International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

DECENTRALIZED SECURED LOGIN SYSTEM USING BLOCK-CHAIN TECHNOLOGY

Dr. P Amudha[1], Chithriya V[2], Dakshada S[3], Jeevashree D [4], Nivodharshaa D[5]

[1] Professor and Head, Department of Computer Science and Engineering-School of Engineering, Avinashilingam Institute of Home science and Higher Education for Women, Coimbatore, Tamil Nadu,India.

[2]Department of Computer Science and Engineering-School of Engineering, Avinashilingam Institute of Home science and Higher Education for Women, Coimbatore, Tamil Nadu, India.

[3]Department of Computer Science and Engineering-School of Engineering, Avinashilingam Institute of Home science and Higher Education for Women, Coimbatore, Tamil Nadu, India.

[4]Department of Computer Science and Engineering-School of Engineering, Avinashilingam Institute of Home science and Higher Education for Women, Coimbatore, Tamil Nadu, India.

[5]Department of Computer Science and Engineering-School of Engineering, Avinashilingam Institute of Home science and Higher Education for Women, Coimbatore, Tamil Nadu, India

ABSTRACT

The fast growth of digital platforms and connected systems has made it very hard to authenticate users in a safe and legal way. Using only passwords for login is more likely to lead to identity theft, data breaches, and illegal access. This situation creates a need for stronger and smarter authentication systems.This research proposes a decentralized secured login system designed to improve security and reliability by combining QR-based identification with facial recognition. The goal of this work is to create a system that reduces reliance on single-factor authentication while offering a secure and scalable login mechanism that suits modern digital environments.The proposed system uses an RFID reader connected to an ESP8266 NodeMCU to send tag information to a server application developed in Python and Flask. It validates the received data using SHA-256 hashing within a blockchain-supported structure. It then uses a webcam and a Dlib CNN-based facial recognition model to confirm identity.This layered authentication process makes identity verification secure and efficient. Testing of the system shows it provides reliable authentication performance with a fast response time during real-time verification. The dual-layer approach greatly reduces the chances of unauthorized access because it requires both physical token validation and biometric identity matching for a successful login. The system also keeps secure and transparent authentication records using blockchain-based logging. The results show that using decentralized security methods with biometric verification could make identity management systems better. This method works well for access control in businesses, schools, and IoT-based networks where safe and easy authentication is important.

Keywords: Decentralized Authentication, Multi-Factor Authentication, RFID, Facial Recognition, Blockchain Security, IoT Security, Single Sign-On.

1.INTRODUCTION

1.1 Background of the Study

Secure user identification has become essential in today's digital world, when smart technologies, online platforms, and connected systems are used extensively across several
industries. Many systems in use today still rely on conventional login techniques like passwords and usernames. However, these techniques are inadequate for safeguarding sensitive data since they are more susceptible to risks including phishing, credential breaches, and illegal access.

1.2 Need for Secure Authentication Systems

Traditional authentication methods' dependence on a single verification factor is one of their main drawbacks. System security can be easily exploited when just one factor is compromised. Furthermore, dangers of data manipulation, single points of failure, and decreased transparency are some of the other issues that centralized authentication schemes may bring about. These challenges

DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

make it evident that more robust authentication methods are required, ones that enhance security without sacrificing usability for everyday applications.

1.3 Problem Statement

Most existing authentication systems depend on centralized databases and single-factor verification, which increases the risk of system failure, data breaches, and identity misuse. If login credentials are compromised, attackers can easily gain unauthorized access. Therefore, there is a need for a more reliable authentication model that reduces these risks while maintaining system efficiency.

1.4 Objective of the Project

The objective of this project is to create an authentication system that is safe, effective, and scalable while addressing the drawbacks of conventional login methods. The system seeks to improve access security, reduce identity theft, and offer a reliable authentication framework appropriate for contemporary applications such as educational institutions, organizational systems, and IoT-based environments by combining biometric authentication with decentralized verification.

1.5 Scope of the Work

The proposed system focuses on secure login and identity verification using a combination of hardware and software modules. It is designed to be adaptable for applications such as institutional access control, enterprise systems, and smart environments where reliable authentication is essential. This paper introduces a Decentralized Multifactor Authentication System prototype that combines facial recognition with RFID-based identification in order to get around these restrictions. Combining two distinct verification principles—something the user owns, like an RFID card, and something that is innate to the user, like face identity—is the foundation of the idea. In the suggested solution, a NodeMCU module wirelessly sends scanned RFID data to a server, where it is validated using a decentralized data structure and hashing algorithms. Facial recognition is used as an extra layer to verify identity after this step has been verified.

2. LITERATURE SURVEY

JSON Based Decentralized SSO Security Architecture in E-Commerce **Ye Jun, Li Zhishu, Ma Yanyan** This work presents a JSON-based decentralized Single Sign-On (SSO) model designed for modern e-commerce platforms. The authors developed an architecture capable of integrating both legacy systems and new authentication modules using lightweight JSON structures. Their approach decentralizes login functions to reduce dependency on a central server and improve system reliability. The study demonstrates that decentralized SSO significantly strengthens security and enables cross-platform interoperability. However, the system primarily focuses on token-based verification and does not incorporate biometric or physical authentication methods—highlighting a gap that real-world access systems still face. This limitation creates a motivation for integrating RFID and facial biometrics in decentralized authentication, as done in the present project.

Trusted Location Sharing on Enhanced Privacy-Protection IoT Without Trusted Center **Bin Lian et al**. This paper explores a decentralized and privacy-preserving authentication system for IoT using blockchain accumulators and zero-knowledge proofs. The authors eliminate the need for a centralized trust authority by implementing local verifiable proofs that validate user identity and device legitimacy. Their method safeguards location data and prevents unauthorized access without storing sensitive information centrally. Although the study proves that decentralized authentication can secure IoT ecosystems effectively, it is based on anonymous cryptographic proofs rather than physical or biometric identity. This research supports the idea of decentralized login but lacks multi-factor authentication involving RFID or face recognition.

Login System for OpenID Connect with Verifiable Credentials **Dario Castellano et al**. The authors integrate Self-Sovereign Identity (SSI) with the OpenID Connect protocol to enhance decentralized login experiences. By leveraging verifiable credentials, users gain full control over their digital identities without depending on third-party providers. The system improves privacy, portability, and trust during authentication. While the research contributes significantly to decentralized web-based identity management, it focuses mainly on digital credentials rather than physical security or

DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

biometric verification. As a result, it does not address real-world access control scenarios where physical tokens (RFID) and face biometrics are essential.

A Middleware Architecture for Self-Sovereign Identity Authentication and Authorization **Felix Hoops, Florian Matthes**. This study proposes a middleware architecture that supports SSI authentication using OpenID Connect and a JSON-based policy language. The middleware helps organizations adopt decentralized identity solutions without overhauling existing systems. It simplifies authorization, enhances privacy, and ensures user-centric identity control. Despite its strong architectural approach, the system focuses solely on digital authentication workflows and lacks multi-factor or physical authentication modules. This gap reveals the need for systems that combine SSI frameworks with on-device verification methods like RFID and biometrics.

Securing the Confidential Data Using Blockchain and DT Framework **Janani S.R. et al**. This paper introduces a blockchain-supported password manager that secures user credentials using SHA-256 encryption and decentralized storage. By eliminating reliance on a centralized database, the system enhances resistance to tampering and credential theft. The authors highlight blockchain's potential in building secure login systems and protecting sensitive data. However, the model only addresses password security and does not include additional verification layers such as biometrics or RFID, which limits its use in physical authentication contexts.

Decentralized Dynamic Identity Authentication System Based on Blockchain. **Jintao Zhu et al**. This work proposes a decentralized authentication protocol using public-key cryptography and dynamically generated nonces to prevent replay attacks. By distributing identity records across blockchain nodes, the system ensures transparency and tamper resistance. Although effective for digital identity verification, the system does not incorporate physical tokens or biometric data, making it insufficient for environments requiring high-security multi-factor authentication. The research nevertheless forms a theoretical basis for decentralized login mechanisms adopted in this project.

PEBIID: Privacy-Preserving and Efficient Biometric Identification for IoV **Dapp Chun Liu et al**. The authors introduce a privacy-preserving biometric identification method for Internet-of-Vehicles decentralized applications. Using invertible matrix-based biometric protection, the framework ensures secure biometric storage and matching on blockchain networks. This demonstrates how decentralized systems can safely incorporate biometric data without exposing sensitive information. However, the study is limited to vehicular networks and does not integrate RFID or multi-factor physical authentication, which is necessary for secure access control systems like the one developed in this project.

EPLRA: Encryption-Based Proactive Load Rebalancing Algorithm **Nithya Kuriakose, Shinu Acca Mani**.This paper presents an encryption-focused load balancing algorithm tailored for cloud environments. The authors show how proactive encryption strategies can improve resource allocation and protect data during distributed computing operations. Even though this research is not directly related to multi-factor authentication, it highlights the importance of strong cryptographic methods in distributed systems. The findings indirectly support the need for secure data handling in decentralized login systems, including the SHA-256 hashing used in this project.

3.METHODOLOGY

3.1 Overview of the Proposed System

The proposed Decentralized Multi-Factor Authentication System is designed to provide a secure and scalable identity verification framework by integrating RFID-based authentication with facial recognition and decentralized validation mechanisms. Unlike traditional authentication systems that rely only on passwords or single-factor verification, the proposed system implements a dual-layer security approach. It combines possession-based authentication using RFID cards with biometric-based authentication using facial recognition. Additionally, SHA-256 hashing and blockchain-style logging mechanisms are integrated to ensure data integrity, transparency, and tamper resistance. This approach significantly enhances security while maintaining real-time

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

performance.

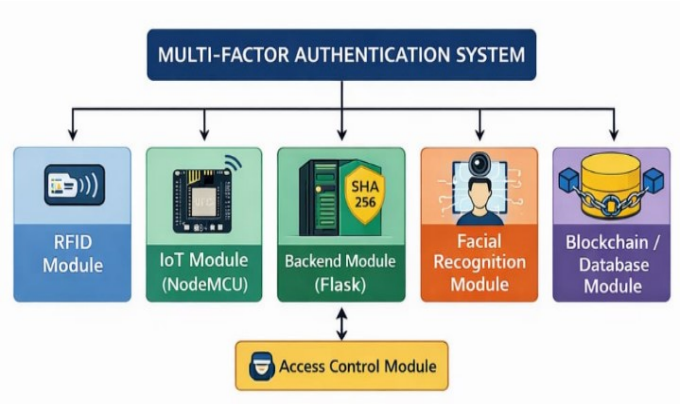


FIGURE 3.1. Overview of the System

3.2 Architecture

The architecture of the proposed system integrates hardware devices, IoT communication modules, backend processing, and decentralized storage into a unified structure. The RFID reader captures the user's card information and forwards it to the ESP8266 NodeMCU. The NodeMCU transmits the RFID data wirelessly to the backend server using Wi-Fi. The backend system, developed using the Flask, processes the received data by applying SHA-256 hashing and verifying it against blockchain-linked records. Once RFID validation is successful, the facial recognition module is activated to complete the second level of authentication. This layered architectural model ensures secure and reliable identity verification.

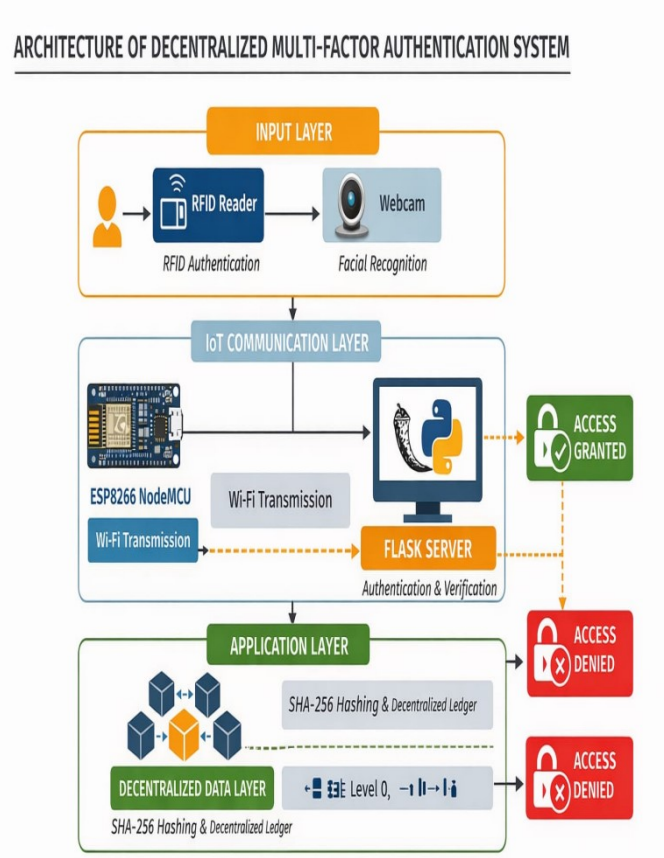


FIGURE 3.2. Architecture of Decentralized Multi-factor Authentication System

3.3 Workflow

The workflow of the system follows a sequential authentication process. Initially, the user

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

scans the RFID card using the RFID reader. The reader captures the unique tag ID and sends it to the NodeMCU. The NodeMCU transmits the tag data to the backend server. The server converts the RFID ID into a SHA-256 hash and validates it using decentralized blockchain-style storage. If the RFID verification is successful, the webcam captures the user's facial image. A CNN-based facial recognition model extracts facial features and compares them with registered data. If both authentication factors match, access is granted; otherwise, access is denied. Each authentication attempt is recorded securely in the decentralized log for auditing and monitoring.

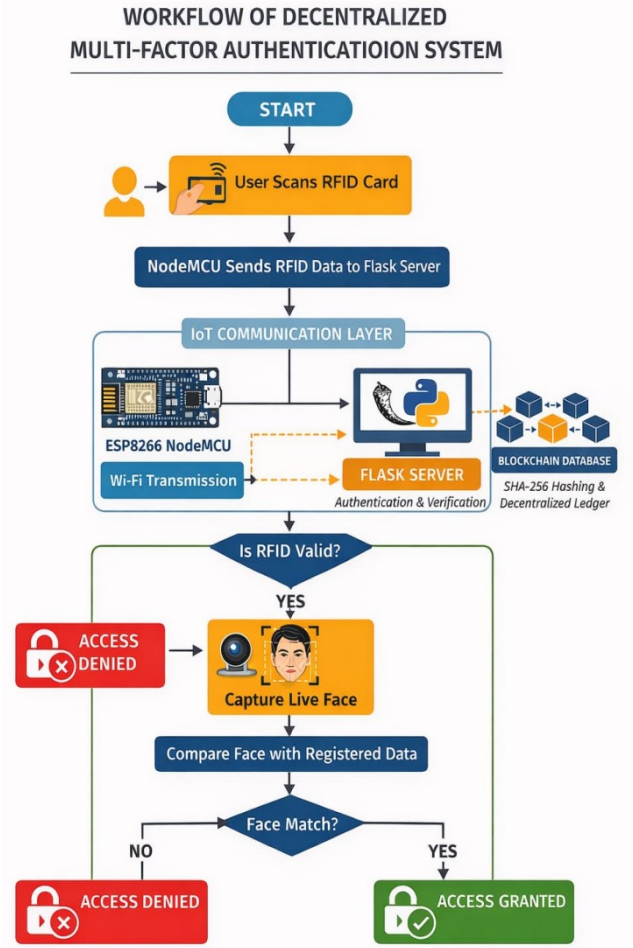


FIGURE 3.3. Workflow of Decentralized Multi-factor Authentication System

3.4 Design Approach

The design approach focuses on enhancing authentication security through multi-layer verification and decentralized data management. The first authentication layer verifies possession of the RFID card, while the second layer verifies the user's identity through biometric facial recognition. The system avoids storing sensitive data in plain text by applying SHA-256 hashing to all credentials. Blockchain-style logging ensures that authentication records are immutable and cannot be altered without detection. The modular design of the system allows scalability and easy integration of additional biometric technologies in the future. This approach ensures strong security without compromising usability or performance.

3.5 System Requirement

The system requires both hardware and software components for successful implementation. The hardware requirements include an RFID reader, RFID tags, a webcam for facial capture, the ESP8266 NodeMCU, and a computer or server system. The software requirements include Python programming language, the Flask, OpenCV library, Dlib library for facial recognition, SHA-256 cryptographic libraries, and a web browser for accessing the interface. These components collectively ensure smooth system operation.

3.6 Security Mechanisms

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

The proposed system incorporates multiple security mechanisms to ensure robust protection. Dual-factor authentication prevents unauthorized access even if one factor is compromised. SHA-256 hashing protects sensitive credential data by converting it into irreversible hash values. Blockchain-style decentralized logging ensures transparency and prevents tampering of authentication records. Real-time monitoring and secure logging further strengthen the system's resistance against replay attacks and impersonation attempts.

3.7 Performance Evaluation

The system performance is evaluated based on authentication accuracy, response time, False Acceptance Rate (FAR), and False Rejection Rate (FRR). Testing results indicate that the dual-layer authentication process achieves high accuracy and fast response time, making it suitable for real-time access control environments such as campuses, offices, and secure facilities.

4.SYSTEM ARCHITECTURE

4.1 Block Diagram

The block diagram of the proposed system illustrates the interaction between hardware and software components. The authentication process begins with the user scanning the RFID card using the RFID reader. The RFID data is transmitted to the NodeMCU, which forwards it to the backend server. The server performs SHA-256 hashing and validates the credentials using blockchain-linked storage. Upon successful RFID verification, the facial recognition module captures and verifies the user's face. Finally, the system generates an access decision (Granted or Denied). The block diagram clearly represents the flow from input acquisition to final authentication decision within a decentralized framework.

4.2 Modules

The system is divided into several functional modules that work together to ensure secure authentication. The RFID Module captures the unique tag ID from the user's card. The IoT Communication Module, implemented using the ESP8266 NodeMCU, handles wireless transmission of RFID data. The Backend Verification Module, developed using the Flask, processes authentication requests and performs hashing validation. The Facial Recognition Module captures live images and compares facial features with stored data. The Decentralized Logging Module stores authentication records securely in blockchain-linked format. Finally, the Access Control Module generates the final decision and controls system entry permissions.

4.3 Data Flow

The data flow begins when the RFID card is scanned. The RFID reader sends the tag ID to the NodeMCU. The NodeMCU transmits the data to the backend server over Wi-Fi. The server hashes the RFID ID using SHA-256 and verifies it against blockchain records. If validated, the system activates facial recognition. The webcam captures the user's face and compares it with stored biometric data. If both authentication factors match, access is granted; otherwise, access is denied. The authentication attempt is then securely logged in the decentralized system.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

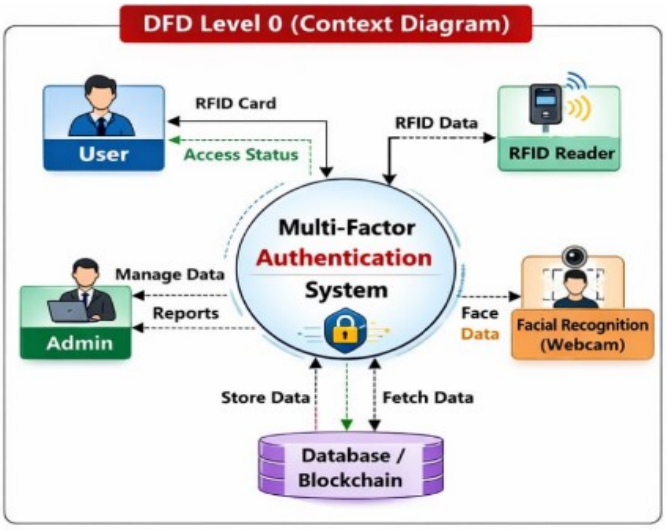


FIGURE 4.1. Data Flow Diagram - Level 0

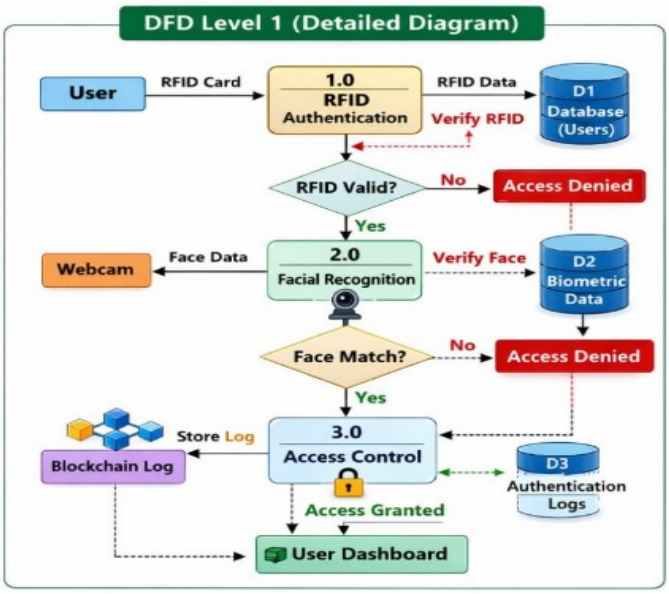


FIGURE 4.1. Data Flow Diagram - Level 1

4.4 Layered Architectural Model

The system architecture is organized into four layers: the Input Layer (RFID and Webcam), the IoT Communication Layer (NodeMCU), the Application Layer (Flask Backend), and the Decentralized Data Layer (Blockchain Logging). Each layer performs specific functions to ensure efficient, secure, and reliable authentication. This layered design improves maintainability and scalability.

4.5 Scalability and Future Enhancements

The modular architecture allows future integration of additional biometric modules such as fingerprint or iris recognition. It also supports expansion to cloud-based blockchain systems and multi-node distributed authentication networks. This flexibility ensures that the system can evolve with technological advancements and increasing security requirements.

5.IMPLEMENTATION

5.1 Introduction

System design defines the architecture, data flow, communication layers, and integration logic required to implement the decentralized multi-factor authentication framework. This chapter

DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

explains the design methodology, system architecture diagrams, workflow processes, database design, and implementation details for the Phase-1 modules: RFID Reader Interface, NodeMCU Gateway, Enrollment Registry, and Face Capture Module.

5.2 System Architecture Setup

The implementation of the proposed decentralized multifactor authentication system was carried out by integrating both hardware and software components into a working prototype. The system architecture was designed in a way that allows smooth communication between the RFID reader, NodeMCU module, backend server, and facial recognition module. Each component plays a specific role in the authentication process, ensuring that the entire workflow remains secure and efficient.

During the implementation phase, the RFID reader was connected to the NodeMCU (ESP8266), which acts as a wireless gateway. When a user scans an RFID tag, the device reads the unique identifier and sends it to the server through a Wi-Fi connection. This step forms the first level of authentication and helps verify whether the RFID card is registered in the system database.

5.3 Backend Server and Database Integration

The backend of the system was developed using a Flask-based web application that manages user authentication, data processing, and communication with the hardware module. A structured database was created to store user identity records, including RFID tag IDs and facial data references.

To enhance security, sensitive identity information was protected using SHA-256 hashing techniques. Instead of storing raw identity details directly, the system stores hashed values, which makes the data more secure and resistant to tampering. This design decision was important for supporting the decentralized approach proposed in the system.

5.4 RFID Authentication Process

The first stage of authentication begins when a user scans their RFID card near the reader. The RFID reader detects the tag and sends the data to the NodeMCU module. The NodeMCU then forwards this information to the server through an API request.

Once the server receives the RFID data, it checks whether the tag exists in the registered identity database. If the RFID information matches the stored records, the system proceeds to the next step of authentication. This stage ensures that only recognized users are allowed to continue in the authentication process.

5.5 Facial Recognition Verification

After successful RFID verification, the system activates the facial recognition module for the second level of authentication. A webcam connected to the system captures the user's facial image in real time. The captured image is processed using a facial recognition library based on deep learning models.

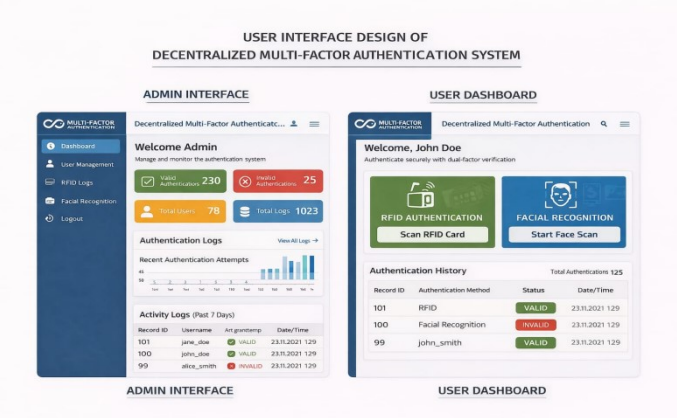
The system compares the captured face with the stored facial data linked to the scanned RFID tag. If the facial features match with sufficient accuracy, the user is verified successfully. This step significantly improves the security of the system because it prevents unauthorized access even if an RFID card is lost or misused.

5.6 Web Interface and User Interaction

A user-friendly web interface was developed to manage enrollment, authentication, and monitoring processes. Through the web interface, administrators can register new users, link RFID tags with facial data, and monitor authentication attempts in real time.

The interface also provides feedback to users during the authentication process. For example, it indicates whether the RFID scan was successful, whether facial verification is in progress, and whether access has been granted or denied. This makes the system easier to use while maintaining strong security controls.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621



5.7 System Workflow and Integration Testing

After implementing all the modules, the system was tested as a complete integrated solution. Several test cases were conducted, including successful authentication, invalid RFID attempts, and facial mismatch scenarios. These tests helped ensure that the system performs reliably under different conditions.

The implementation results confirmed that the system can perform real-time authentication with minimal delay. The coordination between the hardware components and the software modules worked effectively, demonstrating that the prototype is capable of supporting secure authentication in practical environments such as campuses, offices, and smart facilities.

6.RESULTS AND DISCUSSION

6.1 Introduction

System design defines the architecture, data flow, communication layers, and integration logic required to implement the decentralized multi-factor authentication framework. This chapter explains the design methodology, system architecture diagrams, workflow processes, database design, and implementation details for the Phase-1 modules: RFID Reader Interface, NodeMCU Gateway, Enrollment Registry, and Face Capture Module.

6.2 System Implementation Results

The developed prototype of the decentralized multifactor authentication system was successfully implemented by integrating RFID technology, a NodeMCU wireless gateway, and facial recognition. During testing, the RFID reader was able to detect and read the tag information reliably, and the NodeMCU module transmitted this data to the server through a wireless network. The backend system processed the received data and verified it against the stored identity records secured using SHA-256 hashing. Once the RFID authentication was validated, the system triggered the facial recognition process through a webcam interface. The integration of both authentication stages worked smoothly, demonstrating the feasibility of combining hardware-based access with software-driven identity verification in a real-time environment.

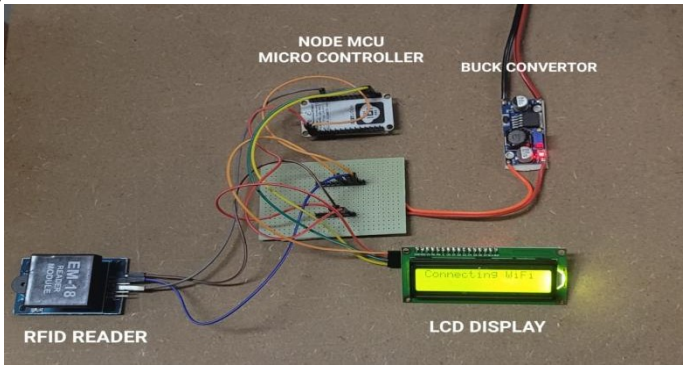


FIGURE 6.3. Process of the dataset [3]

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

6.3 Performance of the Dual Authentication Process

The results showed that using two authentication factors significantly improved system reliability and security. In most test cases, RFID tag detection and facial verification were completed within a short time frame, allowing users to gain access without noticeable delay. The system also showed better protection compared to single-factor authentication methods because access was granted only when both the RFID identity and facial features matched the stored records. This dual-verification process helped reduce the chances of unauthorized entry, especially in situations where a card alone could have been misused.

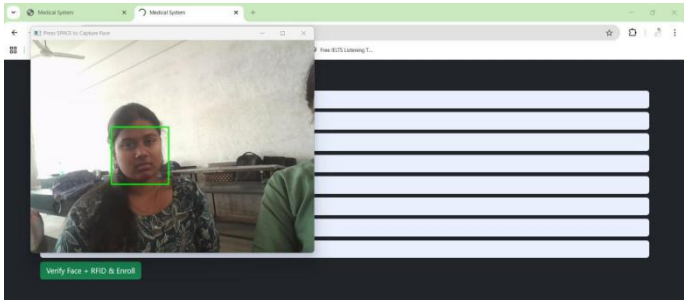


FIGURE 6.2. Process of the dataset [3]

6.4 Security and Data Integrity Evaluation

Another important result observed during the implementation was the improved protection of stored identity data. By using SHA-256 hashing and a decentralized-ready architecture, the system ensured that sensitive information such as identity records and authentication logs could not be easily altered or manipulated. Each authentication attempt was recorded with a timestamp and status, allowing the system to maintain a transparent and traceable verification process. This feature plays a significant role in environments where monitoring and auditability are important.

6.5 Practical Observations During System Testing

While testing the prototype in a real environment, several practical observations were made. The contactless nature of both RFID scanning and facial recognition made the system convenient and hygienic to use. Users only needed to scan their RFID card and face the camera for a few seconds to complete authentication. However, lighting conditions and camera positioning slightly affected facial recognition performance in some cases, indicating that environmental factors should be considered when deploying the system on a larger scale. Despite these minor challenges, the overall system performance remained stable and effective.

6.6 Discussion on System Effectiveness

The results of this study indicate that integrating hardware-based identification with biometric verification can significantly strengthen access control systems. Compared to traditional login methods that rely only on passwords or single authentication factors, the proposed approach provides an additional layer of security. The use of a wireless gateway such as NodeMCU also makes the system suitable for IoT-based environments where devices need to communicate efficiently with central servers. From an implementation perspective, the system demonstrates how decentralized authentication methods can improve reliability while reducing risks associated with centralized databases.

7.ADVANTAGES

7.1. Robust Multifactor Authentication

One of the main strengths of the proposed system is its use of two independent authentication factors: RFID-based identification and facial recognition. By combining a physical credential with a biometric trait, the system provides a significantly stronger level of protection than traditional single-factor methods. Even if one authentication factor is compromised, the second layer continues to safeguard access. This layered verification approach greatly reduces the chances of unauthorized entry and improves overall system reliability in real-world deployments.

7.2. Prevention of Card Misuse

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

Conventional RFID systems rely solely on possession of a card, which makes them vulnerable if a card is lost, duplicated, or stolen. The proposed system addresses this weakness by linking each RFID credential with a registered facial identity. As a result, possession of the card alone is insufficient for access. This dual verification mechanism ensures that only the legitimate user can authenticate successfully, thereby preventing misuse and strengthening identity assurance.

7.3. Contactless and Hygienic Operation

Both authentication stages operate without physical contact, which improves usability and hygiene. RFID scanning does not require touching a device, and facial recognition works through camera-based detection. This feature is particularly beneficial in environments where minimizing physical interaction is important, such as public facilities, workplaces, or healthcare settings. The contactless nature of the system also contributes to faster processing and a smoother user experience.

7.4. Tamper-Resistant Data Storage

The system enhances data security by storing identity records using SHA-256 hashing. Since hashed data cannot be easily reversed or altered, sensitive information remains protected even if unauthorized access to the database is attempted. This approach helps maintain the integrity of authentication records and ensures that stored credentials remain reliable over time.

7.5. Support for Decentralized Architecture

Unlike traditional centralized authentication systems, which rely on a single server, the proposed architecture incorporates decentralized validation concepts. Distributing verification processes reduces dependence on one point of control and minimizes the risk of system failure due to server outages or targeted attacks. This design choice improves resilience, availability, and trustworthiness in large-scale implementations.

7.6. Real-Time Audit and Monitoring

The system maintains detailed logs of authentication attempts, including timestamps and verification status. These records allow administrators to monitor system activity, detect suspicious behavior, and analyze usage patterns. Real-time auditing enhances transparency and provides an additional security layer by enabling quick responses to potential threats or anomalies.

7.7. Scalability and Future Expansion

The architecture has been designed with scalability in mind, allowing it to integrate emerging technologies such as additional biometric modalities, blockchain-based validation, or cloud-based services. This flexibility ensures that the system can evolve alongside technological advancements without requiring major structural changes. As organizational requirements grow, the system can be extended to accommodate larger user bases and more complex security policies.

7.8. User-Friendly Operation

Despite incorporating advanced security mechanisms, the system remains simple for end users. Authentication requires only a quick card scan followed by facial verification, both of which occur within seconds. This balance between strong security and ease of use is essential for practical adoption, as users are more likely to accept systems that do not complicate their daily routines.

8. APPLICATIONS

8.1. Smart Campus Entry Systems

The proposed system can be effectively implemented in smart campus environments where secure and efficient access control is essential. Educational institutions often manage thousands of students, staff, and visitors daily, making manual monitoring impractical. By combining RFID-based identification with facial verification, the system enables automated entry that is both quick and reliable. This not only strengthens campus security but also simplifies attendance tracking, reduces impersonation risks, and ensures that only authorized individuals can access restricted academic or administrative areas.

8.2. Secure Office and Industrial Access Control

In corporate offices and industrial facilities, controlling entry to workspaces, production units, and confidential departments is critical. The dual-authentication approach enhances protection by

DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

ensuring that access is granted only when both identity factors are validated. Even if an RFID card is lost or duplicated, facial verification prevents misuse. This makes the system suitable for organizations handling sensitive data, proprietary technology, or expensive equipment where traditional access cards alone may not provide adequate security.

8.3 Laboratory and Research Facility Security

Research laboratories often store sensitive experimental data, specialized instruments, or hazardous materials that require strict monitoring. The proposed authentication framework provides an additional layer of assurance by validating both possession-based and biometric credentials before access is allowed. This helps institutions maintain compliance with safety regulations, protect intellectual property, and monitor usage logs for accountability. The automated verification process also reduces administrative burden while maintaining strict entry control.

8.4 IoT-Based Smart Buildings

Modern smart buildings rely on interconnected devices and automated systems to manage lighting, climate control, surveillance, and access. Integrating the proposed authentication mechanism into such infrastructures enhances overall system security by ensuring that only verified individuals can interact with building controls. Because the architecture supports wireless communication and decentralized validation, it aligns well with IoT environments where reliability, scalability, and remote monitoring are essential.

8.5 Data Centers and Enterprise Login Systems

Data centers require strict authentication procedures to prevent unauthorized access to critical servers and digital infrastructure. The proposed system can function as a unified login mechanism that bridges physical and digital authentication. Personnel must first verify their identity physically through RFID and facial recognition before being granted system-level privileges. This layered approach significantly reduces the chances of credential theft or insider misuse, making it suitable for enterprises that prioritize cybersecurity and compliance standards.

8.6 Government and Defense Restricted Areas

High-security sectors such as government offices and defense facilities demand authentication systems that are resilient against tampering and identity fraud. The decentralized validation model, combined with hashed identity storage, strengthens trust and data integrity. Since authentication records cannot be easily altered, administrators gain a reliable audit trail of access attempts. Such features make the system appropriate for sensitive environments where transparency, traceability, and strict identity verification are mandatory.

8.7 Hostel and Residential Security Systems

Residential complexes and student hostels can benefit from automated entry monitoring without requiring manual supervision. The contactless nature of RFID and facial recognition allows residents to enter conveniently while maintaining a secure environment. The system can also log entry and exit times, helping administrators monitor visitor activity and ensure resident safety. This approach improves both security and user experience by eliminating the need for keys or manual registers.

8.8 Smart Attendance Management Systems

The technology can also be adapted for automated attendance tracking in classrooms, workplaces, or training centers. Instead of relying on manual roll calls or card-only systems that can be misused, the dual-verification method confirms the physical presence of the correct individual. This ensures accurate attendance records, reduces administrative workload, and prevents proxy attendance. Over time, such automation can improve operational efficiency while maintaining fairness and authenticity in record keeping.

9. CONCLUSION

The proposed decentralized multi-factor authentication system demonstrates how combining RFID-based identification with AI-driven facial recognition can create a more intelligent and reliable method of identity verification. Unlike traditional single-factor approaches, the system

DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

requires both a physical credential and a biometric match before access is granted, thereby significantly strengthening security and reducing the chances of unauthorized entry.

The integration of SHA-256 hashing within the decentralized-ready architecture further enhances trustworthiness by protecting stored identity records from tampering and minimizing risks typically associated with centralized databases. This ensures that sensitive authentication data remains consistent, verifiable, and resistant to manipulation.

In addition, the coordinated operation of the RFID reader, NodeMCU gateway, backend verification engine, and facial recognition module enables real-time, contactless authentication with high accuracy. This seamless interaction between hardware and software components highlights the practicality of the system for real-world deployment.

Overall, the implementation confirms that the proposed model provides a secure and scalable foundation for future identity-centric applications. It can be readily adapted for smart campus environments, IoT infrastructures, and enterprise-level access control systems, offering a dependable pathway toward next-generation authentication solutions.

10.FUTURE SCOPE

While our project implements the core authentication modules, several enhancements can be added in future phases to improve scalability, security, and decentralization:

10.1. Blockchain-Based Verification

Integrating a permissioned blockchain (Hyperledger/Ethereum) will allow:

- Immutable storage of authentication records
- Tamper-proof identity mapping

Decentralized trust without relying on central servers

10.2. Full Web5 DID Integration

Implementing Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) will:

- Provide user-controlled identity
- Enable cross-platform login without passwords
- Improve privacy and data ownership

10.3. Additional Biometric Factors

The system can be extended to include:

- Fingerprint verification
- Iris or voice recognition
- Multi-biometric fusion for higher accuracy

10.4. Edge Computing & Offline Authentication

Performing recognition on edge devices (ESP32-CAM, AI microcontrollers) will:

- Reduce server dependency
- Enable authentication even without internet
- Improve response time and reliability

10.5. Advanced Anti-Spoofing Techniques

Using deep-learning models for:

- 3D face detection
- Motion analysis
- Spoof-prevention using texture and depth cues

10.6. Scalability for IoT and Enterprise Use

Future versions can integrate with:

- Smart door systems
- Industrial access control
- Cloud dashboards for monitoring

10.7. Real-Time Monitoring & Analytics

Adding dashboards for:

- Live authentication status

DOI:10.46647/ijetms.2026.v10i03.033 ISSN: 2581-4621

- Anomaly detection
- Usage patterns and security alerts

REFERENCES

[1]. Ye Jun, Li Zhishu, Ma Yanyan, "JSON Based Decentralized SSO Security Architecture in E-Commerce," *International Journal of Computer Applications*, 2019.
[2]. Bin Lian, et al., "Trusted Location Sharing on Enhanced Privacy-Protection IoT Without Trusted Center," *IEEE Transactions on Industrial Informatics*, 2020.
[3]. Dario Castellano, et al., "Login System for OpenID Connect with Verifiable Credentials," *ACM Digital Library*, 2021.
[4]. Felix Hoops, Florian Matthes, "A Middleware Architecture for Self-Sovereign Identity Authentication and Authorization," *IEEE Access*, 2020.
[5]. Janani S. R., et al., "Securing the Confidential Data Using Blockchain and DT Framework," *International Journal of Engineering Research*, 2020.
[6]. Jintao Zhu, et al., "Decentralized Dynamic Identity Authentication System Based on Blockchain," *IEEE Access*, 2019.
[7]. Chun Liu, et al., "PEBIID: Privacy-Preserving and Efficient Biometric Identification for IoV DApp," *IEEE Internet of Vehicles Journal*, 2021.
[8]. Nithya Kuriakose, Shinu Acca Mani, "EPLRA: Encryption-Based Proactive Load Rebalancing Algorithm," *International Journal of Cloud Computing*, 2018.
[9]. ESP8266 NodeMCU, **"Technical Reference & Wi-Fi Programming Guide,"** Espressif Systems, https://www.espressif.com/
[10]. Flask Framework, **"Flask Web Application Development Documentation,"** https://flask.palletsprojects.com/