Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April -2025 | Page 37-41

Secure ATM Using Card Scanning Plus OTP

[1]Shreya Chakraborty, [2]Ms Manjulata Bhoi
[1]Bachelor of Computer, [2]Assistant Professor

[1,2]CS & IT Department, Kalinga University, Raipur, India
[1]shreya211chakraborty@gmail.com

Abstract:
Automated Teller Machines (ATMs) are essential components of modern banking infrastructure, providing users with convenient access to financial services. However, increasing incidents of ATM fraud, including card skimming and unauthorized access, have necessitated more robust security mechanisms. This study proposes a secure ATM authentication model integrating card scanning with One-Time Password (OTP) verification. The dual-layered approach enhances user authentication by combining physical card presence with dynamic OTPs sent to the registered mobile device, thereby mitigating risks associated with stolen or cloned cards. The system ensures improved user privacy, real-time fraud prevention, and strengthened banking security without compromising accessibility. This model can be effectively deployed in both urban and rural banking setups to safeguard user transactions and restore trust in ATM services.

Keywords: Secure ATM, Card Scanning, OTP Authentication, Banking Security, Fraud Prevention

Introduction

The increasing cases of ATM fraud and unauthorized transactions highlight the need for a more secure authentication system. Traditional ATM authentication relies on a PIN, which can be easily compromised. To address this issue, we propose a two-factor authentication system that combines card scanning with an OTP sent to the user's registered mobile number. This method ensures a more secure transaction process and mitigates potential fraud. This paper further explores the feasibility, benefits, and technical architecture of this system.

Literature Review

Various security mechanisms have been explored in ATM systems, including biometric authentication, chip-based cards, and multi-factor authentication. While biometric authentication provides high security, it requires additional hardware and can lead to privacy concerns. Chip-based cards enhance security but remain susceptible to cloning. OTP-based authentication has been widely used in online banking, proving its effectiveness in preventing unauthorized access. Recent studies highlight the increasing need for multi-layered authentication in financial transactions to prevent cybercrimes and unauthorized access.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April -2025 | Page 37-41

Proposed System

The proposed system enhances ATM security by integrating two authentication factors:

- Card Scanning: The user inserts their ATM card into the machine, which reads the card details.
- OTP Authentication: An OTP is sent to the registered mobile number of the user. The user must enter the correct OTP to proceed with the transaction

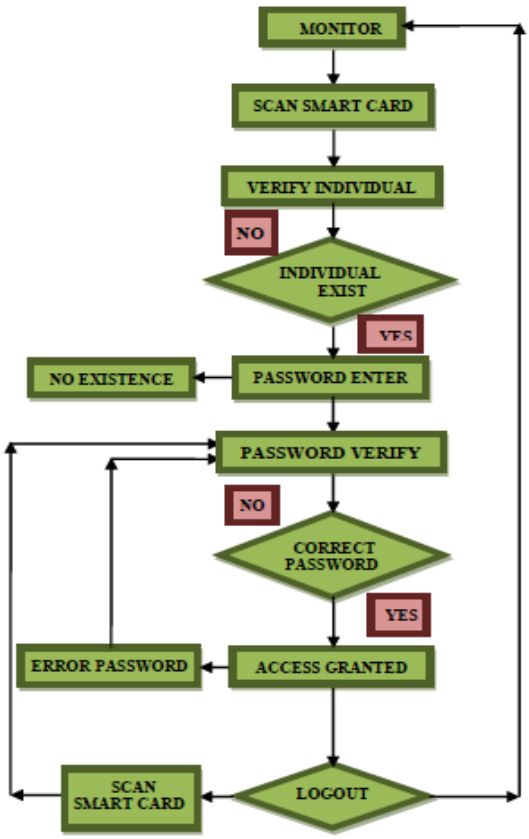


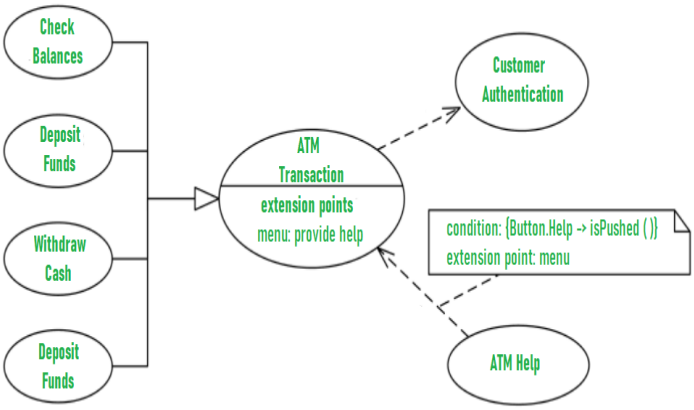
Fig.1 OTP Authentication

System Architecture

The system comprises the following components:

- ✔ ATM Machine: Equipped with a card reader and an OTP verification interface.
- ✔ Bank Server: Responsible for generating and sending OTPs to the user's registered mobile number.
- ✔ User Interface: Allows the user to enter the OTP for authentication.
- ✔ Encryption Module: Ensures secure transmission of card and OTP data to prevent interception.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April -2025 | Page 37-41



Working Mechanism

1. The user inserts their ATM card into the machine.
2. The ATM reads the card details and communicates with the bank server.
3. The bank server generates an OTP and sends it to the registered mobile number.
4. The user enters the OTP into the ATM interface.
5. If the OTP matches, the transaction proceeds; otherwise, it is declined.
6. The transaction details are securely logged for auditing purposes.

Security Analysis

The proposed system enhances security by addressing common threats:

- **Protection against Skimming:** Since an OTP is required, even a cloned card cannot be used without access to the registered mobile number.
- **Prevention of Shoulder Surfing:** Unlike PINs, OTPs are dynamic and change with every transaction, making them resistant to observation-based attacks.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April -2025 | Page 37-41

- **Mitigation of Brute-Force Attacks:** The OTP has a limited validity period and a restricted number of attempts, reducing the chances of brute-force attacks.
- **Data Encryption:** All communication between the ATM and bank server is encrypted, preventing interception by attackers

Implementation Challenges

While the proposed system provides enhanced security, certain challenges need to be addressed:

- **Network Dependency:** The system relies on mobile networks for OTP delivery, which may cause delays in areas with poor network coverage.
- **User Inconvenience:** Users who do not have access to a mobile phone or face difficulties receiving OTPs may experience transaction delays.
- **System Integration:** Banks need to update existing ATM software and infrastructure to support OTP authentication, which may require additional investment.
- **Phishing and SIM Swap Attacks:** Attackers may attempt to gain control over the user's mobile number to intercept OTPs. Advanced authentication measures should be implemented to prevent such risks.

Advantages and Limitations Advantages:

- Enhances security by adding a second authentication layer.
- Prevents unauthorized transactions even if the card is lost or cloned.
- Reduces the risk of PIN-based attacks.
- Uses a time-sensitive OTP, limiting the window for fraudulent activities.
- Improves user confidence in ATM security.

Limitations:

- Requires a mobile network connection for OTP delivery.
- Potential delays in OTP reception due to network issues.
- Users without mobile phones may face difficulties accessing the ATM.
- Additional costs for banks in implementing and maintaining OTP systems.

Key Elements Illustrated:

Biometric Authentication: The user interacts with the ATM through biometric authentication, replacing traditional PINs with more secure and convenient methods. Fingerprint scanning, facial recognition, or even voice recognition are all possible methods for this.

Blockchain Integration: The blockchain symbol signifies the underlying technology ensuring secure and transparent transactions. Blockchain can enhance security, reduce fraud, and improve the efficiency of financial operations.

Fraud Detection Powered by AI: A real-time analysis of transaction patterns by an AI algorithm

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April -2025 | Page 37-41

flags suspicious activity. This proactive approach helps prevent fraudulent transactions and protects user funds.

User-Friendly Interface: The holographic display represents a modern and intuitive user interface, making ATM interactions more seamless and enjoyable.

Additional Visual Cues:

Data Flow: Subtle visual cues like lines or arrows could show how data moves between the bank's systems, the blockchain network, and the ATM.

Security Layers: Visual metaphors, such as a shield or a lock, could represent the enhanced security measures provided by biometric authentication and blockchain technology.

Conclusion

The integration of OTP-based authentication with card scanning significantly improves ATM security. This method ensures that even if an ATM card is stolen or cloned, unauthorized transactions cannot occur without the OTP. Despite implementation challenges, the benefits of improved security outweigh the limitations. Future advancements in biometric authentication, blockchain technology, and AI-driven security can further enhance ATM security, making financial transactions safer and more reliable.

References

1. Alzubaidi, M., & Kalita, J. (2016). Authentication of users using behavioral biometrics.
2. Kaur, H., & Chhabra, A. (2019). Enhancing ATM security using multi-factor authentication.
3. Singh, S. (2020). Analyzing the effectiveness of OTP-based security in banking systems.
4. Verma, R., & Sharma, P. (2021). Trends and Challenges in Banking Cybersecurity Smith, J. (2022). Secure banking transactions made possible by AI and blockchain in the future.