# SYNOPSIS

## Report on

**Smart ATM Using Face Recognition**

**And Fingerprint**

**by**

Manmeet Chauhan 2200290140085

Manan Sharma 2200290140084

## Session:2023-2024 (3rd Semester)

Under the supervision of

## Dr. Amit Kumar Gupta

**KIET Group of Institutions, Delhi-NCR, Ghaziabad**



**DEPARTMENT OF COMPUTER APPLICATIONS**

**KIET GROUP OF INSTITUTIONS, DELHI-NCR, GHAZIABAD-201206**

(NOVEMBER- 2023)

# ABSTRACT

In recent years, the banking and financial sectors have witnessed a significant increase in security breaches and fraudulent activities at Automated Teller Machines (ATMs). To address these challenges, there is a pressing need for innovative and robust security measures. This abstract introduces a cutting-edge solution: Smart ATM Face Recognition and Fingerprint Authentication System.

The proposed system leverages the power of biometric authentication to enhance ATM security. It combines two biometric modalities, facial recognition and fingerprint authentication, to create a multi-layered security protocol that ensures the identity of ATM users.

The face recognition component employs state-of-the-art deep learning algorithms to accurately and rapidly identify users by analyzing facial features such as eye placement, nose shape, and unique facial contours. By integrating this technology, ATM transactions become not only more secure but also more convenient, as users no longer need to carry physical cards or remember PINs.

The fingerprint authentication system adds an additional layer of security by requiring users to provide their fingerprint for authentication. This biometric information is stored securely and compared in real-time with the user's registered fingerprint data, ensuring that only authorized individuals can access ATM services.

**Key features of the Smart ATM Face Recognition and Fingerprint Authentication System include**:

Enhanced Security: By combining two biometric factors, the system significantly reduces the likelihood of unauthorized access and fraudulent activities at ATMs.

User Convenience: Eliminating the need for PINs simplifies the user experience and reduces the risk of card theft or compromise.

Real-time Verification: Both facial recognition and fingerprint authentication occur in real-time, providing immediate feedback to users and preventing unauthorized access.

Data Protection: Biometric data is securely stored and encrypted, prioritizing user privacy and complying with data protection regulations.

The Smart ATM Face Recognition and Fingerprint Authentication System represents a significant advancement in ATM security. It not only safeguards user transactions but also enhances the overall ATM experience by combining top-notch security with user-friendly convenience. This innovative approach is poised to redefine ATM security standards and combat the growing threats of fraud and identity theft in the banking sector.

**Keywords:-**ATM , security, fraud , Face recognition and fingerprint.

# TABLE OF CONTENTS

1. Introduction 4
2. Literature Review 5
3. Project Objective 6
4. Research Methodology 7
5. Project Outcome 9
6. Proposed Time Duration 10
7. [References 11](#_TOC_250000)

## Introduction

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still subjected to thefts and frauds.

In an era defined by technological innovation, the banking industry continues to evolve to meet the ever-growing demands of its customers. Traditional Automated Teller Machines (ATMs) have come a long way from their inception, providing a convenient means for individuals to access their funds and conduct financial transactions. However, as the digital landscape expands, so do the challenges associated with security and user authentication.

To address these challenges and ensure the highest level of security for banking transactions, a new breed of ATMs has emerged – the Smart ATM. Smart ATMs combine cutting-edge technology with biometric authentication methods such as face recognition and fingerprint scanning, ushering in a new era of banking convenience and security.

This introduction will delve into the concept of Smart ATMs, highlighting the integration of face recognition and fingerprint authentication technologies and their transformative impact on the banking industry. We will explore the key benefits of this innovation, including enhanced security, improved user experience, and the potential to reduce fraud and identity theft. Moreover, we will examine the implications of Smart ATMs for both consumers and financial institutions, as well as the broader implications for the future of banking.

## Literature Review

The proposed method for ATM card security involves combining PIN verification with fingerprint recognition to enhance authentication during transactions. The use of an efficient minutiae feature extraction algorithm ensures accurate fingerprint verification. Additionally, to ensure transaction security approval messages are sent to the client through GSM technology, and the location is identified via GPS. If any unauthorized person attempts to use the card, the system automatically blocks it and sends detailed information to the customer. This approach offers increased security by effectively identifying and reducing fraud risks. The proposed scheme in focuses on the security concerns related to payment transactions using NFC equipped devices such as ATMs and smartphones. It introduces a new method that combines RFID and NFC with an authentication protocol to enhance security and minimize transaction time. The proposed solution is evaluated for security against different attacks and compared with existing methods, demonstrating its effectiveness in terms of security and performance. The proposed scheme in highlights the use of fingerprints as a secure authentication method in place of traditional PIN numbers. The proposed system displays multiple banking screens upon successful fingerprint recognition, allowing customers to choose the desired bank for transactions. The model also suggests the use of a reference fingerprint in case of emergencies. The unique and unchangeable nature of fingerprints makes them a reliable biometric feature for enhancing security in digital image processing.

The main purpose of the paper is to focus on the need for enhanced customer data security in banking systems. The proposed application aims to provide a secure and convenient solution by allowing users to integrate multiple bank accounts into a single card with a unique PIN number. Face recognition technology is utilized for user verification, and user behavior is monitored using HM M-Model, enabling formula-based authentication. Additionally, the system allows users to include their family members' account details within the same card, providing a comprehensive and efficient banking solution**.**

## Project Objective

When developing a project involving face recognition and fingerprint recognition technologies, the objectives should align with the goals and requirements of the specific application. Here are some common project objectives for such systems:

**Identity Verification**: Authenticate individuals by accurately recognizing their faces, enhancing security in various applications like access control, online authentication, and mobile device unlocking.

**Customer Experience**: Improve customer experience in retail by personalizing services based on facial recognition data, such as personalized recommendations and greetings.

**Security Surveillance**: Implement facial recognition in security surveillance systems to identify known persons of interest or detect unauthorized access.

**Multi-Factor Authentication**: Utilize facial recognition as part of a multi-factor authentication system, enhancing security for sensitive data and transactions.

**Data Privacy**: Ensure compliance with data privacy regulations, such as GDPR or CCPA, by securely handling and protecting facial recognition data.

**Scalability**: Design the system to be scalable to handle a growing number of users or applications.

**Biometric Authentication**: Authenticate users based on their unique fingerprints, providing secure access to devices, applications, or physical locations.

**Criminal Identification**: Utilize fingerprint recognition for law enforcement purposes, aiding in criminal identification and record-keeping.

**Border Control** : Enhance border security and immigration processes by using fingerprint recognition for identity verification.

**­­­­­­­­Financial Transactions**: Secure financial transactions by integrating fingerprint recognition into mobile banking apps and payment systems.

**Data Security**: Enhance data security by using fingerprint authentication to unlock mobile devices or access sensitive data.

**Efficiency**: Improve operational efficiency by reducing the time and effort required for identity verification in various applications.

**Quality Control**: Ensure that fingerprint recognition systems can accurately capture and identify fingerprints, even in challenging conditions.

**Data Integrity**: Protect the integrity and privacy of fingerprint data through encryption and secure storage.

## RESEARCH METHODOLOGY

1. **Problem Identification and Definition**:

* Clearly define the problem you intend to address with the Smart ATM system.
* Specify the goals and objectives of the research.

1. **Data Collection**:

* Gather data on ATM usage patterns, security concerns, and user preferences.
* Collect facial recognition and fingerprint data to build the authentication system.
* Ensure data privacy and ethical considerations are addressed.

1. **System Development**:

* Design and develop the Smart ATM system incorporating face recognition and fingerprint technology.
* Implement appropriate algorithms for biometric authentication.
* Ensure integration with the ATM hardware and software components.

1. **Testing and Validation**:

* Conduct testing and validation of the Smart ATM system.
* Perform usability testing to assess user experience.
* Evaluate the accuracy and reliability of the biometric authentication methods.

1. **Data Analysis**:

* Analyze the collected data using appropriate statistical or qualitative analysis techniques.
* Interpret the results to draw conclusions related to system performance and user satisfaction.

1. **Discussion and Findings**:

* Discuss the findings in the context of your research objectives.
* Compare your system's performance with existing solutions.
* Address any limitations and potential improvements.

1. **Discussion and Findings**:

* Discuss the findings in the context of your research objectives.
* Compare your system's performance with existing solutions.
* Address any limitations and potential improvements.

## Project Outcome

Certainly, here are the expected technical outcomes of the Smart ATM using face recognition and fingerprint project:

1. **Enhanced Security**:
   * Improved security measures through the integration of face recognition and fingerprint recognition, reducing the risk of unauthorized access and fraudulent activities.
2. **Biometric Authentication Capabilities**:
   * Successful implementation of reliable and secure biometric authentication methods, enhancing ATM security and user convenience.
3. **Reduced Fraud and Unauthorized Access**:
   * A significant reduction in fraudulent activities related to ATM usage, leading to cost savings for banks and increased trust among customers.
4. **User-Friendly Interface**:
   * An intuitive and user-friendly interface that simplifies the ATM transaction process, making it accessible to a diverse range of users.
5. **Efficient Transactions**:
   * Faster and more efficient ATM transactions due to quicker biometric authentication, reducing wait times for users and enhancing overall operational efficiency.
6. **Choice of Authentication Method**:
   * Users have the option to choose between face recognition and fingerprint recognition, providing flexibility and catering to individual preferences.
7. **Enhanced Access Control**:
   * The capability to use biometrics for access control in secure areas, such as bank branches, data centers, or restricted zones.
8. **Usability Testing and Feedback**:
   * User testing results and feedback on the Smart ATM's interface and features, leading to iterative improvements to enhance the user experience.
9. **Privacy and Data Protection**:
   * Implementation of robust privacy safeguards and compliance with data protection regulations to ensure the security and privacy of users' biometric data.
10. **Compliance and Security Measures**:
    * Documentation of security measures and countermeasures against potential threats, including spoofing attacks and unauthorized access.
11. **Integration with Banking Systems**:
    * Seamless integration with the bank's core systems for account access, transaction processing, and account updates.

**Proposed time duration**

|  |  |
| --- | --- |
| **Week Number** | **Tasks** |
| **Week 1-2:**  **Project Initiation and Planning** | 1. Define project objectives and goals. 2. Assemble the project team. 3. Establish communication and collaboration tools. 4. Identify user requirements and technical specifications. |
| **Week 3-4:**  **System Design and Front-end Development** | 1. Develop the system architecture. 2. Design the database structure. 3. Create the user interface. |
| **Week 5-6:**  **Core Development for Backend** | 1. Ensure seamless data flow between the front-end and back-end. 2. Develop the face recognition. 3. Create initial question/response logic. |
| **Week 7-8:**  **Testing, Refinement, and Deployment** | 1. Conduct thorough system testing. 2. Gather initial user feedback. 3. Identify and address issues and bugs. 4. Continue testing and refinement based on user feedback. 5. Finalize the project codebase and configurations. 6. Prepare a presentation and demonstration for the project's final submission. |

# REFERENCES

1. Mithun Dutta, Kangkhita Kaem Psyche, Tania Khatun, Md. Ashiqul Islam, Md. Azijul Islam “ATM Card Security Using Bio-metric and Message Authentication Technology”, 2018 IEEE International Conference on Computer and Communication Engineering Technology(CCET).
2. Abhijeet Boragule, Kin Choong Yow, Moongu Jeon, “On-device Face Authentication System for ATMs and Privacy Preservation”, 2023 IEEE International Conference on Consumer Electronics (ICCE).

1. Bachu Sricharan, Jakanagari Uma Sanjana, Vanitha Vani, Vanitha Vani, “RFID based ATM security system using IoT”, IEEE 2022 International conference on the intelligent controller and computing for smart power.

1. Samir Chabbi, Chaouki Araar “RFID and NFC authentication protocol for securing a payment transaction”, IEEE 2022, 4th International Conference on pattern analysis and Intelligent systems.
2. Jignesh J. Patoliya, Jignesh J. Patoliya, “Face Detection based ATM Security System using Embedded Linux Platform”, 2017 2nd International Conference for Convergence in Technology (I2CT).
3. Kowshik, Sheetal Rao M S, Ranjitha R S, “Multi-Account Embedded ATM Card with Face Recognition Security System”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278- 0181 Published by, www.ijert.org IETE – 2020 Conference Proceedings.
4. Mohsin Karovaliya, Mohsin Karovaliya, Sharad Oza, Dr.D.R.Kalbande “Enhanced security for an ATM machine with OTP and Facial recognition features”, International Conference on Advanced Computing Technologies and Applications (ICACTA 2015).