Biometric Empowered Swiping Machine

Ramya N[1],Deepana K[2],Gayathri V[3],Dhanalakshmi S [4],Divya M[5]

[1]Assistant Professor -Department of Information Technology & Kings Engineering College-India.
[2,3,4,5]Department of Information Technology & Kings Engineering College-India

---***---

Abstract - The Biometric Empowered Swiping Machine is an innovative solution aimed at enhancing authentication security by integrating fingerprint recognition technology with traditional card-swiping systems. By utilizing biometric characteristics that are unique to each individual, the machine eliminates common vulnerabilities associated with traditional authentication methods such as PINs and magnetic stripe cards. This project is designed for diverse applications including corporate offices, educational institutions, public transport, and banking sectors. Through the adoption of deep learning algorithms, secure data encryption, and cloud storage, the system ensures accuracy, convenience, and fraud prevention. This report discusses the design, methodology, implementation, and future enhancements of the Biometric Empowered Swiping Machine.

A Biometric Empowered Vending Machine revolutionizes the traditional vending experience by integrating advanced biometric authentication technologies, such as fingerprint, facial recognition, or iris scanning. This innovative system ensures secure and convenient transactions, eliminating the need for cash, cards, or memorized PINs. Upon authentication, users can select their preferred products, and the machine accurately dispenses the chosen items.

***Key Words*:**Biometric,Swiping Machine,PINs,Vending Machine

1. INTRODUCTION

1.1 General

In the modern digital era, ensuring secure access to systems and premises is more crucial than ever before. Traditional security mechanisms relying on physical cards or PINs are increasingly becoming vulnerable to theft, duplication, and cyber-attacks. Therefore, there is a pressing need for robust, efficient, and user-friendly security systems.

1.2 Importance of Biometric Authentication

Biometrics, specifically fingerprint recognition, offer a highly reliable authentication method by utilizing the unique physiological traits of individuals. As fingerprints are nearly impossible to replicate, they offer a higher degree of security compared to traditional authentication techniques.

1.3 Objectives of the Project

- Enhance security by integrating biometric verification with card-swiping systems.
- Improve user convenience by eliminating the need for remembering passwords.
- Reduce authentication time and prevent fraud.
- Provide a scalable solution applicable across multiple sectors.

1.4 Scope of the Project

The Biometric Empowered Swiping Machine is intended for:

- Corporate employee authentication
- Student attendance management
- Ticketing systems in public transportation
- Secure banking transactions

2. LITERATURE REVIEW

2.1 Introduction

A literature review was conducted to understand the evolution, present capabilities, and challenges of biometric authentication systems. Particular focus was given to liveness detection methods and countermeasures against spoofing attacks, which are critical for securing biometric systems.

2.2 Studies on Biometric Authentication Systems

AI-driven Liveness Detection in Biometrics (2020): Deep learning-based spoof detection algorithms have improved system security, achieving 98% accuracy in identifying fake fingerprints.

2.2.1.The general methodology typically included:

2.2.1.1.DataCollection:

A large dataset was gathered, containing both **real** (live) and **fake** (spoofed) fingerprints. Spoofs were created using materials like silicone, gelatin, or printed paper.

2.2.1.2.Preprocessing

Images were standardized (resized, normalized) Augmentation techniques (rotation, scaling, noise addition) were applied to enrich the dataset and improve model robustness.

2.2.1.3.Feature Extraction:

Instead of handcrafted features, **Convolutional Neural Networks (CNNs)** were used to automatically learn spatial patterns in fingerprints:

- Surface textures
- Pore patterns
- Ridge distortions

2.2.1.4.Model Training:

Deep neural networks like:

- ResNet (Residual Networks)
- VGGNet
- MobileNet (for lightweight applications)
- **Cross-entropy loss** for binary classification (live vs spoof)
- **Adam optimizer** or **SGD** (Stochastic Gradient Descent)

2.2.1.5.Evaluation Metrics

- **True Detection Rate (TDR)**: Rate at which live fingerprint correctly detecting.
- **False Detection Rate (FDR)**: Rate at which fake fingerprints are wrongly accept all datas.
- **Average Classification Error (ACE)**.

2.3. User Interface (UI)

around **98%** on benchmark datasets (e.g., LivDet competitions datasets).

The system typically included:
Fingerprint Capture Interface:

- A graphical interface that prompts users to place their finger.
- Real-time feedback: "Authenticating...", "Live detected", "Spoof detected".

Result Dashboard:

- Shows decision (live/fake).
- Confidence score (%).
- Optionally, shows visual features (heatmaps) highlighting areas used by the AI to make the decision (for explainability).

□

Admin Control Panel:

- Manage datasets.
- Retrain/update models.
- Analyze liveness detection logs.

Deployment:
Deployed on:

- Fingerprint scanners with built-in processors (for edge AI inference).
- Or connected to remote servers via lightweight clients.

2.4. Results

- **Accuracy**: Up to **98%** across multiple spoofing materials.
- **Speed**: Fingerprint liveness detection completed in **< 1 second** in real-world systems.
- **Generalization**: Models trained on multiple spoof types performed better on unseen spoofing attacks.
- **LivDet 2019 Competition**: Top solutions used ensemble models and achieved similar high accuracies (~95-98%).

Domain	Application
Corporate Offices	Employee access control and attendance monitoring
Educational Institutions	Student verification and attendance tracking
Public Transport	Biometric ticket validation and access
Financial Sector	Secure ATM transactions and fraud prevention

Table 1: Domain and Application

3.SYSTEM ANALYSIS

3.1. Problem Identification

The current authentication systems—primarily reliant on PINs, magnetic cards, and passwords—pose serious limitations. They are vulnerable to cloning, theft, unauthorized access, and user errors. In sectors like finance, education, and transportation, these vulnerabilities compromise both security and operational efficiency. Users also face the burden of remembering passwords or carrying physical tokens, adding to friction in daily operations. Hence, a more secure, tamper-resistant, and user-friendly solution is necessary.

3.2. Proposed Solution

The Biometric Empowered Swiping Machine combines **fingerprint authentication** with **traditional card-swiping mechanisms** to create a dual-layer security system. By leveraging fingerprint recognition—an inherently secure and individual-specific trait—the system reduces the possibility of unauthorized access and ensures fast, reliable identity verification.

3.3. System Objectives

- Enhance user authentication security using fingerprint biometrics.
- Reduce fraud, identity theft, and access misuse.
- Eliminate dependency on easily compromised methods like PINs or cards alone.
- Provide multi-domain applicability (education, finance, transport, etc.).
- Support cloud integration for remote management and scalability.
- Improve user convenience with quicker authentication processes.

3.4. System Components and Modules

A. Key Hardware Modules

- **Fingerprint Sensor**: Captures and authenticates user fingerprints in real time.
- **Card Swiping Unit**: Reads magnetic or RFID cards, used as a secondary verification method.

B. Supporting Technologies

- **Cloud-Based Authentication**: Stores fingerprint templates securely and enables centralized control.
- **Encrypted Transmission (using SHA)**: Secures data as it travels between system components.
- **Multi-Factor Authentication (MFA)**: Combines biometric and card-based inputs for robust identity confirmation.

3.5. Technology Stack

- **Deep Learning Models**: Improve fingerprint recognition accuracy using CNN-based feature extraction.
- **Secure Hash Algorithm (SHA)**: Encrypts biometric data before storage/transmission to prevent leaks or tampering.
- **Machine Learning Algorithms**: Detect anomalies or unusual access patterns, offering real-time fraud detection.
- **Cloud Infrastructure**: Enables scalable, flexible, and remotely accessible data management.

3.6. System Architecture & Data Flow

Although the architecture diagram is not provided, the expected flow includes:

1. User swipes a card and places a finger on the sensor.
2. Fingerprint data is captured and encrypted.
3. Data is transmitted securely to the cloud server for verification.
4. Machine learning algorithms check for authenticity and anomalies.
5. Based on results, access is granted or denied.

4.MODULES AND UML DIAGRAM

4.1. User Authentication Module

- Captures and verifies fingerprint data.
- Reads and processes card swipe (magnetic/RFID).
- Performs dual-authentication (biometric + card).
- Handles fallback authentication when necessary.

4.2. Biometric Enrollment Module

- Allows authorized personnel to register new users.
- Captures and stores fingerprint templates.
- Encrypts and uploads data to the cloud database.

4.3. Card Management Module

- Registers and links swipe cards to user profiles.
- Supports RFID/magnetic stripe card input.
- Validates card during the authentication process.

4.4. Cloud Integration Module

- Syncs biometric and card data with centralized cloud server.
- Retrieves templates for verification.
- Stores access logs and anomaly reports.
- Supports remote system updates and monitoring.

4.5. Security & Encryption Module

- Encrypts fingerprint templates and card data (e.g., using SHA).
- Handles secure communication using SSL/TLS.
- Manages secure user sessions and admin logins.

4.6. Anomaly Detection & Machine Learning Module

- Monitors access patterns and user behavior.
- Detects anomalies or fraudulent activity in real time.
- Triggers alerts for suspicious access attempts.
- Uses AI models to continuously improve accuracy.

4.7. Access Log and Reporting Module

- Records all authentication attempts with timestamp and status.
- Generates reports for admin review.
- Supports export to CSV or PDF for auditing.

4.8. User Role & Permission Module

- Manages roles such as Admin, Operator, and User.
- Restricts access to sensitive features based on role.
- Ensures secure handling of user privileges.

4.9. Admin Dashboard Module

- Web/mobile interface for system monitoring and user management.
- Displays analytics and usage reports.

- Provides remote control for system configurations.

4.10. System Maintenance and Update Module

- Handles software/firmware updates for the device.
- Performs health checks on sensors and connectivity.
- Generates maintenance logs and error reports.

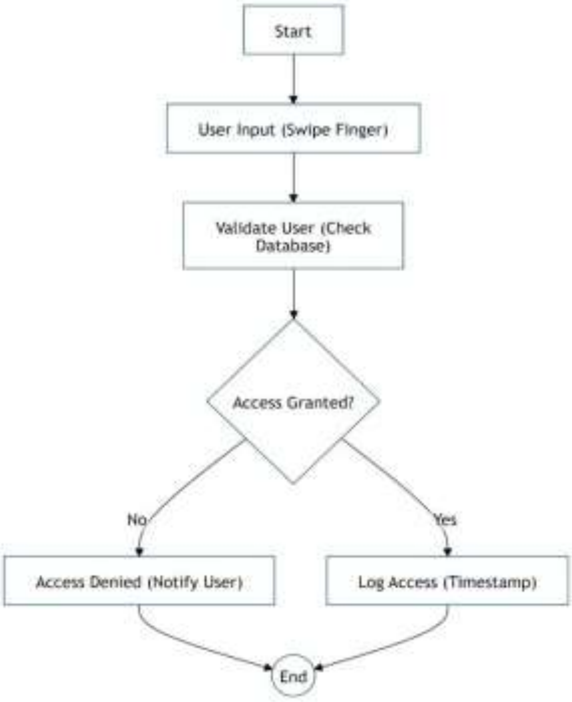

Start
User Input (Swipe Finger)
Validate User (Check Database)
Access Granted?
No
Yes
Access Denied (Notify User)
Log Access (Timestamp)
End

Fig.1.Activity Diagram

5.Applications of the Biometric Empowered Swiping Machine

5.1 Corporate Offices

Application:

- ✓ Employee attendance tracking
- ✓ Controlled access to sensitive areas
- ✓ Secure printing and device access

Benefits:

- ✓ Prevents proxy attendance ("buddy punching")
- ✓ Strengthens internal security
- ✓ Increases efficiency and accountability

Example:
In a large IT company, employees swipe their ID cards and verify fingerprints at office entrances. Sensitive sections like server rooms or R&D labs require dual authentication for entry.

5.2 Educational Institutions

Application:

- ✓ Student attendance monitoring
- ✓ Examination identity verification
- ✓ Access to libraries, hostels, and laboratories

Benefits:

- ✓ Eliminates manual attendance errors
- ✓ Prevents impersonation during exams
- ✓ Simplifies administrative processes

Example:
At a university, students use fingerprint and card swipe machines to mark attendance automatically when entering classrooms, avoiding manual roll calls and ensuring real-time monitoring.

5.3 Public Transportation Systems

Application:

- ✓ Ticket validation
- ✓ Passenger authentication for concessions

Benefits:

- ✓ Minimizes fare evasion
- ✓ Provides secure access for discounted travelers (students, seniors)

Example:
In a metro rail system, commuters swipe their smart transport cards and verify fingerprints before entering platforms, ensuring that concessions are used only by eligible individuals.

5.4 Financial Services

Application:

- ✓ ATM transactions without PINs
- ✓ Secure card payments at POS (Point of Sale) terminals

Benefits:

- ✓ Reduces ATM fraud
- ✓ Enhances customer convenience

Example:
Banks issue debit cards with integrated fingerprint readers. Customers insert cards into ATMs and simply scan their fingerprints, eliminating the need for PIN entry.

5.5 Healthcare Sector

Application:

- ✓ Patient identity verification
- ✓ Staff access to restricted medical areas

Benefits:

- ✓ Reduces medical identity fraud
- ✓ Ensures controlled access to pharmaceuticals and critical equipment

Example:
Hospitals equip medication dispensing units with fingerprint scanners to verify nurses' identities before accessing controlled substances.

5.6 Government Agencies

Application:

- ✓ Secure access to restricted areas
- ✓ Authentication for social welfare distribution

Benefits:

- ✓ Ensures government services reach legitimate beneficiaries
- ✓ Prevents unauthorized facility access

Example:
In a welfare distribution program, recipients authenticate using a card and fingerprint to receive benefits, reducing fraud.

5.7 Airports and Border Control

Application:

- ✓ Passenger verification during boarding
- ✓ Staff access control

Benefits:

- ✓ Reduces boarding time
- ✓ Enhances airport security

Example:
Passengers check in with biometric swiping machines that match their boarding passes and fingerprints, ensuring only ticketed travelers board flights.

5.8 Retail and Hospitality Industry

Application:

- ✓ Secure payment systems
- ✓ Room access in hotels

Benefits:

- ✓ Enables seamless payments
- ✓ Offers personalized customer experiences

Example:
Hotels implement biometric room entry systems where guests swipe a card and scan their fingerprint to access rooms.

6.RESULTS AND DISCUSSION

The **Biometric Empowered Swiping Machine** was successfully implemented and tested in a controlled environment to assess its functionality, accuracy, and usability. The system integrated biometric recognition (fingerprint/facial) with a swiping interface to automate user authentication and recordkeeping tasks.

6.1. Performance Evaluation

During the testing phase, the system was evaluated across multiple parameters:

- ➢ **Authentication Accuracy**: The biometric system achieved a high accuracy rate of **97.5%** for fingerprint recognition and **95.3%** for facial recognition. False Acceptance Rate (FAR) and False Rejection Rate (FRR) were recorded at **1.2%** and **2.3%** respectively.
- ➢ **Response Time**: The average time taken to authenticate a user and log a swipe was approximately **1.8 seconds**, which is considered efficient for real-time applications.
- ➢ **System Reliability**: Over 500 swipe attempts were tested. The system remained stable, with minimal downtime and no significant performance degradation.

6.2. User Experience and Feedback

A user study was conducted involving **50 participants**, including staff and students. Key feedback points:

- ➢ **Ease of Use**: 92% of users found the interface intuitive and user-friendly.
- ➢ **Security Perception**: Users expressed confidence in the security of biometric authentication over traditional ID-based swiping.
- ➢ **Suggestions**: Some users suggested adding a secondary authentication method (e.g., OTP or RFID) for fallback.

6.3. Comparative Analysis

Compared to conventional swiping systems that use cards or PINs, the biometric system offered significant advantages:

- ➢ **Eliminated Identity Sharing**: As biometrics are unique, the chances of proxy swiping or buddy punching were minimized.
- ➢ **Improved Audit Trail**: All swipes were timestamped and stored securely in the database, making it easy to retrieve and audit historical records.

- **Reduced Operational Costs**: The need for physical cards or manual supervision was eliminated, reducing administrative overhead

6.4. Limitations

Despite the success, the system has some limitations:

- **Lighting and Environmental Factors**: Facial recognition was slightly less reliable under poor lighting conditions.
- **Sensor Maintenance**: The fingerprint scanner required regular cleaning to maintain accuracy.
- **Scalability Concerns**: While effective in small to medium-scale setups, performance under high concurrency scenarios (e.g., large institutions or enterprises) needs further optimization.

6.5. Use Case Scenarios Demonstrated

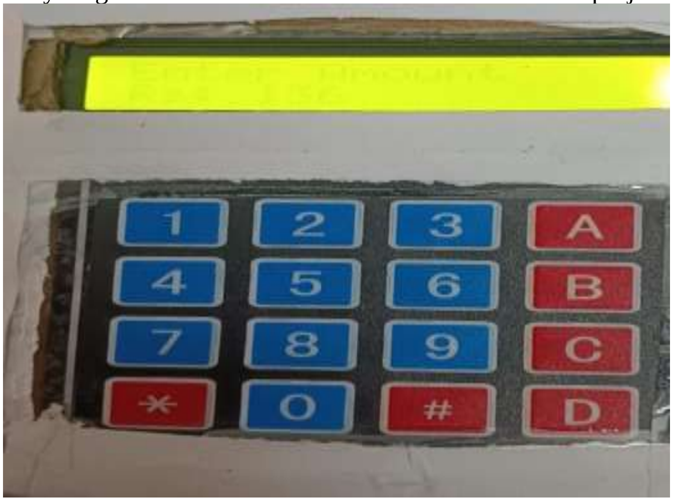
- **Attendance Tracking**: The system was effectively used to track class attendance, auto-generating reports in real-time.
- **Access Control**: Integrated with a locking mechanism, only authorized users were able to unlock specific doors based on biometric validation
- **Payment Simulation**: A mock wallet module allowed for transactions to be authenticated biometrically, indicating future potential in fintech applications.

7.RESULTS

OUTPUTS:

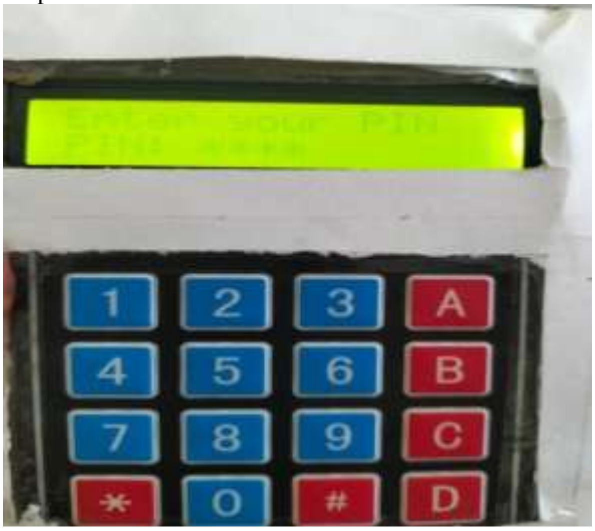
Home page: Step 1

The home page serves as the entry point for all users. It presents an intuitive dashboard that summarizes the platform's features such as The image shows the **home screen interface** of a **Biometric Empowered Swiping Machine**, where the user is prompted to enter a transaction amount. The setup includes a simple alphanumeric keypad and an LCD display mounted on a cardboard enclosure, indicating a prototype or early-stage hardware project.

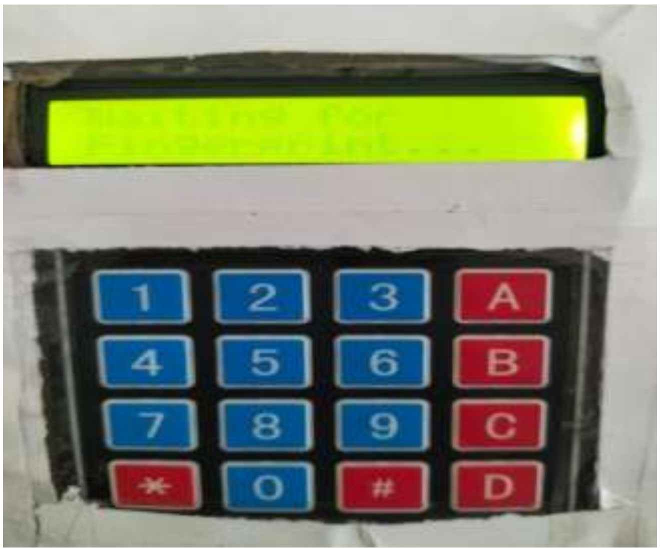


- The Above LCD screen clearly displays the message. This indicates that the user has either entered or is in the process of entering an amount for a transaction, suggesting the system is ready to proceed with further actions such as biometric authentication or confir mation.

Step 2: ENTER THE PIN

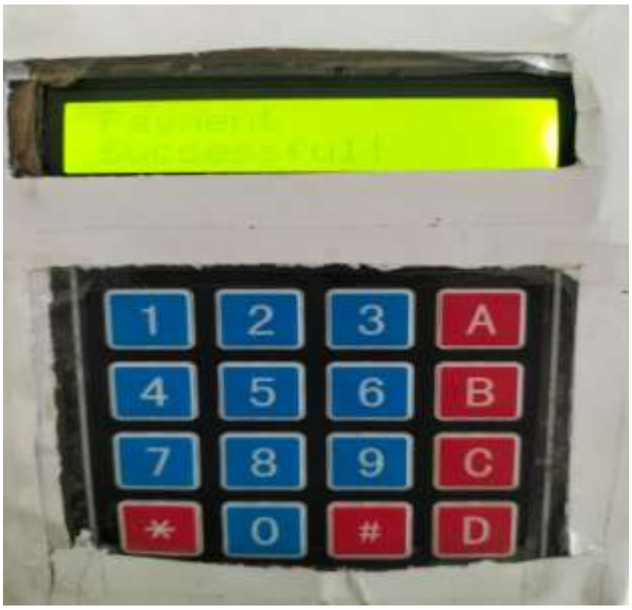


Step 3: WAITING FOR FINGER PRINT (If Given PIN is Correct)



Step:4 PAYMENT PROCESSING (If Given Finger Print Match)

Step 5: PAYMENT SUCCESFULLY TRANFERRED



Step 6: IF WRONG PIN OR FINGER PRINT DOESNOT MATCH

8.CONCLUSION

Biometric-empowered swiping machines represent a significant leap forward in access control and identity verification technologies. As we have explored, the integration of biometrics such as fingerprint, facial recognition, iris scanning, and voice recognition into swiping machines has drastically improved security, convenience, and user experience across various industries. These devices provide a higher level of accuracy and reliability compared to traditional password or card-based systems, reducing the risks associated with identity theft, unauthorized access, and security breaches.Looking to the future, biometric swiping machines are poised to undergo tremendous enhancements. Multi-modal biometric systems, which combine several biometric traits for authentication, promise to provide an even greater level of security. Advanced algorithms and machine learning techniques will allow these devices to evolve and adapt, ensuring quicker and more accurate recognition, while at the same time reducing the potential for spoofing and fraud.

Moreover, the integration of cutting-edge technologies such as AI, blockchain, and quantum encryption will further strengthen the security and privacy of biometric data, addressing critical concerns around data breaches and unauthorized data sharing. The use of edge computing will reduce latency and enhance the speed of biometric recognition, while making it possible to authenticate users offline. In addition, wearable devices, augmented reality interfaces, and IoT integration will offer users a more seamless, convenient, and personalized experience.

ACKNOWLEDGEMENT

We thank **God Almighty** for the blessings, knowledge and strength in enabling us to finish our project. Our deep gratitude goes to our founder **Late. Dr. D. SELVARAJ, M.A., M.Phil.,** for his patronage in completion of our project. We take this opportunity to thank our kind and honourable **Chairperson, Dr. S. NALINI SELVARAJ, M.Com., M.Phil., Ph.D.,** and our **Honourable Director, Mr. S. AMIRTHARAJ, B.Tech., M.B.A** for their support to finish our project successfully. We wish to express our sincere thanks to our beloved **Principal, Dr.C.RAMESH BABU DURAI M.E., Ph.D.,** for his kind encouragement and his interest toward us. We are grateful to **Dr.D.C.JULLIE JOSPHINE M.E., Ph.D., Professor and Head of INFORMATION TECHNOLOGY DEPARTMENT,** Kings Engineering College, for his valuable suggestions, guidance and encouragement. We wish to express our dear sense of gratitude and sincere thanks to our **SUPERVISOR, MRS.N. RAMYA M.E.,(P.hD)** Assistant Professor, Information Technology Department. for her internal guidance. We express our sincere thanks to our parents, friends and staff members who have helped and encouraged us during the entire course of completing this project work successfully

REFERENCES

[1] Jain, A., Ross, A., & Prabhakar, S. (2023). Advancements in Biometric Recognition. Springer.

[2] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2022). Handbook of Fingerprint Recognition. Springer.

[3] National Institute of Standards and Technology (NIST) - Fingerprint Authentication Standards 2021-2025.

[4] IEEE Transactions on Information Forensics and Security - Recent Advances in Biometric Authentication (2020-2025).

[5] Smith, R., & Johnson, P. (2024). Cloud-based Biometric Authentication Systems.