# Fingerprint-Based ATM System: A Biometric Approach to Secure Banking

Mohar Singh Gurjar, Student, mail.mohargurjar@gmail.com

Ritu Saini, Student, sainiritu132@gmail.com

Ankit Goyal, Student, 2021pietadankit004@poornima.org

Dept. of Artificial Intelligence & Data Science

Poornima Institute of Engineering & Technology

Jaipur, Rajasthan, India

M/s. Bhawana Kumari, Assistant Professor

bhawana.kumari@poornima.org

Dept. of Artificial Intelligence & Data Science

Poornima Institute of Engineering & Technology Jaipur,

Rajasthan, India

 Abstract

**In society, rapid advancement in technology along with increasing dependence on digital access of information has posed the security of transactions as one of the most important aspects. The Automated Teller Machine (ATM) was designed to offer 24/7 banking service but is highly threatened by security issues such as card skimming, pin theft, identity fraud, and unauthorized access. This paper presents a robust and innovative solution to these issues called a Fingerprint Based ATM System that uses biometric verification with customary banking modes. This hybrid approach is more secure and accessible for users of financial services as the members in the digital transformation plan in the modern financial sector. The application was implemented utilizing python and Tkinter for the user interface, while the SQLite was an effective database to manage users credentials and transaction logs. The ATM system supports two transaction modes: conventional card access and biometric (cardless) fingerprint access. The dual access approach provides servants of financial services with flexibility and an increased range of usability, which increases the ATM applications user diversity. The fingerprint authentication system addresses the glaring weaknesses to pin and card systems in relation to options with double verification that is almost impossible to duplicate or exploit.**

**Through a comprehensive testing and validation process this system has shown significant reductions in ATM fraud, improvement in user authentication and principal security in financial data confidentiality and integrity. This paper outlines the design architecture; system components; software development process; and implications of the implementation of**

**biometric systems in the financial industry. It also highlights future directions including QR-based transactions; a cloud-based payment**

**system; and real-time fraud detection.**

Introduction

Automated Teller Machines (ATM's) are fundamental to the modern banking system, giving access to financial services for millions of users globally. Most ATM transactions use a magnetic stripe, chip card, and a Personal Identification Numbers (PIN) for identifying users. In their widespread usage, ATM systems have demonstrated an increasing threat to ATM systems from many attacks including card skimming, card cloning, shoulder surfing, and brute force PIN hacks. The financial industry has a need for more secure and reliable user identification technologies.

Biometric authentication systems, particularly fingerprint recognition systems, have become a viable alternative to passwords and cards. Biometric traits are unique to each person, thereby making it a non-transferable trait that is also very difficult to counterfeit. Fingerprints are a fast and convenient way of uniquely identifying people and converting a person’s fingerprint to a digital image is a fast, accurate, and simple process. As image processing algorithms continue to advance quickly and biometric hardware is inexpensive and accessible, creating fingerprint-based security solutions for real-world uses becomes a more practical option.

This research project will be on the real-world implementation and deployment of a Fingerprint-Based ATM System to increase the security of banking services. The ATM system will be biometric (fingerprint) and will give the bank customer several access methods (biometric and

traditional card access) to access their banking

services to accommodate their attitude toward any biometric access process and their access capabilities. In addition to any banking security precautions, this project will seek to ensure usability, robustness of the system, and value for money for both urban and rural banking eco-systems.

The overarching motivation for this project is driven by the increasing prevalence of ATM fraud and identity theft. If successful, our system will complete the security aspect of traditional ATM services with biometric authentication. The project will also note the advantages having used open-source technology to a create modular financial systems capable of scaling over, for example, the national identity systems. It will be both a research exercise and a prototype that can extend to support more biometrics and combinations if needed.

Literature Review

The use of biometric technologies has proliferated in many sectors, such as border security, health care, mobile devices, and finance. Within banking, biometrics have emerged as a significant technology for improve identity verification and reducing fraud. Due to its maturity and accuracy, fingerprint recognition has become one of the most prevalent biometric modalities. Fingerprint recognition systems have operating low false acceptance and false rejection rates (Jain et al., 2004), making them attractive for applications requiring a high level of security. For example, Maltonietal. (2009) considered various fingerprint matching algorithms and proposed that minutiae-based systems provide the best performance in real-world settings.

Overall, these studies provide a robust indication of the extent to which fingerprint authentication can be integrated in banking applications.

Real-life implementations serve as a further demonstration of the viability of these systems. The Aadhaar-enabled Payment System (AEPS) in India has served over a billion fingerprint-based transactions in both urban and rural populations (Dewan, 2018). Nigeria's Biometric Verification Number (BVN) links a customer’s biometric data with their bank account and should help eliminate uncertainty in the identification process as well as ultimately reduce fraud committed against a bank customer. Brazil has also explored mobile banking options using biometric fingerprints for pension payments and welfare services (Matos, 2017). Chatterjee and Bhattacharyya (2018) performed an analysis of biometric banking from socio-technical dimensions and highlighted the necessity for rigorous data protection. The authors acknowledged that while biometric authentication is regarded as a significant anti-fraud method, it created new issues concerning privacy, misuse of data, and technology literacy. Rathaetal. (2001) also noted the importance of protecting biometric templates from spoofers and other attackers using encryption and secure transmission channels. Several regulatory bodies have also considered the problems surrounding biometric systems. The General Data Protection Regulation (GDPR) from Europe and the Personal Data Protection Bill from India both outline strict measures for the collection, processing, and storing of biometric data to ensure that biometric methods do not contravene user rights and privacy.

This paper contributes to the literature by proposing an original and modular system that combines biometric authentication with traditional ATM functions. It draws lessons from academic work and real-world deployments and proposes a system that is implementable, secure, and user-friendly. The project drew on both technical and human factors, providing a preliminary standard for future biometric-enabled financial systems.

System Architecture

Our Fingerprint-Based ATM System will consist of a layered architecture that maximally enhances modularity, maintainability, and scalability. The layered architecture will consist of:

Presentation Layer: This layer is created using the Python Tkinter library menu system. This layer provides the user interface for users to interact with the system through distinct, visible, and easy to navigate screens. It includes modules for login, registration, transaction, and feedback/error screens.

Application Logic Layer: This layer provides the glue connecting the user interface and the data layer in the database. It takes in the user inputs, executes the transaction logic, processes biometric images, and performs security checks. In this layer, all validations, business logic, and security conditions are handled.

Data Layer: The data layer is built-on SQLite, which stores necessary data such as user credentials, transaction history, fingerprint hashes, session handling logs, and a trail of changes to the data. The data base is constructed such that it is normalized, ensuring optimal performance out of each query run on it, which is aided by referential integrity.

System Features and Modules:

Dual Transaction Modes:

1. Card Mode: Users authenticate using a combination of Card Number, CVV, and a secure PIN. This mode mimics the experience for the traditional ATM users.

2. Cardless Mode: Users upload a fingerprint image and use a secure PIN to authenticate. Upon successful match, users will gain access to ATM services. If we do not match the fingerprint, the user is expected to be prompted to register.

Authentication Module: Authentication is provided with combinations of usernames, passwords, PINs, and fingerprints. The comparison of fingerprint images is accomplished using image hashing algorithms in comparing the uploaded fingerprint images and the saved templates.

Transaction Module: Transactions with functionalities such as Balance Inquiry, Cash Withdrawal, Deposit Funds, Change PIN, and more, will be enabled through the transaction module. A historical transaction log will be created in all actions.

Registration Module: The module for the registration of new users, collects personal information and biometric fingerprint images. The registration module will ensure there are no duplicates, and that secure information storage is adhered to.

Security Module: The security module includes many features such as limits on multiple attempts, locking accounts, encrypting storage, rolling-back features.

Logging and Monitoring Module: The logging and monitoring module maintains log files for security purposes (i.e. audits), performance of the system, and debugging.

This system design not only meets our functional needs now but provides a framework for extending our functionality in the future, such as inclusions KR Codes, Mobile Authentication and/or Cloud based services.

Methodology

The process frameworks demonstrated in the project life cycle were based on fundamental software engineering principles and were deliberately designed to emphasize an iterative development cycle, user engagement, and testing.

Requirements Gathering: Requirements were decided through literature reviews, user surveys, and interviews with individuals at several banks. Priorities included security of the system, usability, modular, and low hardware coupling.

System Design: The processes were developed using the UML. Models such as use case and class diagrams and data flow diagrams were produced to represent system interactions and data paths. System states were represented using state transition models.

4.1 Technology stack:

- Python 3.10 for application development

- Tkinter for the GUI

- SQLite for local database storage

- PIL, OpenCV, and image hash for dealing with fingerprints

- NumPy for processing the image arrays

4.2 The Development Process:

Phase I: GUI Development with validation prompts

Phase II: Integration of traditional card-based authentication

Phase III: Implementation of biometric verification

Phase VI: Integrating transaction module and hardening security

4.3 Testing:

Unit Testing: Custom test cases with Pytest to test every function

Integration Testing: Ensure all functionality is seamless from end to end across modules

User Testing: 20 users tested the prototype, conspicuously inputting feedback about UI/UX

Load Testing: Multi-threading simulated a high number of access hits to test access frequency

Implementation

The Fingerprint-Based ATM System was developed using a modular and incremental development methodology. This approach allows for ease of understanding, maintainability, and the ability to debug problems as they arise. The development can be broken down into many modules, where each module is purpose-built, communicating with other modules using APIs.

5.1 User Interface Development

The GUI user interface was built using Tkinter for Python, which provides a lightweight graphical environment that can be run on multiple platforms. The pages are:

Main Page: This user interface page welcomes the user with the words: "Welcome to Bank!" and requests the user to select the transaction mode they prefer: Card or Cardless.

Authentication Pages: Card Mode provides a card number, CVV, and pin entry page. Cardless Mode provides the fingerprint upload and a pin entry page.

ATM Operating Page: After successful authentication, the user sees a page with the options Check Balance, Withdraw Cash, Deposit Cash, and Change PIN.

Registration Page: New users are provided with a form to enter their basic information, including an image of their fingerprint to be enrolled.

5.2 Biometric Integration.

For fingerprint processing, the design employed Python Imaging Library (PIL), OpenCV, and Image Hash libraries:

Uploaded fingerprint images are converted to grayscale and resized for uniformity.

The image is then hashed using perceptual hashing (p-hash) functionality which generates a unique and compact representation of the processed image.

Authentication occurs with a comparison of the hash of the uploaded image to the hashed images in the database.

Authentication also allows for minor tweaks in the input images.

5.3 Database Design

The backend was managed using SQLite which is a lightweight and self-contained database engine. In the SQLite backend there is:

Users Table: user id, username, card number, CVV, hashed PIN, fingerprint hash, registration date.

Transaction Table: stores each transaction individually, with transaction type, amount, time of transaction, and transaction status.

Audit logs: maintains records of attempts to log in, whether the authentication was successful, attempts that resulted in errors.

Security measures were implemented. Such as hashing sensitive data, limiting access to directly creating SQL queries or select statements on the back end, and parameterized statements to prevent SQL injections or leaks in the data.

5.4 Transaction Process

Authenticated users can carry out ATM Transaction operations:

Balance Inquiry - the system retrieves the overall balance.

Withdrawal of Cash - if the user requests an amount which is less than the overall balance, then it does.

Deposit Cash - deposits the user's deposit to their overall balance.

Change PIN - allows the user to change their PIN after they are verified.

Each transaction is logged, with each transaction getting a unique transaction ID.

Result And Discussion

The Fingerprint Based ATM System was evaluated in a series of controlled tests and simulated users to evaluate the functional reliability, security and usability of the system. The tests provided a wealth of information regarding the systems practical outcomes and functionality.

6.1 Performance Evaluation

Authentication Accuracy - The fingerprint recognition module uses image hashing to match inputs to be stored credential images. The testing revealed 92% authentication accuracy. Not perfect, but enough for proof-of-concept and illustrated that more complicated biometric matching algorithms are conceivable.

Authentication Speed - The average biometric authentication took 1.9 seconds while the average card-based authentication duration was 1.5 seconds.

Response Time - The average response time between login and performing operations on the ATM was 1.2 seconds, when using card-based authentication, and 2.1 seconds when using biometric authentication. The delay in biometric mode primarily stemmed from image processing and matching.

Transaction Success - Of the 200 simulated transactions, 95% of transactions completed successfully with 5% either abandoned incorrectly or aborted due to failed matches of the fake fingerprint.

Transaction Time - The average time taken of all end-to-end transactions (login to conclusion) was under 8 seconds.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Parameter** | **System****Authentication Method** | **Vulnerability to Skimming** | **Forgotten Credentials** | **Average Access Time** | **User Satisfaction (Survey)** | **Implementation Complexity** | **Security Risk** |
|  |  |  |  |  |  |  |  |
| Traditional ATM | Card + PIN | Yes | Common | ~1.1 sec | 3.7/5 | Low | High |
| Fingerprint ATM | Finger + PIN | No | Rare | ~2.1 sec | 4.5/5 | Moderate | Low |

6.2 Validation Metrics:

Authentication Accuracy: 97.5%

Average transaction Time: < 8 seconds

False Acceptance Rate (FAR): 1.2%

False Rejection Rate (FRR): 1.8%

User Satisfaction (Survey) 92%

These metrics guild to performance expectations

related to reliability, speed and usability, thus being well positioned for further deployment and research.

6.3 User Experience Feedback

Feedback was obtained from 20 users with various levels of technical expertise:

Ease of Use: 85% said it was an intuitive interface and easy to use.

Security Perception: 90% believed the fingerprint system enhanced security.

Suggestions: User inputs included mobile notifications for transactions/users, and the inclusion of face recognition.

6.4 Security Evaluation

The system successfully prevented all brute-force PIN attempts after three attempts, locking the session automatically.

Fingerprint spoofing attempts (i.e., uploads of non-

demonstrating a basic level of input validation, that nonetheless worked.

The logging mechanism ensured that all access attempts (successful and unsuccessful) are logged which is essential for post-incident analysis and audit trails.

6.5 Comparison Evaluation

The results support that fingerprint authentication for ATM systems demonstrate that it is feasible to integrate increased authentication measures that will support enhanced security features and provide a higher level of user acceptance and satisfaction. However, significant real-world adoption would require stronger infrastructure support and more advanced fingerprint recognition algorithms.

6.6 Advantages

Improved Security: Biometric data is non-transferable and not easily replicated. The chances of unauthorized access are significantly lower.

Increased Accessibility: Card-less transactions address transactional convenience, particularly in contexts of rural users or semi-literate users.

Low-cost Design: Built using open-source tools, and low hardware requirements, enables deployments of the system where there are minimal resources.

6.7 Limitations

Although the system is performing well, several limitations were identified as follows:

Variability of Image: Fingerprint recognition can fail for reasons of poor imaging, dirty sensors or worn-out fingerprints.

Privacy: Users are concerned for how you store and use their biometric data.

Scalability: There will be a transition beyond SQLite, which is adequate for the small-scale development stage, to enterprise-level databases if deployed on a national scale.

Security of Local Storage: Biometric data is stored in locally, so anyone with access to the machine could potentially turn the biometric data into malfeasance

unless adequate encryption is in place.

These limitations give rise to areas of improvement and iterations for future work.

6.8 Ethical Considerations Consent:

Consent must be obtained prior to physiological biometric data collection.

Transparency: Users ethics must be informed on the nature, and length of time that the biometric sample might be used.

Protection of Data: comply with statutory procedures such as GDPR, ensures that the system acts in consideration of user rights and privacy.

Conclusion

This paper presents a Fingerprint-Based ATM System's Design and Implementation aimed at security and convenience in banking transactions. It provides users with rich and varied needs through modular architecture and dual-mode ATM transaction interface while also providing protection from common ATM fraud.

The biometric fingerprint authentication method is widely considered a reliable second factor of security and represents a vital personal identity and security essential in an environment of growing cyberspace and physical banking risks. Performance evaluations have shown speed, accuracy, and users' satisfaction levels promising.

The proposed ATM structure balances security with technology that is commonly available to the public while providing value through strong encryption and safe authentication protocols. It is presently developed as a prototype ATM, and the solution provides promising opportunities for full implementation within existing banking infrastructures.

Future Scope

Several improvements and additions can be looked at for future versions of the system:

QR-Based Access, Cardless: Adding QR-based cardless access using mobile apps.

Cloud database: Moving to the cloud for better scalability, backup, and remote monitoring.

Multi-biometric system: Incorporating facial recognition or iris scanning for accuracy and inclusiveness. Real-time fraud detection:

Mobile banking integration: Linking the ATM system with mobile banking apps for notification and monitoring of transactions, fund transfers, pin management.

With these enhancements, the Fingerprint-Based ATM System can become the next generation of banking, aligned with secure, inclusive, and digital-first financial services.

References

**-** Jain, A.K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology.

**-** Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer.

**-** Chatterjee, S., & Bhattacharyya, D. (2018). Biometric Authentication: A Review of the State-of-the-Art. International Journal of Biometrics.

**-** Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal.

**-** European Union. (2018). General Data Protection Regulation (GDPR).

**-** Government of India. (2019). Personal Data Protection Bill.