AUTOMATED TELLER MACHINE

Submitted in the partial fulfillment for the award of the

degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE WITH SPECIALIZATION IN DEVOPS

Submitted by:
Adarsh Kumar Singh – 22BDO10053
Ayush Pandey – 22BDO10038
Krishna Sharma – 22BDO10029
Akansh Arya – 22BDO10027

Under the Supervision of:
Mr. Tejinderpal Singh (E16552)

Department of AIT-CSE

Outline

- Introduction to Project
- Problem Formulation
- Objectives of the work
- Methodology used
- Results and Outputs
- Conclusion
- References

Introduction:

An ATM (Automated Teller Machine) is an electronic machine used for financial transactions. As the term implies, it is an ‘automated’ banking platform that does not require any banking representative/teller or a human cashier.

Types of Automated Teller Machines

Automated Teller Machines (ATMs) are mainly of two types –

- **On-Site ATMs:** These ATMs are typically located within bank branches or at other fixed locations such as shopping malls, airports, or universities. They provide basic banking services to customers of the associated bank and may offer additional functionalities like cash withdrawals, deposits, and balance inquiries.

- **White Label ATMs:** White label ATMs are owned and operated by non-bank entities such as independent ATM deployers (IADs) or retail businesses. They are not affiliated with any specific bank and may offer services from multiple banks through interoperable networks like National Financial Switch (NFS) in India.

Fig: On-Site ATMs

Fig: White label ATMs

Continue…

- **Mobile ATMs:** Mobile ATMs are vehicles equipped with ATM machines that travel to different locations to provide banking services. They are often used in rural or remote areas where access to traditional banking infrastructure is limited. Mobile ATMs may be operated by banks, government agencies.

Fig: Mobile ATMs

- **Smart ATMs:** Smart ATMs incorporate advanced technologies such as touchscreen interfaces, biometric authentication, and contactless card readers to offer enhanced user experiences and security features. They may also provide additional services like bill payments, fund transfers, and account management.

Fig: Smart ATMs

Problem Formulation:

- Despite advancements in ATM technology, traditional authentication methods such as PINs and magnetic stripe cards remain vulnerable to security threats such as skimming and card cloning. As a result, there is a pressing need to explore and implement more robust authentication.
- A software is to be designed that reads an ATM card, a keyboard and display for interaction with the customer, a cash dispenser in multiples of Rs 100, Rs 200 and Rs 500, a printer for printing customer receipts.
- In terms of Information Security (IS) for ATMs, cybersecurity is a critical concern. ATMs face threats like skimming, malware attacks, and physical tampering.

Objectives of the Work:

- Designing of a software that reads an ATM card and display for interaction with the customer, a cash dispenser in multiples of Rs 100, Rs 200 and Rs 500 to dispense money, a printer for printing customer receipts.

- To develop a framework or guidelines for integrating advanced authentication technologies into ATM systems while ensuring usability, reliability, and compliance with regulatory requirements.

- To explore and evaluate advanced authentication technologies such as biometrics (e.g., fingerprint scanning, facial recognition) and token-based authentication (e.g., dynamic CVV) for their suitability in ATM environments.

- Implementing data encryption between the ATM and the processing center, preventing arbitrary code execution, and safeguarding against network attacks targeting ATM transactions. Additionally, securing communication with the card reader, encrypting card data, and adhering to best practices outlined in the report are essential to mitigate card data theft.

Methodology used:

Optimizing ATM Cash Management Using Machine Learning:-

- **Using the past to predict the future:** An efficient ATM cash management system needs a cash demand forecasting model for each ATM. This forecasting model is mostly based on historical cash demand data. Cash withdrawals are subject to trends and generally follow weekly, monthly, and annual cycles.

Harnessing artificial neural networks:-

- **Artificial neural networks (ANNs):** are extremely flexible function approximators that are used in machine learning applications such as pattern recognition, classification, and time series forecasting. ANNs map the nonlinear relationships between numerous factors affecting cash withdrawal and cash demand.

Results and Outputs:

Security Measures:

- **PIN Validation:** The ATM software implements PIN validation to ensure that only authorized users can access their accounts. Upon entering the PIN, the system verifies it against the stored PIN. If the entered PIN matches, the user is granted access to perform transactions.

- **Card Blocking:** The system includes a mechanism to block the card if the user enters an incorrect PIN multiple times. After a certain number of unsuccessful attempts, the card is blocked for 24 hours. This measure protects against unauthorized access and potential PIN guessing attacks.

- **PIN Reset:** In case the user forgets the PIN or the card gets blocked, the system prompts the user to contact the bank for a PIN reset. This ensures that only the legitimate cardholder can reset the PIN and regain access to their account, enhancing security and preventing unauthorized PIN changes.

Conclusion:

- In conclusion, vulnerabilities related to network security, improper configuration and poor protection of peripherals taken together, provide criminals with the ability to steal ATM cash or obtain card information.
- Logging and monitoring security events facilitate prompt threat detection and response. Regular security analyses, including reverse engineering of ATM software, are crucial for identifying and addressing vulnerabilities, including zero-day exploits, to mitigate emerging threats effectively.

References:

- https://paytm.com/blog/atm/
- https://www.scribd.com/document/
- https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/
- https://www.visionet.com/blog/optimizing-atm-cash-management-using-machine-learning