IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207067|

Biometric-Driven ATM Services

Ananya A.V[1], Usha M[2]

Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Department of MCA, Bangalore Institute of Technology, Karnataka, India[2]

ABSTRACT: This paper outlines the development and deployment of a Biometric-Driven ATM system that utilizes fingerprint and facial recognition technologies for user authentication. The primary goal is to improve ATM security and user convenience by eliminating physical ATM cards and PINs. Implemented on a local server, the system exhibits strong performance in real-time biometric authentication, ensuring both secure and efficient transaction processing. This paper details the methods for data collection, pre-processing, model training, and system integration, as well as the outcomes of rigorous testing phases that affirm the system's efficacy.

KEYWORDS: Biometric-Driven ATM, Biometric Authentication, Fingerprint Recognition, Facial Recognition, Machine Learning, Local Server, Security, User Convenience

I. INTRODUCTION

Automated Teller Machines (ATMs) are essential for modern banking, offering users convenient access to their accounts. However, traditional ATMs that rely on cards and PINs are vulnerable to security threats like card skimming and PIN theft. This paper proposes an innovative Biometric-Driven ATM system that employs biometric authentication to address these vulnerabilities. By using fingerprint and facial recognition technologies, the system enhances security and provides a smoother user experience. The implementation, performed on a local server, encompasses comprehensive data processing, model training, and system integration.

II. PROBLEM STATEMENT

Traditional ATM systems, which rely on physical cards and PINs, are increasingly prone to fraud and security breaches. Issues such as card skimming, cloning, and PIN theft compromise user security, while the necessity of carrying physical cards poses both inconvenience and risk of loss or theft. There is a critical need for an alternative authentication method that enhances security and improves user convenience. This project aims to develop a Biometric-Driven ATM system that leverages biometric authentication to address these issues and enhance the overall user experience.

III. LITERATURE SURVEY

Existing System

The existing ATM system primarily relies on physical ATM cards and PINs for user authentication. While this method provides a basic level of security, it is susceptible to various security threats. Common issues include:

1. **Card Theft:** Physical ATM cards can be stolen, allowing unauthorized access to the user's bank account if the thief also obtains the PIN.
2. **Skimming:** Skimming devices installed on ATMs can capture card information, leading to fraudulent transactions.
3. **PIN Fraud:** Shoulder surfing and other techniques can compromise the security of PINs, making it easier for criminals to access accounts.
4. **Loss and Inconvenience:** Losing an ATM card can create significant inconvenience, especially when immediate access to funds is required.

Proposed System

The proposed card-less ATM system addresses the security vulnerabilities of the existing system by utilising biometric authentication methods. Key features of the proposed system include:

1. **Fingerprint Recognition:** Utilises Minutiae feature extraction techniques to authenticate users based on their unique fingerprint patterns.
2. **Face Recognition:** Employs Convolutional Neural Networks (CNN) to accurately recognise and authenticate users based on their facial features.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207067|

3. **Multi-user Access:** Allows multiple authorised users to access a single account without the need for physical cards, providing flexibility and convenience.
4. **Enhanced Security:** Eliminates the risk of card theft, skimming, and PIN fraud by relying on biometric data for authentication.

Methodology

1. Data Collection:
- Face image datasets were gathered using a custom application designed to capture and store images under various conditions.
- Fingerprint datasets were obtained from Kaggle, ensuring a diverse and comprehensive collection.

2. Data Pre-Processing:
- Images were resized to standardized dimensions and divided into training and testing sets.
- Additional pre-processing techniques, such as converting images to grayscale and normalizing data, were applied to improve data quality.

3. Model Training:
- Convolutional Neural Networks (CNNs) were employed to train models for both fingerprint and facial recognition.
- The training process involved feeding the pre-processed data into the CNNs and fine-tuning hyperparameters to enhance accuracy.

4. System Integration:
- The trained models were incorporated into the ATM system, which operates on a local server.
- The system was designed to process biometric data in real-time, ensuring secure and efficient transaction handling.

5. Testing:
- Extensive testing was performed, including functional, performance, security, usability, and system stability evaluations.
- Test cases were developed to cover a wide range of scenarios, ensuring thorough assessment.

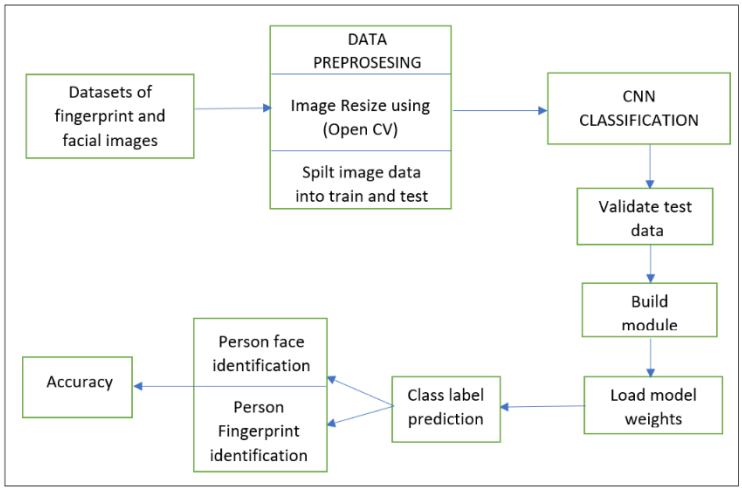

Fig 1.1 System Architecture

Results and Discussion: The testing phase confirmed that the Biometric-Driven ATM system effectively authenticated users using fingerprint and facial recognition. Key findings include:
- Accuracy: The CNN models achieved high accuracy rates in biometric recognition, validating the pre-processing and training methodologies.
- Performance: The system demonstrated reliable performance under various load conditions, with quick response times and stable operation.
- Security: The system effectively prevented unauthorized access and protected biometric data through encryption and secure storage.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207067|

- User Experience: Users reported a positive experience, noting the system's ease of use and added convenience.

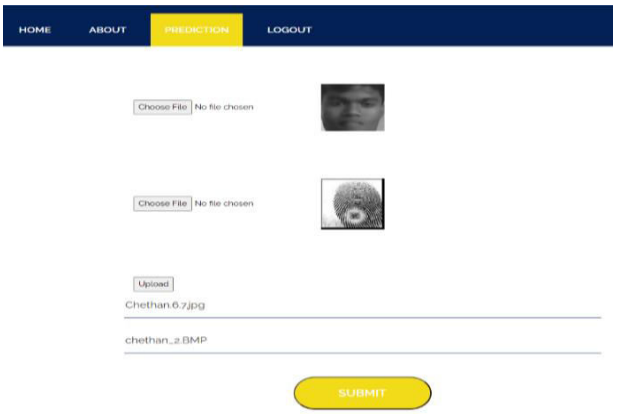

Fig 1.2 Image unloading page

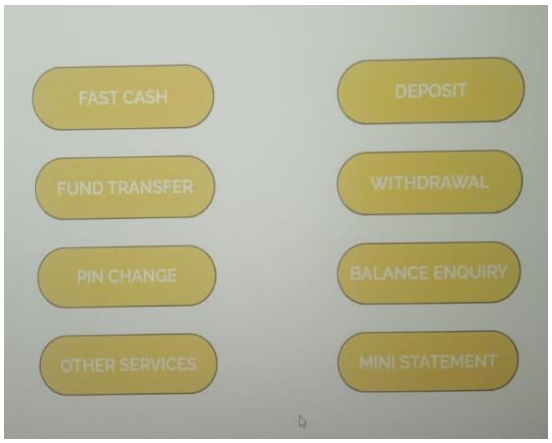

Fig 1.3 Transaction page

These results affirm that the Biometric-Driven ATM system significantly improves security and user convenience, providing a viable alternative to traditional ATM authentication methods.

Future enhancement

1. Multimodal Biometric Authentication:

- **Additional Biometric Modalities:** Incorporating additional biometric modalities such as iris recognition, voice recognition, and palm vein recognition can further enhance security and reduce the likelihood of spoofing attacks.

2. User Experience Improvements:

- **Accessibility Features:** Adding accessibility features, such as voice assistance and screen readers, can make the system more accessible to users with disabilities.

REFERENCES

1. Jain, A. K., Nandakumar, K., & Ross, A. (2008).Biometrics: Technology, Systems, and Applications.Springer.
2. Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003).Face recognition: A literature survey.ACM Computing Surveys (CSUR), 35(4), 399-458.
3. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009)Handbook of Fingerprint Recognition.Springer Science & Business Media.
4.Schroff, F., Kalenichenko, D., & Philbin, J. (2015).Facenet: A unified embedding for face recognition and clustering.Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 815-823.
5. Kumar, A., Zhang, D., & Miao, Z. (2017).Biometric recognition: Security and privacy concerns.IEEE Security & Privacy, 15(5), 80-87.
6. Bolle, R., Connell, J., Pankanti, S., Ratha, N., & Senior, A. (2003). Guide to biometrics. Springer Science & Business Media.
7. Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer Science & Business Media.
8. Ratha, N. K., & Bolle, R. M. (1998). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details