Securing ATM Payment Transactions

Subjects: Computer Science, Artificial Intelligence

Contributor: Abdullah Alabdulatif , Rohan Samarasinghe , Navod Neranjan Thilakarathne

Credit/debit cards are a ubiquitous form of payment at present. They offer a number of advantages over cash, including convenience, security, and fraud protection. In contrast, the inherent vulnerabilities of credit/debit cards and transaction methods have led many payment institutions to focus on strengthening the security of these electronic payment methods. Also, the increasing number of electronic payment transactions around the world have led to a corresponding increase in the amount of money lost due to fraud and cybercrime. This loss of money has a significant impact on businesses and consumers, and it necessitates the development of rigid and robust security designs for securing underlying electronic transaction methods.

security data privacy authentication multi-factor authentication one-time password electronic payments transaction security

1. Introduction

Even though the technology behind electronic payment transactions is becoming more complicated day by day due to the ever-increasing nature of sophisticated cyberattacks that target these ecosystems, billions of dollars continue to be lost owing to the profitable nature of executing such attacks. According to the latest research [1][2], it is evident that electronic transaction security is becoming a common problem worldwide, causing considerable financial chaos. Hence, it becomes essential to develop security mechanisms that are reliable and trustworthy that the cardholders or end users can always trust. Unauthorized access to credit/debit card data, moreover, might lead to financial loss due to fraud by unscrupulous persons [1]. Thus, to cultivate trust in the minds of cardholders, many banks/payment institutions have introduced various security schemas for authenticating authorized end users over the last few years [3]. In addition, the booming of electronic commerce, most popularly known as e-commerce, has led to online banking, where customers can pay money online for the goods they purchase online, expanding the scope of cyberattacks that target the electronic payment ecosystem.

In light of credit/debit card transactions, the main purpose is to promote cashless transactions [1][2][3], comparing user-submitted details with the user's bank account. Often, there are a number of entities associated with and involved in this payment card authentication: the card-issuing bank, the user or the cardholder, the ATM, the bank database server, and the card affiliation or the association [3][4]. According to studies [3][4], it is evident that credit/debit card theft has evolved dramatically in recent years. In earlier times, fraudsters employed basic skimming tactics with pinhole cameras to capture the associated PIN at the ATM to harvest card credentials for

card cloning [5][6][7][8], whereas attack methodologies have developed over time employing a variety of approaches, such as social engineering attacks [3][4].

Thus, in order to prevent the compromise of electronic payments that are being made, banks/financial institutions have introduced novel ways of authenticating users when they are executing ATM transactions [7][8][9]. These include both single-factor and multi-factor authentication methods such as username and password, OTP, and PIN. However, most of these methods are no longer secure and open the cardholder to risk where user credentials can be captured through interception and person-in-the-middle attacks for gaining access to the user account, especially when dealing with payment gateway mobile apps and web platforms, as PINs can be captured with card details for cloning the card. Thus, single-factor authentication is no longer deemed sufficient for user authentication and is regarded as insecure for high-risk financial transactions. This has resulted in the usage of multi-factor authentication to safeguard payment transactions and boost user confidence in making such payment transactions, which at times appears to be insufficient due to PIN harvesting and card cloning security attacks [10][11][12][13][14].

2. Securing ATM Payment Transactions

Overall, ATMs play a crucial role in providing convenient and secure access to banking services. As the use of ATMs continues to grow, ensuring robust authentication methods becomes paramount in preventing fraudulent activities and protecting user data [15][16][17][18][19]. According to the latest literature [1][6][7][8][9][10], some common ways of compromising the security of these electronic transaction methods are described further in the following for better understanding.

- Stealing from the database
    - Many retailers prefer to keep debit/credit card numbers in online databases to facilitate customer purchases. According to recent reports, attackers have breached merchant websites and stolen databases containing millions of debit/credit card details [1][5], e.g., the compromising of Capital One, a US credit card issuer, which led to the exposure of 106 million customers' credit card information in 2019 [6], and the compromising of the TJX company chain, which led to the exposure of 94 million customers' credit card information in 2006 [6].
- Sniffing/packet intercepting
    - During online debit/credit card payments, an attacker sniffs data packets to infer confidential payment information. In most circumstances, the attacker does not need to decrypt the presumably encrypted online payment packets (e.g., through Secure Sockets Layer) [1][3][5], but instead deceives the consumer into believing they are visiting a legitimate site while in fact, they are viewing the attacker's spoofing site.
- Shoulder surfing

- An attacker stands nearby and observes a customer type in their credit/debit card number and other credentials or listens to the discussion if the consumer gives their credit/debit card information to some other party [2][6].

- Skimming
  - Fraudsters utilize this approach to collect sensitive information from a credit or debit card's magnetic strip [3][6].

- Keypad overlays
  - This is a technique that is meant to fit in with the normal ATM keypad and this allows it to go unnoticed. The overlay allows the keypad beneath it to work properly, allowing the person to operate the ATM without any difficulty; when a person punches their PIN onto the fake keypad installed over the existing ATM keypad, an overlay records and captures keystrokes (e.g., customer PIN). Simultaneously, the ATM card slot overlays/records the secret data from the ATM card's magnetic strip. Using blank cards, the fraudster combines information in their computer to clone the ATM card, and nowadays, this is becoming a significant threat [3].

Having provided a brief background to how overall electronic payment transactions are compromised by cyber criminals, the latter part of this section provides a brief review of available authentication methods for securing payment transactions.

In general, ATMs are fundamentally autonomous banking workstations that are designed to offer easy transaction services to the customers that use them [3][4][20]. The fact that the ATM can provide its users service around the clock, seven days a week, is the primary advantage it offers [21][22][23][24][25]. ATMs are used at practically every convenient location in today's society, including busy streets, public spaces, and other areas. Despite the fact that ATMs have been an important part of our lives since the 1960s [3][4][5][6], the authentication mechanisms that are used for transactions at ATMs have changed very little over the years [26][27][28][29]. The security flaws inherent to magnetic media are the primary cause of the constraints imposed on ATMs' ability to protect their customer transactions. Since it is neither difficult nor costly to acquire the necessary equipment to encode magnetic stripes, the data stored on them are often encoded using two or three tracks [11][12][13][14]. Later on, this weakness of magnetic stripe cards was somewhat remedied by the advent of smartcards that were compatible with EMV [11][12][13][14][30][31][32][33]. The PIN of the cardholder is often the sole way to testify to the identity of the user. However, this method is susceptible to a variety of risks, including loss, illegal access, forgetfulness, etc. [34][35][36][37]. On the other hand, many individuals, in spite of the many warnings that are sent to card users regarding the risk associated with usage, continue to choose passwords and PINs that are easy to guess, such as their social security number, birthday, etc. However, because of the constraints of this design, an intruder who obtains a user's card and then attempts to guess the user's PIN or predicts the user's password may do so successfully, which is known as a brute-force attack. In spite of all of the security precautions that have been put into place, there are still instances of criminal activity involving ATMs all over the world.

As the use of ATMs continues to grow, ensuring robust authentication methods becomes paramount in preventing these fraudulent activities and protecting user data. Starting from single-factor authentication, authentication technology has evolved to the level of multi-factor authentication. The most straightforward way of authentication is known as single-factor authentication, where an individual may authenticate their identity by matching only one credential (e.g., providing a password for a username/providing a PIN for an ATM). MFA, also known as Two-Factor Authentication or Two-Step Verification, is a security process that requires users to provide two or more different forms of identification or credentials to verify their identity before gaining access to a system, application, or service. The primary goal of MFA is to add an extra layer of security beyond traditional username–password combinations, making it more difficult for unauthorized individuals to access sensitive information or perform malicious activities.

The three typical factors used in MFA are:

- Knowledge factor (something you know)
    - This factor involves information that only the authorized user should know, such as a password, PIN, or a specific answer to a security question [10][11].
- Possession factor (something you have)
    - This factor involves possessing a physical device or object that uniquely belongs to the user, such as a smartphone, smart card, hardware token, or an OTP generator [10][11].
- Inherence factor (something you are)
    - This factor refers to biometric characteristics unique to each individual, such as fingerprints, facial recognition, iris patterns, voice recognition, or even behavioral biometrics (e.g., keystroke dynamics) [10][11].

To authenticate using MFA, a user needs to provide at least two of these factors. For example, after entering their username and password (something they know), the user may be prompted to enter a one-time code generated on their smartphone (something they have) or use their fingerprint on a biometric scanner (something they are) [5][10][11]. The main advantages of MFA include enhanced security by combining multiple factors and significantly reducing the risk of unauthorized access, even if one factor is compromised [5][10][11]. Other key advantages of MFA include:

- Protection against password attacks
    - MFA provides an additional layer of protection against common password-based attacks like brute-force and phishing [14][38][39].
- Compliance requirements

- Many industry regulations and security standards, such as PCI DSS and GDPR, require or strongly recommend the use of MFA to protect sensitive data [15][39][40][41][42].

- User-friendly
  - MFA can be implemented in a user-friendly manner, often through smartphones and apps, without causing significant inconvenience to users [14][38][39].

Overall, MFA is an essential security mechanism that adds an extra layer of protection to ensure the identity of users attempting to access sensitive information, systems, or services. It has become increasingly prevalent across various applications and industries as a crucial defense against cyber threats [15][40][41][42]. Further, the landscape of payment security is constantly evolving, and new methods are being introduced occasionally [16][17][18][19][20]. The following paragraphs discuss some of the commonly used authentication methods for securing ATM transactions as of now.

- EMV
  - EMV is a widely adopted global standard for chip-based payment cards. EMV cards contain embedded microchips that generate dynamic authentication codes for each transaction [3][4][8]. When the card is inserted into an EMV-enabled ATM or POS terminal, the chip communicates with the terminal to verify the card's authenticity and the cardholder's identity. This method makes it difficult for fraudsters to clone or counterfeit cards [21][22][23][24].

- PIN
  - For ATM transactions, PIN-based authentication is widely used. The cardholder must enter their unique PIN to complete the transaction, ensuring that only the authorized user can access the funds [5][6][7].

- Biometric authentication
  - Some modern ATMs and POS systems are equipped with biometric authentication methods, such as fingerprint scanners or facial recognition. Biometric data provides a highly secure way to verify the cardholder's identity [16][17][18][25][26][27]. However, the major drawback of biometric approaches is that they require large systems with very high power and processing capability with high implementation and deployment costs.

- OTP
  - The use of OTPs as a second layer of authentication has been extensively studied. OTPs sent via SMS, email, or generated through authenticator apps add an extra security layer, protecting against unauthorized access even if the primary authentication credentials (e.g., PIN) are compromised [3][4][5]. However, concerns have been raised regarding the reliance on mobile networks and email security.

- Voice recognition
    - Voice recognition technology has also been investigated for ATM authentication. Early studies indicate that voice-based systems can be vulnerable to voice-mimicking attacks, which raises concerns about their reliability as a standalone authentication method. However, when used in conjunction with other factors, such as location-based authentication, voice recognition can be a valuable component of a multi-layered security approach [9][16][17][18][19][28][29][30].

References

1. Pranith, C.V.; Sujith, V.L.; Kiran, K.S.; Goutham, P.; Kiran, K.V.D. A Multifactor Security Protocol for Wireless Payment-Secure Web Authentication Using Mobile Devices. In Cybernetics, Cognition and Machine Learning Applications; Gunjan, V.K., Suganthan, P.N., Haase, J., Kumar, A., Eds.; Springer Nature: Singapore, 2023; pp. 29–38.
2. Bissada, A.; Olmsted, A. Mobile multi-factor authentication. In Proceedings of the 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 210–211.
3. Sankhwar, S.; Pandey, D. A Safeguard against ATM Fraud. In Proceedings of the 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, 27–28 February 2016; pp. 701–705.
4. Gold, S. The evolution of payment card fraud. Comput. Fraud. Secur. 2014, 2014, 12–17.
5. Yang, S.; Meng, J. Research on Multi-factor Bidirectional Dynamic Identification Based on SMS. In Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 October 2018; pp. 1578–1582.
6. Li, Y.; Zhang, X. A security-enhanced one-time payment scheme for credit card. In Proceedings of the 14th International Workshop Research Issues on Data Engineering: Web Services for e-Commerce and e-Government Applications, 2004. Proceedings, Boston, MA, USA, 28–29 March 2004; pp. 40–47.
7. Kish, L.B.; Entesari, K.; Granqvist, C.-G.; Kwan, C. Unconditionally Secure Credit/Debit Card Chip Scheme and Physical Unclonable Function. Fluct. Noise Lett. 2017, 16, 1750002.
8. Jerry Gao, J.C. A Wireless Payment System. In Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05), Xi'an, China, 16–18 December 2005; pp. 367–374.

9. Greene, C.; Stavins, J. Did the Target Data Breach Change Consumer Assessments of Payment Card Security? Social Science Researh Network: Rochester, NY, USA, 2016; Available online: https://papers.ssrn.com/abstract=2818262 (accessed on 5 July 2023).
10. ATM/PoS Malware ‘Recovers’ from COVID-19, with the Number of Attacks Continuing to Grow in 2022|Kaspersky. Available online: https://www.kaspersky.com/about/press-releases/2022_atmpos-malware-recovers-from-covid-19-with-the-number-of-attacks-continuing-to-grow-in-2022 (accessed on 24 July 2023).
11. Nambiar, S.; Lu, C.-T.; Liang, L.R. Analysis of payment transaction security in mobile commerce. In Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, IRI 2004., Las Vegas, NV, USA, 8–10 November 2004; pp. 475–480.
12. Asokan, N.; Janson, P.A.; Steiner, M.; Waidner, M. The state of the art in electronic payment systems. Computer 1997, 30, 28–35.
13. Téllez Isaac, J.; Sherali, Z. Secure Mobile Payment Systems. IT Prof. 2014, 16, 36–43.
14. Herzberg, A. Payments and banking with mobile personal devices. Commun. ACM 2003, 46, 53–58.
15. Bhutta, M.N.M.; Bhattia, S.; Ali Alojail, M.; Nisar, K.; Cao, Y.; Chaudhry, S.A.; Sun, Z. Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). Wirel. Commun. Mob. Comput. 2022, 2022, 9942270.
16. Geolocation Drives Future of Payments; GeoComply: Vancouver, BC, Canada, 2020. Available online: https://www.geocomply.com/blog/geolocation-drives-future-of-payments/ (accessed on 6 July 2023).
17. Schuman, E. Geolocation: Great for Authentication, but Far from Perfect. 2016. Available online: https://blog.sift.com/geolocation-nice-tool-authentication-far-perfect/ (accessed on 6 July 2023).
18. Ashfield, J.; Shroyer, D.; Brown, D. Location Based Authentication of Mobile Device Transactions. U.S. Patent US8295898B2, 23 October 2012. Available online: https://patents.google.com/patent/US8295898B2/en (accessed on 6 July 2023).
19. Securing FinTech Apps With GPS Data. Velmie. 2020. Available online: https://www.velmie.com/post/securing-fintech-apps-with-gps-data (accessed on 6 July 2023).
20. Twum, F.; Nti, K.; Asante, M. Improving Security Levels in Automatic Teller Machines (ATM) Using Multifactor Authentication. IJSEA 2016, 5, 126–134.
21. Hassan, M.A.; Shukur, Z. Device Identity-Based User Authentication on Electronic Payment System for Secure E-Wallet Apps. Electronics 2021, 11, 4.
22. Sanyal, S.; Tiwari, A.; Sanyal, S. A Multifactor Secure Authentication System for Wireless Payment. In Emergent Web Intelligence: Advanced Information Retrieval; Chbeir, R., Badr, Y.,

Abraham, A., Hassanien, A.-E., Eds.; Springer: London, UK, 2010; pp. 341–369.

23. Hassan, M.A.; Shukur, Z.; Hasan, M.K.; Al-Khaleefa, A.S. A Review on Electronic Payments Security. Symmetry 2020, 12, 1344.
24. Sahi, A.M.; Khalid, H.; Abbas, A.F.; Zedan, K.; Khatib, S.F.A.; Al Amosh, H. The Research Trend of Security and Privacy in Digital Payment. Informatics 2022, 9, 32.
25. Hassan, M.A.; Shukur, Z.; Hasan, M.K. An Efficient Secure Electronic Payment System for E-Commerce. Computers 2020, 9, 66.
26. Liu, Y.; Huang, W.; Zhuo, M.; Zhou, S.; Li, M. Mobile Payment Protocol with Deniably Authenticated Property. Sensors 2023, 23, 3927.
27. Jiang, Y.; Sun, G.; Feng, T. Research on Data Transaction Security Based on Blockchain. Information 2022, 13, 532.
28. Hwang, Y.; Park, S.; Shin, N. Sustainable Development of a Mobile Payment Security Environment Using Fintech Solutions. Sustainability 2021, 13, 8375.
29. De Luca, A.; Langheinrich, M.; Hussmann, H. Towards understanding ATM security: A field study of real world ATM use. In Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA, 14–16 July 2010; pp. 1–10.
30. Singh, A.; Singh, K.; Khan, M.H.; Chandra, M. A Review: Secure Payment System for Electronic Transaction. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2012, 2, 237–243.
31. An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems—ScienceDirect. Available online: https://www.sciencedirect.com/science/article/pii/S1567422309000283 (accessed on 6 August 2023).
32. Ceipidor, U.B.; Medaglia, C.M.; Marino, A.; Sposato, S.; Moroni, A. KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions. In Proceedings of the 2012 9th International ISC Conference on Information Security and Cryptology, Tabriz, Iran, 13–14 September 2012; pp. 115–120.
33. Kovács, L.; David, S. Fraud risk in electronic payment transactions. J. Money Laund. Control 2016, 19, 148–157.
34. Chaum, D. Security without identification: Transaction systems to make big brother obsolete. Commun. ACM 1985, 28, 1030–1044.
35. Tsiakis, T.; Sthephanides, G. The concept of security and trust in electronic payments. Comput. Secur. 2005, 24, 10–15.

36. Bellare, M.; Garay, J.A.; Hauser, M.; Herzberg, A.; Krawczyk, H.; Steiner, M.; Tsudik, G.; Van Herreweghen, E.; Waidner, M. Design, implementation, and deployment of the iKP secure electronic payment system. IEEE J. Sel. Areas Commun. 2000, 18, 611–627.
37. Ali, G.; Dida, M.A.; Elikana Sam, A. A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications. Future Internet 2021, 13, 12.
38. Chabbi, S.; Araar, C. RFID and NFC authentication protocol for securing a payment transaction. In Proceedings of the 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS), Oum El Bouaghi, Algeria, 12–13 October 2022; pp. 1–8.
39. Yeh, K.-H. A Secure Transaction Scheme with Certificateless Cryptographic Primitives for IoT-Based Mobile Payments. IEEE Syst. J. 2018, 12, 2027–2038.
40. Yeh, K.-H.; Su, C.; Hou, J.-L.; Chiu, W.; Chen, C.-W. A Robust Mobile Payment Scheme With Smart Contract-Based Transaction Repository. IEEE Access 2018, 6, 59394–59404.
41. Sharma, A.; Kansal, V.; Tomar, R.P.S. Location Based Services in M-Commerce: Customer Trust and Transaction Security Issues. Int. J. Comput. Sci. Secur. 2015, 9, 11–21.
42. Konidala, D.M.; Yeun, C.Y.; Kim, K. Enhanced protocol for location-based services in ubiquitous society. In Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM ’04, Dallas, TX, USA, 29 November–3 December 2004; pp. 2164–2168.