. Email ID: jannetjemima@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

organizations to suffer large losses; in certain cases, the damages can reach \$50,000 or more per occurrence [16].

C. Malware Attack

When malicious software is put in ATMs, it can lead to malware infection, which gives hackers access to sensitive data [17]. Usually, thieves take advantage of system flaws or inserts infected USB drives, CDs, or DVDs into the ATM's internal computer [18]. The malware can alter transaction amounts and dispense cash, disable security cameras and alarms, send stolen data to distant sites, and capture card numbers, expiration dates, and PINs once it has been infected [19].

III. LITERATURE SURVEY

A. Udhayakumar N, Sri Vasu R, Subhash S, Sharmila Rani D, "ATM-Security using Machine Learning Technique in IoT"

In the current endeavor, the taker will only be permitted once if their face has been recognized by the ATM's CCTV camera. The OTP is remit to the enrolled mobile phone, which the user must enter if the authorized user is unable to operate the ATM. Here the main drawback is the authorized person's face can't be recognized if the light setting is bad or he/ she wears an glasses or he may have beard in such cases it fails to recognize the person's face. New modules can be introduced in the future

B. Jathumithran S, Thamilarasan V, piratheepan P, Rushanthini P, Mercy veniancy J, Nirupa P, Thiruthanigesan K, "Enhancing ATM Security using Fingerprint"

This research is based on implementing the Fingerprint mechanism in the ATM system [3]. Here the user need to be registered his/her Fingerprint during the account open. At first it verifies with the Fingerprint of the user if it matches it asks for the PIN of the account after the verification the user can withdraw the amount. The drawback here is the only authorized person has the access and Fingerprint may change in few years, in some case the Fingerprint may mismatch.

C. Abdul Rahman Alhothaily, Arwa Alrawais, Xiuzhen Cheng, Rongfang Bie, "A Novel Verification Method for Payment Card Systems"

Payment systems must be secure, yet some payment card security implementations rely on lousy cardholder verification techniques, including using the card, or utilize the card without any cardholder verification procedures at all. They present a brand-new cardholder verification technique that offers a high degree of security for payment card systems in order to solve this issue. This approach guards against a wide range of security threats by combining a distance bounding mechanism with multi-possession factor authentication [20]. Thus, this methodology relies on one or more personal RFID devices, such smart watches, smart phones etc, and allows the user to choose the appropriate security level and add one or more additional devices.

D. Nongmeikapam Thoiba Singh, Richa Dhiman, Amrita Chaudhary, Prerna Dhawan, Asem Debala Chanu, "Enhancing ATM Security and Convenience with Fingerprint-Based Biometric Authentication"

To increase the security and usability of the system, finger print recognition technology is employed for both identification and verification [21]. This research offers a succinct examination of the intellectual underpinnings and organizational design of fingerprint recognition [22]. the implementation of biometric authentication in ATM systems, has the potential to revolutionize banking services, offering users a more secure and convenient way to access their funds [23]. Further investigation in this area can forefront to even more robust and sophisticated biometric authentication systems, ensuring the safety of users' financial transactions [24].

IV. CONCLUSION

The ATM security foster effectively shown how incorporating forward-thinking security methods to defend against a variety of attacks may be beneficial. This project greatly improved ATM transaction security by using a multipronged strategy that combined voice recognition with an OTP and real-time transaction monitoring. The integrated security system increased the confidence and trust that users had in their ATM transactions. These results are transferable to other financial institutions and sectors.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCE

1. Udhayakumar N, Sri Vasu R, Subhash S, Sharmila Rani D, "ATM-Security using machine learning technique in IOT" in International Journal of Advance Research Ideas and Innovations in Technology. <https://www.ijariit.com/manuscripts/v5i2/V5I2-1225.pdf>
2. Jathumithran S, Thamilarasan V, piratheepan P, Rushanthini P, Mercy veniancy J, Nirupa P, Thiruthanigesan K, " Enhancing ATM Security using Fingerprint " in ICTACT Journal on Micro Electronics (2018, vol-04). https://ictactjournals.in/paper/IJME_Vol_4_Iss_2_Paper_4_570_575.pdf
3. Om kumar Gaurav, Sanjay Prasad rao, "Biometric System based ATM Security System" in international Journal of Scientific Engineering and

- Technology Research, Research Gate (2016). https://www.researchgate.net/profile/Banoth-Rao/publication/348162743_Biometric_Systems_based_ATM_Security_System/links/5ff165d6a6fdccdc8266c99/Biometric-Systems-based-ATM-Security-System.pdf
4. Abdulrahman Alhothaily, Arwa Alrawais, Xiuzhen Cheng, Rongfang Bie, "A novel verification method for payment card systems", In Springer Verlag London, October 2015, Volume 19, Issue 7, pp 1145-1156, October 2015. DOI: <https://doi.org/10.1007/s00779-015-0881-9>
5. Nongmeikapam Thoiba Singh, Richa Dhiman, Amrita Chaudhary, Prerna Dhawan, Asem Debalu Chanu, "Enhancing ATM Security and Convenience with Fingerprint-Based Biometric Authentication" in Research gate at 2024. DOI: <http://dx.doi.org/10.1109/GCITC60406.2023.10426103>
6. Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Muhammad Nizam Kamarudin, Chow Kok Lin and Zalina Kamis, "Biometric Voice Recognition in Security System" in Indian Journal of Science and Technology at 2014. DOI: <http://dx.doi.org/10.17485/ijst/2014/v7i1.9>
7. Dwi Ana Ratna Wati, Dika Abadianto "Design of Face Detection and Recognition System for Smart Home Security Application." IEEE (2017). DOI: <https://doi.org/10.1109/ICITISEE.2017.8285524>
8. Muhammad-Bello B.L., Alhassan M.E, Ganiyu, S.O' "An Enhanced ATM Security System using Second-Level Authentication" in International Journal of Computer Applications at 2015. DOI: <http://dx.doi.org/10.5120/19533-1181>
9. Adepoju, A.S & Alhassan, M.E. "Challenges of automated Teller Machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna metropolis", in Journal of Internet Banking and Commerce. At 2010 Vol 15, No. 2. <https://www.researchgate.net/publication/228464353>
10. Selvaraju, N. & Sekar, G. (2010), A method to improve the security level of ATM banking systems using AES algorithm, International Journal of Computer Applications. June 2010 Vol 3 No.6. <https://www.researchgate.net/publication/272862868>
11. K.Yadav, S. Mattas, L. Saini and P. Jindal, "Secure Card-less ATM Transactions," 2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA), Kurukshetra, India, 2020, pp. 1-4. DOI: <https://doi.org/10.1109/ICMICA48462.2020.9242713>
12. S. Sharma and V. Sejwar, "Impementation of QR Code Based Secure System for Information Sharing Using Matlab," 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), Tehri, India, 2016, pp. 294-297. DOI: <https://doi.org/10.1109/CICN.2016.64>
13. S. Kumaresan, G. D. Kumar and S. Radhika, "Design of secured ATM by wireless password transfer and shuffling keypad," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 2015, pp. 1-4. DOI: <https://doi.org/10.1109/ICIIECS.2015.7192993>
14. A. Mandalapu, Daffney Deepa V, L. D. Raj and Anish Dev J, "An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies," 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, BC, Canada, 2015, pp. 1-6. DOI: <https://doi.org/10.1109/IEMCON.2015.7344491>
15. A. Muley and V. Kute, "Prospective solution to bank card system using fingerprint," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018, pp. 898-902. DOI: <https://doi.org/10.1109/ICISC.2018.8398930>
16. Sonal Mahajan, Anagha Awale, Rutuja Gurav, Pranjal Satpute, Ms. Hema Karande, Mr. Jitendra Bakliwal, "Cardless transaction in ATM" IJRASET Journal For Research in Applied Science and Engineering Technology, 2023. DOI: <https://doi.org/10.22214/ijraset.2023.50741>
17. Sahil Bajaj, Sumit Dawda, Pradnya Jadhav, Rasika Shirude, "Card less ATM Using Deep Learning and Facial Recognition Features", Journal of Information Technology and Software Engineering, Vol.12 Iss.5 No:302, JITSE-21-11077, 14-Oct-2022. <https://www.longdom.org/open-access/card-less-atm-using-deep-learning-and-facial-recognition-features-87209.html>
18. Vaishnavi M. Shinde, Dhanashri B. Shinde, Pravin B. Shinde, Aditya V. Wandhekar, Pallavi S. Kohakade, "Virtual ATM through Fingerprint and Face recognition using Deep Learning", International Journal of Innovative Research in Technology (IJIRT), ISSN: 2349-6002, Volume 9 Issue 10, March 2023. <https://www.ijrd.com/Article.php?manuscript=IJSRDV10190012>
19. Ai based E-Atm security and surveillance system using blynk-lot server international conference on. Ieee, 2022. DOI: <https://doi.org/10.1109/C21456876.2022.10051613>
20. Jay Jadhav, Shrikant Chavhan, Manohar Chavan, Tushar Mohite, "Design and Implementation Of Advanced Security-Based System For Atm", International Research Journal of Modernization in Engineering Technology and Science, 2024. https://www.irjmets.com/uploadedfiles/paper/issue_4_april_2024/53535/final/fin_irjmets1716642324.pdf
21. Basha, Dr. S. M., Ramkumar, Mr. V., Reddy, Mr. S. P. V. V., Bhuvaneswari, Ms. V., & Kumar, Mr. V. P. (2020). Secured Banking using Multilevel Authentication by Face Recognition and SIM Card Verification for ATMs. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 3, pp. 2596–2599). DOI: <https://doi.org/10.35940/ijtee.b7062.019320>
22. Naqi, Mohd. A., & Pendem, S. (2019). Advanced ATM Crime Prevention System by using Wireless Communication. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 4, pp. 11839–11844). DOI: <https://doi.org/10.35940/ijrte.d9567.118419>
23. Jabili, G., Bhatt, A. S., Kosuri, T., Pisay, B., & Nadhan, A. S. (2020). Multilevel Security System for ATM Machines. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 4, pp. 651–653). DOI: <https://doi.org/10.35940/ijeat.d7437.049420>
24. Mandal, Dr. T. (2023). Adoption of UPI and Implementation of UPI-ATM in India: A Logit Analysis. In Indian Journal of Economics and Finance (Vol. 3, Issue 1, pp. 52–59). DOI: <https://doi.org/10.54105/ijef.e7990.03010523>

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.