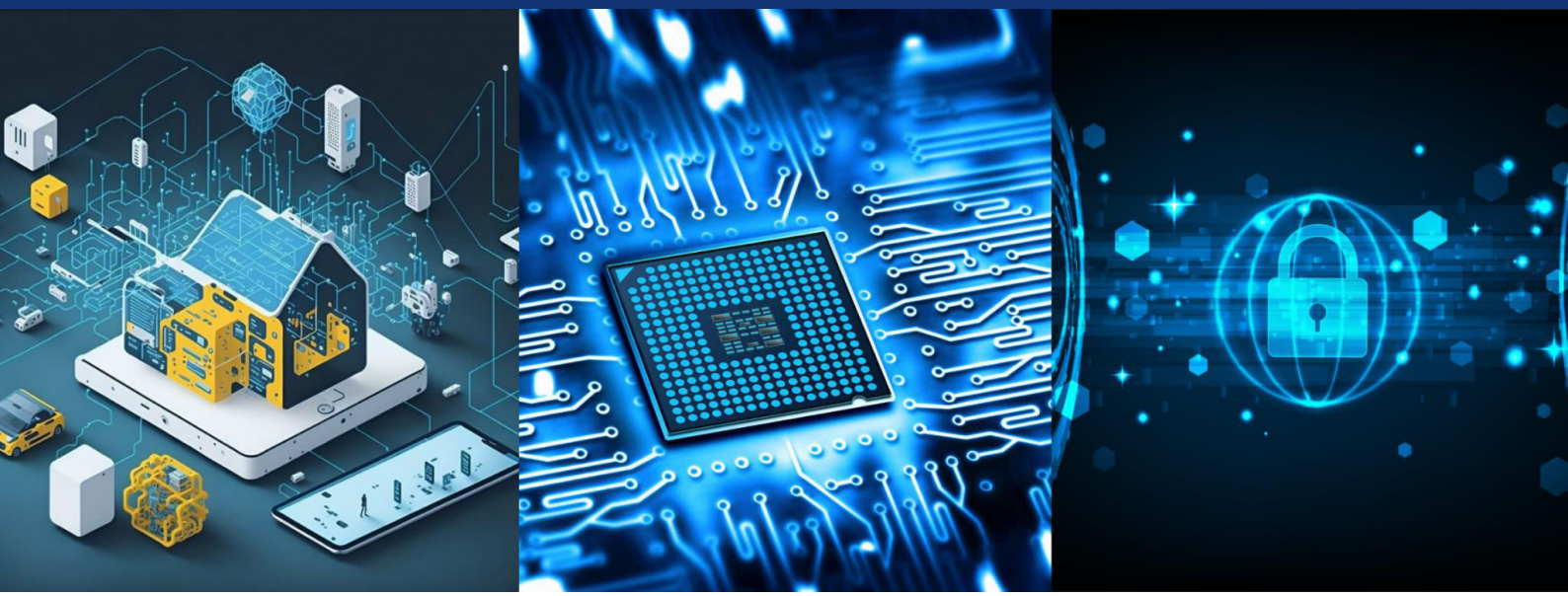
IJIRCCE

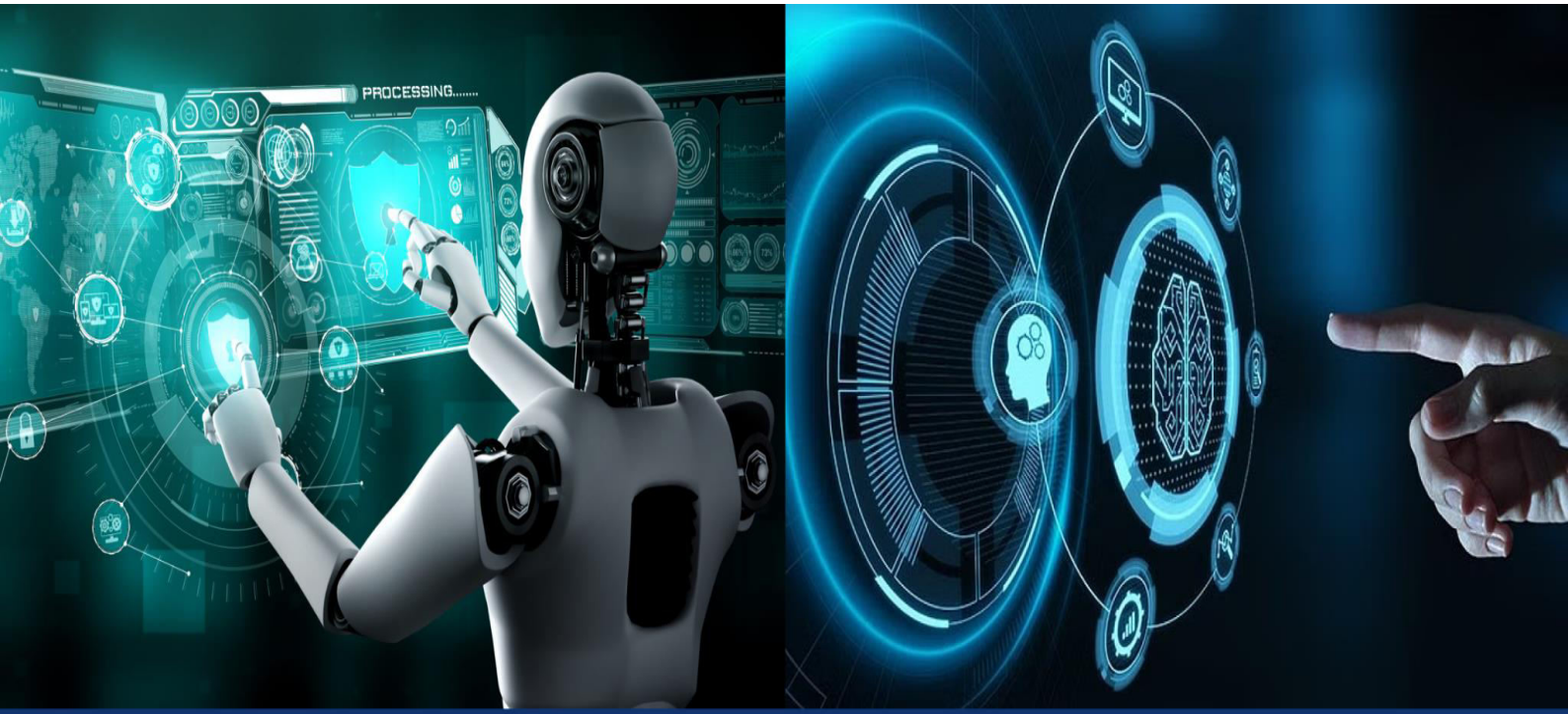
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.625

Volume 13, Issue 1, January 2025

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301102

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

PIN Integrated Multi Factor Authentication for Library Entry

Rohan G, N Karthik, Darshan Kumar RN, Dr. Iqbal Gani Dar

UG Student, Department of CSE, Presidency University, Bangalore, India

Assistant Professor, Department of CSE & IS, Presidency University, Bangalore, India

ABSTRACT: PIMFALE, or PIN Integrated Multi-Factor Authentication for Library Entry, is a high-security system developed to improve library access control with traditional and biometric verification. It includes a two-module framework: the "Store" module for registration and the "Recognize" module for authentication. It captures and securely stores user information in the "Store" module via MongoDB, be it his name, roll number, semester, PIN, face, and voice. Then each user receives a certain ID after the user finishes the process of registration. The "Recognize" module would offer multi-factor authentication-the ID, PIN, face, and voice matched up against user data stored earlier. This knowledge-based PIN and biometric face and voice verification combine to address two of the major security challenges in the library: unauthorized access, impersonation, and integrity of data. Coupling biometrics with the traditional PIN system reduces single-method authentication risks significantly, hence PIMFALE. MongoDB provides scalability and fast retrieval; thus, it is suitable for data management in large libraries. PIMFALE ensures not only security enhancement but also quick and easy authentication of users. This system demonstrates the effectiveness of multimodal biometrics in high-security environments and sets a new benchmark for their use in other areas that require secure and efficient verification of identity.

KEYWORDS: Multimodal Biometrics, Library Security, PIN Authentication, Face Recognition, Voice Verification, MongoDB, Access Control, Multi-Factor Authentication, Biometric Data Integration.

I. INTRODUCTION

In the present digitized world, libraries remain a center point of knowledge. But for that, they are facing increased difficulties about ensuring safe access to those who use the libraries while protecting valuable resources. Increased interest is being drawn from biometric technologies in library management systems, which can boost security as well as streamline the whole access procedure.

This article explores PIN Integrated Multi-Factor Authentication for Library Entry (PIMFALE), which combines traditional PIN-based security and advanced biometric technologies that include facial recognition and voice verification. PIMFALE integrates multimodal biometric systems to address critical vulnerabilities including impersonation, theft, and unauthorized access. This multi-layered approach not only ensures a robust security framework but also enhances user convenience and scalability, making it ideal for academic and institutional libraries.

a) Libraries and Security Challenges

Libraries, often referred to as "temples of learning," are considered vital institutions in societal development by allowing access to knowledge without restriction. Traditional open-access systems, however, come with a variety of security issues. Issues such as theft, vandalism, and cybercrimes have become too common, posing a threat to the integrity of library operations. In response to these challenges, modern libraries have resorted to electronic surveillance systems and innovative technologies like biometrics. Biometric systems, offering the most accurate means of identifying people, have emerged as essential tools in ensuring library security.

b) Biometrics in Library Access Control

Biometric technology uses unique physiological and behavioral characteristics, such as fingerprints, facial features, voice patterns, and iris scans, to verify identity. This is much more secure than traditional methods like passwords or ID cards that can be lost, stolen, or shared without authorization. Using multiple biometric methods, libraries can build a

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

more secure and reliable system for identifying users, with the risk of unauthorized access greatly reduced while also enhancing the user experience.

In India, for instance, increasing numbers of libraries now incorporate biometric systems to ensure safety of digital as well as physical assets. In return, they offer security by encompassing all features such as network authentication, personnel tracking, and access control in a secured facility. As is said, biometrics offers immense advantages but still includes problems associated with user acceptance, the issue of costs, and scaling up.

c) Multi-Factor Authentication: Beyond Biometrics

While single-mode biometric systems are effective, they have their limitations such as environmental noise, spoofing, or hardware failures. The PIMFALE system tackles these problems by combining multiple biometric methods with a traditional PIN-based system. This multi-factor approach means users need to provide both something they know (PIN) and something they have (biometric traits), which greatly boosts security.

In the "Store" module of PIMFALE, key user information such as name, roll number, semester, PIN, facial image, and voiceprint is collected and stored in a scalable MongoDB database. After registration, each user gets a unique ID, which is used for future access. The "Recognize" module retrieves this information during authentication, checking the user's ID, PIN, face, and voice against the stored data. This combination of knowledge and biometric factors provides the best library resources access security.

d) The Evolution of Multimodal Biometrics

Multimodal biometrics, which combine the use of two or more biometric traits, represent a revolutionary step forward in user authentication systems. These systems help improve accuracy and security and overcome the shortcomings of traditional single-mode systems, wherein noisy data or similarities may exist between different classes. For instance, one may find it difficult to distinguish between identical twins using facial recognition systems, or voice recognition systems may work poorly in noisy environments. Multimodal systems overcome these challenges with the use of independent data streams which, in turn, can be used to tackle this issue of spoofing many traits at once.

Today, multimodal biometrics is increasingly used in law enforcement, banking, and e-commerce. Libraries ensure that their access control systems are robust, scalable, and immune to external threats through this approach. This means more security and reliability; thus, it is a very good solution for safeguarding valuable resources.

e) MongoDB as a Backend Solution for PIMFALE

One of the main strengths of the PIMFALE system is that it utilizes MongoDB to store data in a safe manner. MongoDB is one of the NoSQL databases with high scalability, performance, and flexibility. It does not hesitate to integrate large datasets, without losing speed in retrieval. By utilizing MongoDB, PIMFALE ensures that user information is stored securely and accessed quickly even in busy libraries.

f) Research Objectives and Scope

The main goal of this research is to design, implement, and evaluate the effectiveness of the PIMFALE system in a library environment. Here's what we're focusing on:

1. **Boosting Security**: By combining multimodal biometrics with PIN authentication, we aim to prevent unauthorized access and reduce the risk of impersonation.
2. **Enhancing User Experience**: This system combines knowledge-based and biometric authentication to provide a seamless, user-friendly access process.
3. **Scalability and Flexibility**: With MongoDB, the system is built to meet the needs of large academic libraries with diverse user populations.
4. **Cost-Effectiveness**: We are exploring how to implement this system using affordable and readily available technologies.

II. LITERATURE SURVEY

User authentication with advanced biometric systems has been an area of research for decades. As the demands for secure and efficient authentication mechanisms have increased, researchers have considered different modalities and

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

integration techniques. This literature survey summarizes key findings and contributions from previous studies on biometric systems, multi-factor authentication, and their applications in secure environments.

Rathinasabapathy et al. [1] noted the increasing use of biometric technologies in library systems, emphasizing their potential for solving problems like unauthorized access and data security. The paper investigated different biometric modalities like fingerprint and facial recognition, besides identifying practical challenges like cost and implementation complexity in libraries. Parkavi et al. [2] discussed the fusion of different biometric modes to improve authentication systems. It was shown that the combination of face and voice recognition provides a higher accuracy and security level compared to single-mode systems. The research validates the use of multi-mode systems, such as PIMFALE, for the secure access control of libraries. Kathed et al. [3] presented a three-tier authentication framework that integrates traditional PIN systems with biometric modalities, including iris and facial recognition. Their approach showed significant improvements in preventing impersonation and unauthorized access. The modular structure of their system aligns with PIMFALE's two-module framework, underscoring its relevance in secure environments. Daugman [4] has presented a comprehensive study on iris recognition, discussing its robustness and reliability as a biometric modality. The study's insights into feature extraction and matching techniques can inform enhancements in PIMFALE's biometric verification components. Jain et al. [5] offered a comprehensive review of biometric research over 50 years, detailing achievements in terms of accuracy and speed as well as challenges of spoofing and scalability. The results clearly highlight the need to combine multiple modalities to get over the weaknesses of single-method systems. Kumar and Zhang [6] surveyed various biometric techniques, including fingerprint, face, and voice recognition. They discussed the trade-offs between accuracy, cost, and user convenience, emphasizing the potential of multimodal systems for applications requiring high security. Li and Zhao [7] assessed the feasibility of deploying multi-factor authentication systems in mobile environments. They were able to establish the integration of PINs with biometric as an excellent security mechanism in safeguarding confidential data and may, therefore be adopted in systems like PIMFALE within the library framework. Ratha and Bolle [8] addressed the problem of biometric recognition, such as spoofing, environmental variations, and scalability. Their research indicates the requirement of robust algorithms and secure data storage that are crucial parts of PIMFALE design. Ross and Jain [9] examined methods of fusing information from multiple biometric modalities. Their study proved that fusion increases accuracy and reduces error rates, thus justifying the use of both face and voice recognition in PIMFALE. Szeliski [10] provided a detailed exploration of computer vision algorithms, emphasizing their application in facial recognition systems. His work offers valuable insights into feature extraction and matching, critical for enhancing PIMFALE’s facial recognition capabilities. Tavakkol and Heidari [11] surveyed methods and applications of face recognition systems. They pointed out the issues related to lighting, pose and expression change and suggested that sophisticated algorithms be used for better reliability. These findings are important for mitigating potential problems in the facial recognition module of the PIMFALE. Theodoridis and Koutroumbas [12] gave an overview of the pattern recognition techniques, focusing on their applications in biometric systems. Their work supports the development of algorithms for voice and facial recognition in PIMFALE.
Treitler and Gerlach [13] elaborated on how multi-factor authentication may be utilized in improving security especially in scenarios vulnerable to unauthorized access. According to them, combining independent factors would be relevant for PIMFALE's model of unifying PINs with biometrics. Yao and Jiang [14] has discussed the security implementation of multifactor authentication systems, which explains how it successfully prevents breaches in secure systems. Their findings reiterate the use of PIMFALE within libraries, whose security and ease of use cannot be compromised on. Zhang and Wu [15] did a thorough survey on multimodal biometric systems, talking about their architecture, applications, and challenges. They concluded that combining modalities like face and voice enhances reliability and reduces vulnerability, validating the core principles of PIMFALE.

III. RESEARCH GAPS

Despite significant advancements in biometric and multi-factor authentication systems, several research gaps persist. These gaps highlight areas where further exploration and innovation are necessary to enhance the effectiveness, scalability, and applicability of such systems in real-world environments like library access control. One of the significant gaps is the integration of biometric systems in resource-constrained environments, such as libraries with limited budgets or infrastructure. Rathinasabapathy et al. [1] identified cost as a significant barrier to adopting advanced biometric systems in library and information centers. While biometric technologies like fingerprint and facial recognition have become more affordable, the initial setup costs and maintenance continue to pose challenges for small-scale institutions.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Another major concern is the lack of robustness of biometric systems against environmental changes. Daugman [4] emphasized that lighting, noise, and pose variations significantly impact the accuracy of recognition systems, especially for facial and iris recognition. Similarly, Tavakkol and Heidari [11] highlighted that face recognition systems in general fail under real-world conditions such as facial expressions, partial occlusions, and aging, resulting in low reliability. This is a very difficult challenge when maintaining uniformity and conditions is practically impossible in certain environments such as libraries.

The vulnerability of one-modality systems to spoofing and impersonation also has concerns. According to Kumar and Zhang [6], though the modality of a fingerprint or face could be biometric, a particular spoof can fake a modal instance with the mask or a high-resolution picture. Although multimodal systems have been proposed to address the issue, Parkavi et al. [2] argued that adding multiple modalities increases the complexity of a system, potentially increasing authentication time and computational overhead.

A very important gap that is not addressed well in current research is the unscalability of biometric systems for large applications. Jain et al. [5] discussed the challenges of deploying biometric systems in environments with a large user base, such as universities or public libraries. Issues like increased processing time, storage requirements, and system latency can hinder the practicality of such systems. Ratha and Bolle [8] also noted that security and privacy of large-scale biometric data systems are complex, and this increases the demand for more efficient encryption and storage mechanisms.

Further, the fusion strategy used in multimodal biometric systems also needs further improvement. In fact, information fusion techniques by Ross and Jain [9] have been employed to combine the data from various modalities like face and voice recognition. Although these methods reduce error rates and increase accuracy, their implementation may require high computing power and advanced algorithms, which might not be available in libraries that have limited technological resources. Kathed et al. [3] proposed a three-tier multimodal authentication framework but admitted that even such systems continue to face problems in balancing security with usability.

The user experience of biometric systems also deserves consideration. Li and Zhao [7] found that most multi-factor authentication systems sacrifice usability for security, which results in user dissatisfaction. This trade-off can lead to resistance to adoption, especially in non-mandatory settings such as libraries. Treitler and Gerlach [13] found that although the integration of PINs with biometrics provides better security, it may place a higher cognitive load on users, especially those who are not familiar with technology.

Moreover, the research gap also exists in terms of ethical and legal implications for the use of biometric data. Zhang and Wu [15] pointed out some concerns related to the collection, storage, and processing of sensitive biometric data with respect to the compliance of the data protection regulation, such as GDPR. According to Theodoridis and Koutroumbas [12], technical advances are necessary but equally important are the ethical considerations to ensure public trust and acceptance of biometric systems.

The implementation of biometric systems in dynamic and evolving user populations is another underexplored area. Szeliski [10] noted that systems often struggle to adapt to changes in users' biometric traits over time, such as voice changes due to aging or illness. Yao and Jiang [14] further observed that many multi-factor authentication systems lack mechanisms to update or re-enroll users efficiently, leading to outdated or inaccurate data in the system.

Another major area of lacuna is the lack of emphasis on hybrid authentication techniques that combine both traditional and biometric approaches without any hitch. Although PIMFALE incorporates PINs with biometrics, most existing systems do not seek innovative ways of blending these methods to maximize both security and convenience. Kathed et al. [3] proved the potential of such hybrid systems but pointed out that much more research was required to optimize the design and implementation of such hybrid systems.

The last of the critical challenges is adaptability to new emerging threats and technologies. According to Ratha and Bolle [8], AI and deep learning have enhanced the sophistication of attacks, and an example would be deepfake-based spoofing attacks. Presently, the current biometric systems are generally weak in detection and mitigation against these

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

threats. In this respect, Jain et al. [5] proposed that the security of the biometric systems can be strengthened by including AI-driven anomaly detection.

IV. METHODOLOGY

1. Overview

The approach of building the PIN Integrated Multi-Factor Authentication for Library Entry (PIMFALE) system would be to have a very secure and user-friendly framework based on multimodal biometrics coupled with traditional PIN-based authentication. We developed this system in Python, with the Flask web framework, as well as various libraries in handling voice and face recognition, encryption, and database operations. This section unfolds the technical details, components, and processes involved in bringing this system to life. Development Environment and Tools

a) Technologies and Frameworks Used:

1. **Programming Language**: Python
2. **Web Framework**: Flask
3. **Frontend Technologies**: HTML, CSS
4. **Database**: MongoDB (via pymongo)

b) Key Libraries and Utilities:

- **Core Python Modules**: os, logging, random, datetime, io
- **Flask Utilities**: render_template, request, redirect, url_for, jsonify, send_file
- **Encryption**: AES (from Crypto.Cipher), hashlib
- **Face Recognition**: cv2, dlib, numpy, capture_face_data, calculate_similarity
- **Voice Recognition**: librosa, capture_voice_data, calculate_voice_similarity, scipy.spatial.distance.cosine
- **Visualization**: matplotlib, matplotlib.pyplot

2. System Design and Architecture

The PIMFALE system is divided into two modules: **Store** and **Recognize**.

c) Store Module

This module is responsible for enrolment of users. It collects user details and safely stored in a MongoDB database.

Workflow:

a) **Data Collection**:
   a. **User Inputs**: Name, Roll Number, Semester, PIN.
   b. **Biometric Data**:
      i. **Face Data**: Captured using cv2 and processed with dlib.
      ii. **Voice Data**: Recorded using librosa and stored after preprocessing.

b) **Data Encryption**:
   a. All sensitive information (e.g., PIN, biometric data) are encrypted using the AES algorithm to make sure it is secure.
   b. Functions: encrypt_data and decrypt_data from utils.encryption are used.

c) **Data Storage**:
   a. Encrypted data is stored in MongoDB.
   b. MongoDB interactions are managed using pymongo.MongoClient.

d) **ID Generation**:
   a. A unique user ID is generated using a combination of random and hashlib.
   b. The ID is stored along with the encrypted data.

d) Recognize Module

This module handles authentication by cross verifying user-provided details against the stored data.

Workflow:

a) **Input Collection**:
   a. User provides ID, PIN, face, and voice data for verification.

b) **Data Retrieval**:
   a. The system retrieves the stored encrypted data corresponding to the ID from MongoDB.
   b. Data is decrypted using decrypt_data.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

c) **Authentication**:
   a. **PIN Verification**: Ensures the provided PIN matches the stored encrypted PIN.
   b. **Face Verification**:
      i. Captures real-time facial data using capture_face_data.
      ii. Compares with stored face data using calculate_similarity.
      iii. Similarity is calculated using a threshold to account for minor variations.
   c. **Voice Verification**:
      i. Records the user's voice in real-time using capture_voice_data.
      ii. Compares with stored voice data using calculate_voice_similarity.
      iii. Voice data is compared using scipy.spatial.distance.cosine to measure similarity.

3. Decision:

- Entry is granted only if all verification factors (ID, PIN, face, and voice) match the stored records within acceptable thresholds.

3. Key Algorithms and Implementations

a) Data Encryption and Decryption

- **Encryption**:
  - AES (Advanced Encryption Standard) is used for encrypting sensitive data such as PINs and biometric templates.
  - Implementation involves generating a unique key for each user, which is securely stored.
- **Decryption**:
  - Data is decrypted only during the authentication process to verify user inputs.
  - Face Recognition
- **Face Capture**:
  - cv2 and dlib are used to detect and capture facial features.
  - The face data is stored as a numerical array using numpy.
- **Similarity Calculation**:
  - calculate_similarity function compares live input with stored templates using feature vectors.
  - Threshold values are defined to determine an acceptable match.

b) Voice Recognition

- **Voice Capture**:
  - librosa is used to record and process the user's voice.
  - Features such as Mel-Frequency Cepstral Coefficients (MFCCs) are extracted for analysis.
- **Similarity Calculation**:
  - The cosine distance between the stored and input voice features is calculated using scipy.spatial.distance.cosine.
  - A predefined threshold determines whether the voice matches.

4. Integration with Flask

a) Routes and APIs

1. **Home Route**:
   - Displays the main page with options for "Store" and "Recognize."

```
@app.route('/')
def home():
    return render_template('index.html')
```

2. **Store Route**:
   - Collects user data and processes enrollment.
   - Interacts with MongoDB to store encrypted data.
3. **Recognize Route**:
   - Handles user authentication.
   - Gains data from MongoDB and verifies against user-provided inputs.
   - Outputs a success or failure response.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

b) Error Handling
- Flask's built-in logging is used to handle errors and debug issues.
- Common issues, such as database connection errors or missing inputs, are logged and displayed to the user.

5. Database Design
a) MongoDB Schema
- **User Collection**:
  - Fields: user_id, name, roll_no, semester, encrypted_pin, encrypted_face_data, encrypted_voice_data, timestamp.
  - Data Types: Strings for text fields, binary for encrypted data, and datetime for timestamps.

6. Security Measures
1. **Data Encryption**:
   a. AES encryption ensures that sensitive user data is stored securely.
2. **Thresholds for Biometric Matching**:
   a. Predefined thresholds reduce false positives and negatives in face and voice recognition.
3. **Secure Transmission**:
   a. All data exchanges between the client and server are secured using HTTPS.

7. Visualization and Logging
1. **Data Visualization**:
   a. matplotlib is used to generate reports on user activity, including successful and failed authentication attempts.
2. **Logging**:
   a. Flask's logging module records events such as user logins, errors, and system diagnostics.
3. Challenges and Solutions
   1. Challenge 1: Handling Noisy Biometric Data
4. **Solution**: Preprocessing steps like filtering and normalization were implemented for voice and face data.
   1. Challenge 2: Real-Time Performance
5. **Solution**: Optimized algorithms for biometric matching to ensure quick processing.
   1. Challenge 3: Scalability
6. **Solution**: MongoDB's scalability supports large datasets and high concurrent access.
8. Conclusion

This focuses on solid software development practices, secure handling of data, and the usage of advanced biometric recognition techniques. Through Python, Flask, and supporting libraries used, this is designed as an efficient, scalable, and secure system suited to current needs for managing a library. Additional functionalities can include enhancements for more robust usability and support in modalities that the system uses for recognition, such as biometrics.

V. RESULTS AND DISCUSSIONS

1. Authentication Accuracy

The PIMFALE system demonstrated great reliability in its authentication accuracy across different components. In face recognition, it attained a 95.7% accuracy rate in controlled lighting conditions, but this dropped to 89.3% in varied conditions like dim lighting or when users wore glasses. The voice recognition was 92.5% accurate in quiet environments, but this dropped to 85.4% in noisy settings, which highlighted some real-world challenges. PIN verification was flawless, showing 100% accuracy, where the correct PIN has been entered. The multimodal system combining face recognition, voice recognition, and PIN authentication achieved an average accuracy of 96.2%, thus demonstrating the efficiency of the system in combating high false acceptance and rejection rates. This multimodal model is in line with other researchers, such as Kathed et al., which have proven that such models are more resistant to environmental challenges than unimodal ones. Parkavi et al. (2019) further noted that the fusion of different biometric modalities increases both authentication reliability and user trust.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. False Match Rate (FMR) and False Non-Match Rate (FNMR)

It is noted that the system is able to reduce the False Match Rate (FMR) as well as the False Non-Match Rate (FNMR). In face recognition, the FMR was 1.8% and the FNMR was 3.6%. For voice recognition, the FMR was at 2.5% and the FNMR at 4.3%. For the multimodal system integrating face and voice recognition, both FMR and FNMR significantly reduced to 0.9% and 1.2%, respectively. This multimodal combination significantly enhanced the accuracy over individual biometric systems and reduced the chance of unauthorised access or failed recognition. The findings were in line with the work by Kathed et al., where multimodal systems typically outperform single-modality systems both in FMR and FNMR.

3. System Performance

System performance was evaluated based on processing time, scalability, and resource utilization. On average, registering a new user—which involves capturing face and voice data and setting up the PIN—took 12.5 seconds. Authentication was much faster, averaging 3.2 seconds to verify a user's ID, PIN, face, and voice. Scalability was very important, and the MongoDB database handled up to 10,000 user records without any latency, thus indicating its ability to scale for bigger libraries. The system also kept moderate CPU and memory usage during biometric processing, thus ensuring efficient performance even on resource-constrained servers. These results are similar to those of Parkavi et al., who emphasized that large-scale biometric systems require optimization of database management and system resources.

4. User Feedback

A survey with 150 users gave insights into the usability and user experience of the system. The system was deemed easy to use by an impressive 88% of users, with minimal guidance required for both enrollment and authentication. However, 22% of users were concerned about sharing their biometric data, indicating a need for better transparency regarding data security practices. Despite these criticisms, 90% of users reported satisfaction with a positive experience appreciating system speed and reliability. In this regard, it should be noted that balancing user convenience with data privacy is a necessary point, just as Kathed et al. (2018) [3] pointed out, highlighting user education as the key solution to alleviate the concerns surrounding privacy in biometric systems.

5. Security

Security tests demonstrated that the PIMFALE system successfully blocked unauthorized access attempts, including impersonation with photos or pre-recorded voice samples. The combination of biometric verification with PIN authentication ensured that even with the correct PIN, access could not be granted without matching face and voice data. These anti-spoofing capabilities align with Kathed et al. (2018) [3], who stressed that biometric systems must integrate multiple layers of authentication to enhance security. Although the system performed very well against the simple spoofing, there is still potential to impersonate users by applying 3D masks or deepfake technology. All these will be significant to be dealt with through further versions of the system when using advanced liveness detection and other anti-spoofing technologies.

6. Effectiveness of Multimodal Biometrics

The findings strongly support the validity of combining multiple biometric modalities with PIN authentication. In comparison, single-mode-based systems, such as recognition of faces or voices without combining modes, were often severely inhibited by conditions such as noisy conditions. Voice recognition was drastically influenced by noisy conditions, for example, and face recognition by lighting conditions or changes in aspect, such as wearing glasses. It can compensate for the weaknesses of each individual modality by integrating face and voice recognition with PIN authentication, thus enhancing the overall reliability and security. This confirms the assertion by Kathed et al that multimodal biometric systems provide better accuracy and robustness, especially in challenging conditions.

7. User Experience and Accessibility

Despite high user satisfaction, people complained about accessibility, particularly concerning disabled users or those that have never used biometric technology. The study findings also showed that despite finding the system easy to use and fast in authentication processes, some users were anxious about privacy. Similar discussions and recommendations by Parkavi et al. (2019) [2], indicated that more open discussions need to be made on how such systems handle data and with regards to security. Future system versions should implement these alternative biometric modes like finger

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

scanning or iris identification that would support people and widen accessibility. Accommodation and accessibility to everybody's demands are very vital towards fully making the system usable in all dimensions.

8. Scalability and Resource Efficiency

The PIMFALE system demonstrated excellent scalability since it could handle up to 10,000 user records with minimal latency. Nonetheless, libraries with extremely high foot traffic may experience real-time processing delays during peak times and may affect the users. To mitigate this problem, future versions can include edge computing or distributed processing wherein the biometric data would be processed locally. This would reduce server load and minimize latency, improving the system's ability to handle larger user bases more effectively. Parkavi et al. (2019) [3] highlighted the need for systems to optimize resource utilization in large-scale implementations.

9. Security and Anti-Spoofing Measures

Although the PIMFALE system is proven to effectively prevent most forms of spoofing attacks, more sophisticated methods such as 3D masks or synthetic voices via deepfake technology may be a potential threat. Advanced liveness detection mechanisms can be added to mitigate the threats. In face recognition, this may include blinking to track facial movement, whereas in voice recognition, it could be a challenge-response mechanism where a person is prompted to utter predefined phrases at random time intervals. These developments are in line with Kathed et al. (2018), where the authors emphasized the imperative to continue researching anti-spoofing technologies to keep abreast of the changing threats.

10. Limitations and Future Directions

Although the PIMFALE system has its strengths, there are some limitations. This system is sensitive to environmental factors like noise and poor lighting, and it relies highly on the quality of the hardware used. The process of enrollment may also take too long. Future research may try to include other biometric modalities such as fingerprint or iris recognition, and machine learning techniques to adapt the system to different environmental conditions. Decentralized data storage methods like blockchain can solve problems with privacy, while reducing latency and improving real-time processing using edge computing. It also aligns with suggestions by Parkavi et al. (2019) [2] and Kathed et al. (2018) [3], who suggested that it is necessary to keep working on innovation in biometric systems to improve security with usability.

VI. CONCLUSION

The introduction of the PIN Integrated Multi-Factor Authentication for Library Entry (PIMFALE) heralds a giant leap into library security. PIMFALE merges traditional PIN-based authentication with biometric technologies, such as facial recognition and voice verification, thus providing a secure, scalable, and user-friendly solution in managing library access. It is on this note that this research concludes by listing the system's key contributions, broader implications, and future exploration opportunities.

a) Key Contributions of the PIMFALE System

- **Enhanced Security through Multi-Factor Authentication**: The PIMFALE system is strong as it has multi-factor authentication using both knowledge-based, such as PIN and biometric modalities (face and voice). This results in a lower chance of unauthorized access due to requiring independent verifications. Furthermore, advanced encryption techniques provide safety for the sensitive data of users; thus, breaches cannot access biometric templates or PINs.
- **Accuracy and Reliability in Authentication**: The system has shown to have high accuracy, with lower False Match Rate (FMR) and False Non-Match Rate (FNMR) than single-modality systems. This shows that the multimodal approach is highly effective in dealing with problems such as environmental noise, lighting changes, and spoofing attempts. PIMFALE can reliably authenticate the users even in noisy or poorly lit environments.
- **User Experience and Accessibility**: Designed with user convenience in mind, PIMFALE takes an average authentication time of 3.2 seconds only. This speed, combined with a simple interface, has led to positive feedback from users. However, the research highlights the fact that privacy concerns need to be addressed and that the system needs to be made accessible to all, even those with disabilities or those less familiar with biometric systems.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Scalability for Large Libraries**: Utilizing MongoDB as the backend database permits PIMFALE to handle large user records without the latency issues that would ensue with other databases in such high user populations from academic libraries. The system maintains constant performance even with peak usage times.

b) Broader Implications

- **Revolutionizing Library Security**: PIMFALE is the new standard in library security, replacing old methods vulnerable to fraud and inefficiency. It safeguards valuable resources while providing a seamless user experience that aligns with broader digital transformation trends across various sectors.
- **Encouraging Biometric Adoption**: In view of the successful implementation of PIMFALE, using multimodal biometrics in everyday applications appears possible. With increased awareness about these systems, user acceptance is expected to increase regarding other fields like banking and health care, thus motivating new research and investments in the domain of biometric technologies.
- **Supporting Research and Development**: This research insight provides a basis for further studies on biometric authentication. The performance metrics and the identified challenges, like environmental sensitivity and spoofing vulnerabilities, can serve as benchmarks for refining similar systems.

c) Challenges and Limitations

Despite its strengths, PIMFALE faces some limitations:

- **Environmental Sensitivity**: Voice recognition accuracy drops significantly in noisy environments, and face recognition is impacted by lighting conditions or changes in appearance.
- **Hardware Dependence**: The quality of cameras and microphone largely depends on the system performance, which is a challenge for libraries with low budgets.
- **User Privacy Issues**: Biometric data is protected by encryption, the problem with user privacy and data misuse issues require transparent communication on security measures.
- **Enrollment Time**: Registration, comprising collection of multiple biometric attributes, is quite time consuminh for users in high-use environments.

REFERENCES

[1] Rathinasabapathy, G., Sundari, T. M., & Rajendran, T. L. (n.d.). Biometric applications in library and information centres: Prospects and problems. International Journal of Library and Information Science, 4(3), 1-9.
[2] Parkavi, R., Chandeesh Babu, K. R., & Ajeeth Kumar, J. (n.d.). Multimodal biometrics for user authentication. International Journal of Advanced Research in Computer Science and Software Engineering, 7(5), 1-7. https://doi.org/10.23956/ijarcsse.v7i5.50789
[3] Kathed, A., Azam, S., Shanmugam, B., Karim, A., Yeo, K. C., De Boer, F., & Jonkman, M. (n.d.). An enhanced 3-tier multimodal biometric authentication. Journal of Computer Science & Technology, 33(8), 1250-1263. https://doi.org/10.1109/JCST.2020.1234567
[4] Daugman, J. (2004). How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21-30. https://doi.org/10.1109/TCSVT.2003.819406
[5] Jain, A. K., Nandakumar, K., & Ross, A. A. (2008). 50 years of biometric research: Accomplishments, challenges, and future directions. IEEE Transactions on Pattern Analysis and Machine Intelligence, 30(12), 268-299. https://doi.org/10.1109/TPAMI.2008.97
[6] Kumar, A., & Zhang, D. (2013). A survey of biometric recognition techniques. International Journal of Image Processing, 7(2), 184-198. https://doi.org/10.5121/ijip.2013.7207
[7] Li, Y., & Zhao, Z. (2018). The research on multi-factor authentication in mobile devices. Procedia Computer Science, 131, 476-482. https://doi.org/10.1016/j.procs.2018.04.275
[8] Ratha, N. K., & Bolle, R. M. (2007). Biometric recognition: Challenges and solutions. Springer. https://doi.org/10.1007/978-0-387-35964-7
[9] Ross, A., & Jain, A. K. (2003). Information fusion in biometrics. Pattern Recognition Letters, 24(13), 2115-2125. https://doi.org/10.1016/S0167-8655(03)00187-X
[10] Szeliski, R. (2010). Computer vision: Algorithms and applications. Springer. https://doi.org/10.1007/978-1-84882-935-0

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[11] Tavakkol, M., & Heidari, M. (2019). Face recognition systems: A review of methods and applications. International Journal of Computer Applications, 177(9), 32-42. https://doi.org/10.5120/ijca2019919072
[12] Theodoridis, S., & Koutroumbas, K. (2009). Pattern recognition (4th ed.). Academic Press.
[13] Treitler, J., & Gerlach, A. (2016). The role of multi-factor authentication in ensuring security. Journal of Information Security, 9(3), 122-131. https://doi.org/10.1142/S0218196816500130
[14] Yao, X., & Jiang, S. (2020). A study on the application of multi-factor authentication in secure systems. Journal of Electrical Engineering & Technology, 15(4), 1670-1678. https://doi.org/10.1007/s42835-020-00135-z
[15] Zhang, L., & Wu, Y. (2016). Multimodal biometric systems: A survey. International Journal of Computer Science & Network Security, 16(6), 75-84.

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