International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 4, pp 234-241, April-2026

https://doi.org/10.47001/IRJIET/2026.104034

A Privacy Preserving Multi Factor Identity Framework for Smart Campuses Using Biometrics and Blockchain

[1]Aditi Bhadake, [2]Snehal Khode, [3]Nikita Uphade

[1,2,3]PG Student , Department of MSc (CS-II), HAL College of Science and Commerce ,Ozar, Affiliated to SPPU, Maharashtra, India

***Abstract* - The rapid emergence of digitization in higher education institutes highlights the inefficiencies and weaknesses of legacy identification methods, such as manual register systems. These are both time-consuming and susceptible to fraud in the form of proxy attendance ("buddy punching"). The USSCS framework proposed in this paper presents a privacy-first model for integrating campus services, namely attendance, access, and cashless payment mechanisms into one digital identity system.**

The USSCS framework utilizes an ESP32-S3-based hub, 13.56 MHz RFID, and fingerprint biometric methods for efficient multi-factor identification. In order to improve privacy and security, blockchain-based identity management and Zero-Knowledge Proofs (ZKPs) were integrated into the USSCS framework. Thus, the verification process will be possible without exposing sensitive data to unauthorized parties.

In order to measure the effectiveness of the proposed multi-factor identification system, prototype implementation and testing was performed. The experiment shows that the proposed framework is capable of identifying individuals with up to 95-99% accuracy. It not only minimizes administrative burden but also prevents proxy attendance from occurring in campuses. Moreover, the framework conforms to the DPDP Act 2023 of India by following Privacy by Design.

Keywords: Smart Campus Identity, Multi Factor Authentication (MFA), Biometric Verification, Zero Knowledge Proofs (ZKP), Blockchain Technology, Decentralized Identifiers (DID), Data Privacy, DPDP Act 2023.

I. INTRODUCTION

The digital revolution in the education sector has contributed to the fast growth of the Smart Campus, which involves embedding ICT and IoT technologies into organizational activities to increase efficiency, enhance security measures, and promote sustainability. Based on the principles of the Smart City, smart campuses operate through centralized management systems and analytics, making decisions in areas such as academics, administration, the environment, and governance. In such an environment, the student ID is an essential tool that can be used as a means of access to academic and administrative services [1][2][3].

Despite the prevalence of digital technologies, most organizations still rely on manual attendance records and simple magnetic stripe cards. Such approaches have proved to be outdated in today's world, as they involve several shortcomings, including the lack of efficiency and the possibility of human errors during manual processes and the existence of proxy attendance ("buddy punching"). Although RFID systems offer better performance and greater ease of operation, they still pose significant risks because students can share or duplicate cards and abuse the system. Moreover, centralizing biometric information raises privacy concerns because student data can be a potential target for cyberattacks [4]. In light of the increasing demand for effective and efficient campus management systems, a multi-functional identity smart system framework is necessary. With the use of an automated process for attendance, access management, and other associated processes, the management of institutions will be simplified to enable better focus of the educators on results rather than processes. At the same time, privacy laws such as the recent DPDP Act 2023 in India necessitate adherence to the Privacy by Design model. Hence, a modern smart campus identity solution must be capable of offering robust security, effective management operations, and privacy for users [5].

This research paper outlines the design of the Unified Student Smart Card System (USSCS) , a scalable and privacy-enabled solution in a smart campus scenario. Some of the key contributions of this study include:

1. **Multi-factor Authentication Hub:** Developing a novel ESP32-S3 hardware node for integrating the 13.56 MHz RFID and Fingerprint authentication.
2. **Privacy Preserving Architecture:** Implementation of dual blockchain architecture (zkEVM) through the use of Non-interactive Zero Knowledge (NIZK) for secure credential validation without revealing Personally Identifiable Information (PII) [6].

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

3. **Decentralized Identity Management:** Adoption of Decentralized Identifiers (DID) to avoid having any single point of failure and empower the student with control over their identity information.
4. **Compliance Framework:** Technical framework that aligns with DPDP Act 2023, with focus on obtaining informed consent, minimizing data, and securing data processing.

The framework seeks to create an environment of identity management that is efficient, trustworthy, and scalable enough to handle the high throughput requirements of today's universities.

II. RELATED WORK

A. The Development of Campus Identification Systems:

The development of campus identification systems has seen progression from basic barcode and magnetic card technologies to more sophisticated smart campuses driven by the Internet of Things. The initial semi-automated technology helped reduce the time spent taking attendance and minimized paperwork, but it was susceptible to fraudulence and misuse.

There are recent works involving the use of ESP32 microcontrollers, RFID readers, and cloud databases for real-time attendance monitoring purposes, as well as works that make use of RFID technology alongside image recognition for the purposes of verifying identity. [1]

However, RFID technology alone lacks proper authentication features and is still prone to being used by proxies and cloned cards [4].

B. Biometric and Multi-Factor Authentication:

In an effort to mitigate the problems associated with the use of cards alone, studies on multi-factor authentication systems utilizing various biometrics, such as fingerprints and face recognition, have been conducted.

Multi-Factor Authentication (MFA) models that include:

- Possession factor: RFID card
- Inherence factor: Biometrics identity

Show higher reliability and accuracy compared to single-factor systems.

Hybrid approaches involving the use of ESP32 controllers equipped with fingerprint recognition sensors have proven to enhance attendance validation and minimize false acceptance rates. Still, multi-factor authentication models involving fingerprints can raise certain operational challenges, including:

- Surface cleanliness
- Sensor maintenance
- Performance degradation due to moisture or damaged fingerprints.

These issues must be considered for large-scale institutional deployment [2].

C. Security and Decentralized Identity Frameworks:

Prior literature points out an important problem related to the trade-off between usability, privacy, and security. The traditional centralized identity systems pose Single Point of Failures (SPOFs) where breach in one database will affect the student's confidential data [1].

In order to counter this problem, recent research works have turned towards Self-Sovereign Identity (SSI) and decentralization of trust models.

Identity systems based on blockchain technology provide control over the credentials using:

- Decentralized identifiers (DIDs)
- Verifiable credentials
- Tamper-proof audit trails

Additionally, Non-Interactive Zero Knowledge proofs (NIZK) including zk-SNARKs facilitate selective disclosures where students could demonstrate their qualifications or identity without revealing all personal details to third parties [6].

Gaps of Previous Research

Even though some prior research has focused on RFID system, biometrics-based attendance management, and identity system independently, there has been no study that combines:

- Multifactor authentication
- IoT Edge Devices
- Blockchain-based secure and verifiable identity
- Compliance regulatory mechanism

Within a single scalable smart campus framework.

This gap motivates the development of the proposed USSCS model.

III. SYSTEM ARCHITECTURE AND PROPOSED FRAMEWORK

The USSCS is envisioned as an information-rich and tightly integrated environment which seamlessly combines the

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

physical infrastructure of the college campus with its management information system.

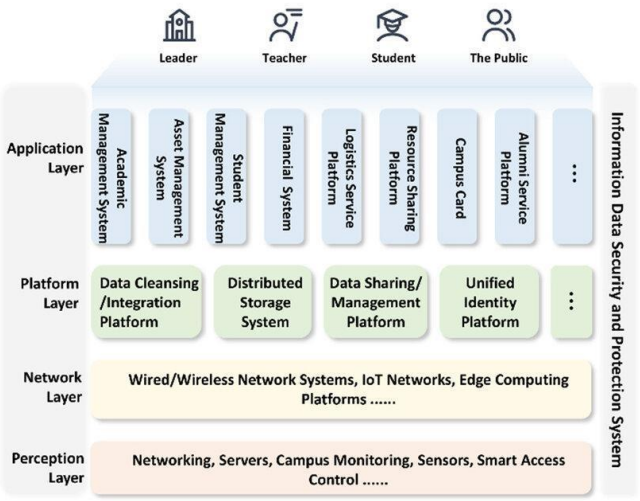

Figure 1: Four-layer architecture of the proposed USSCS framework

The proposed framework uses a hierarchical architecture comprising four layers for the Internet of Things (IoT).

A. Perception Layer (Sensing and Device Layer): The perception layer serves as the physical medium connecting users to the system, allowing instantaneous identity recognition and environmental monitoring.

- **Central Hub:** The primary hardware component revolves around the ESP32-S3 microcontroller (dual-core 32-bit, clocked at 240 MHz), chosen for its superior computing power and pre-installed Wi-Fi/Bluetooth capabilities. The microcontroller facilitates effective implementation of multi-factor authentication procedures independently from cloud resources.
- **Identification Devices:** The MFRC522 RFID tag reader (operating at 13.56 MHz) carries out non-contact-based identity recognition. The R307 fingerprint scanner is used for secondary biometric authentication. Biometric security is guaranteed via local hashing of fingerprint templates using the SHA-256 algorithm to maintain the confidentiality of biometric information.
- **Environmental Sensors:** The system incorporates an MQ2 gas sensor for the detection of harmful gases like smoke and LPG. Consequently, the system transcends basic identity management and can be utilized as a safety node within the campus network, providing real-time detection of hazards [7].

B. Network Layer (Communication Layer): The network layer guarantees secure, dependable, and efficient communication between edge devices and backend infrastructure.

- **Heterogeneous Connectivity:** The architecture leverages Wi-Fi 6 and 5G technology to enable dense connectivity on the campus, whereas LoRaWAN technology is deployed to provide long-distance, low-energy connectivity for campuses of significant size.
- **Integration With Edge Computing:** Basic authentication operations, like UID verification and Match-On-Card verification, are carried out by edge devices themselves, thereby reducing reliance on servers, alleviating network congestion, and minimizing delays when using services at peak times [8].

C. Middleware/Security Layer (Core Processing Layer): This layer is responsible for dealing with identity, privacy, and distributed trust.

- **Dual-Blockchain Design (zkEVM):** Private information about PII data will be hosted using the zkEVM blockchain while credentials hash will be on a public blockchain.
- **Zero-Knowledge Proofs Engine:** The system uses zk-SNARKs (Groth16 Non-Interactive Zero Knowledge). This allows students to selectively disclose attributes like enrollment without exposing sensitive private identities information.

D. Application Layer (User Interface Layer): This layer offers services to end-users and administrators for the campus community.

- **Dashboard for Administrators:** This was built using Django and FastAPI. It is designed to monitor attendance data, financial transactions, and the usage of institutional resources in real-time [7].
- **Mobile Application for Students:** The React Native mobile application acts as a digital identity wallet, allowing NFC-based cashless payments and an SOS button that sends GPS coordinates to campus security [7].

Through the proposed architecture of four layers, USSCS will operate as a smart campus identity ecosystem with secure and privacy-preserving characteristics.

IV. METHODOLOGY AND SYSTEM DESIGN

The proposed system, referred to as the Unified Student Smart Card System (USSCS), will be created through the use of an architecture that incorporates both hardware and software to ensure secure and efficient management of identities within smart campuses.

A. Hardware Component Specifications: The purpose of the perception node is to ensure reliable performance, rapid

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

reaction times, and the ability to conduct secure calculations at the edge in a highly dense institutional setting.

- **Central Processing Unit:** The chosen platform for the proposed solution is ESP32-S3 microcontroller due to the dual core capabilities, low power usage, Wi-Fi/Bluetooth capabilities. Moreover, it provides support for hardware-assisted encryption methods such as SHA-256 and AES, which allow local processing and minimize cloud dependence.
- **RFID Subsystem:** For contactless authentication purposes, an RFID reader is used with the frequency of 13.56MHz and is connected to the microcontroller via SPI protocol. With a small read range (up to 3-5 cm), it allows preventing unauthorized access as well as the risk of relay and cloning attacks.
- **Biometric Engine:** The fingerprint scanner chosen for the implementation is the R307 model that allows performing local storage and on-device matching (Match-on-Card). This prevents transmission and external storing of sensitive information related to biometrics.

B. Software Stack and Cryptographic Framework: The software stack is modular and designed to be scalable and concurrent with high security levels.

- **Backend Middleware:** This is built using FastAPI, an asynchronous framework that enables several authentications requests concurrently, particularly in IoT settings.
- **Zero Knowledge Proof Pipeline:** For privacy-preserving authentication, Circom based circuits have been used to generate Rank-1 Constraint Systems (R1CS). The framework employs Poseidon hash function, which is more computationally effective within ZKP frameworks.
- **Database Management System:** This is facilitated by Firebase Realtime Database and Firebase Cloud Messaging (FCM), providing real-time updates within 300ms.

C. Sequential Authentication Flow: To ensure strong identity verification, the system adopts a Three-Factor Authentication (3FA) model combining possession, inherence, and cryptographic proof.

Algorithm: Multi-Factor Authentication Procedure

Input: RFID_UID, Fingerprint_Scan

Output: Authentication_Status

1. The ESP32-S3 continuously scans for RFID card presence.
2. The system reads the RFID card UID.
3. UID is validated using a locally encrypted cache.
4. If valid, the fingerprint sensor captures and verifies a live sample.
5. The mobile application generates a zk-SNARK proof using the user's private credentials.
6. The backend verifies the proof using a blockchain verification key.
7. If successful:
   - Access granted
   - Attendance logged in Firebase

   Else:
   - Access denied
   - Unauthorized alert generated

D. System Working Process: Enrollment to Verification: The entire process of identity life cycle is segregated into three working phases.

1. Enrollment Phase: At the time of enrollment:

- Details about the student identity are obtained
- Fingerprint template hashing happens with the help of SHA-256 algorithm
- Data is registered on the private zkEVM blockchain
- Decentralized Identifiers (DID) are issued
- DID is kept stored in the mobile wallet of the student

2. Operational Phase: In the day-to-day functioning of the campus:

- Authentication takes place through RFID and fingerprints
- Zero-knowledge proof is generated via the mobile app
- Proofs for credentials are verified via blockchain without disclosing any identity information

3. Safety Monitoring Phase: At the same time, the system facilitates campus safety monitoring through the following mechanism:

- Smoke detection and LPG gas leakage are identified using MQ2 gas sensor
- Random Forest algorithm is used to analyze the information
- Alert notifications are sent out through the SIM900A GSM module to the campus authorities.

V. SECURITY AND PRIVACY FRAMEWORK

The Unified Student Smart Card System (USSCS) utilizes the Privacy by Design framework where privacy and data protection are at the heart of the entire design process,

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

thus ensuring user sovereignty, confidentiality, and robustness against attacks on the system from both physical and networking fronts.

A. Dual Blockchain and Zero-Knowledge Proof System: The ID management system uses a dual-blockchain system where sensitive data is stored on one blockchain layer while the other blockchain layer provides a means of verifying credentials.

1. Private zkEVM Blockchain Layer: The private blockchain layer stores sensitive PII that includes:

- Biometric hash, educational credentials, Registration credentials

For increased security and decentralization, encryption of documents takes place via Interplanetary File System (IPFS).

2. Public zkEVM Blockchain Layer: The public blockchain layer performs the following tasks:

- Generates ZKP, validates user credentials, Maintains trust records

Only non-reversible credential hashes are maintained in the public blockchain layer. As a result, there would be no revelation of any raw student information even when the public ledger is hacked.

B. Zero-Knowledge Proof Mechanism: The NIZK proofs are achieved via the use of zk-SNARKs that utilize Non-Interactive Zero-Knowledge Proofs (NIZK).

This enables the user to prove properties like:

- Membership status, Access privileges, Ownership of the identity

Without disclosing any details about their private information.

For an efficient proof process, the framework adopts the Poseidon hash function, which has been built for zero-knowledge protocols. The Poseidon hash function is much better than SHA-256 as it has much lower arithmetic circuits, thus decreasing computing cost on mobile/embedded devices.

C. Data Security and Cryptographic Approach: In order to ensure the integrity and confidentiality of the data in all stages of processing, USSCS employs several encryption techniques.

1. At-Rest Data: All caches, biometric references, and backend database records are encrypted using AES-256 encryption technology. In the event that the device is stolen, this ensures the protection of the data from unauthorized access.

2. Data in Transit: The communication channels in USSCS include ESP32 edge devices, mobile applications, and backend servers. These are encrypted using:

- HTTPS/TLS protocols, Elliptic curve integrated encryption scheme (ECIES)

This ensures that data transmission is immune to various forms of eavesdropping and attacks, including interception, replay attacks, and man-in-the-middle attacks.

3. Biometric Irreversibility: Instead of storing fingerprints as image or scan files, USSCS stores fingerprints as hashed values, which cannot be converted back into their original form.

D. Security Advantages of the Proposed Approach: Benefits of the suggested security system include:

- No risks from centralized biometric database, Does not reveal personal identification information, secures information on the storage and communication levels, Complies with applicable regulations and requirements

All in all, the USSCS security and privacy framework offers a scalable, decentralized, and regulation-compliant identity management approach for smart campuses.

VI. RESULTS AND DISCUSSIONS

The pilot deployment of USSCS has provided evidence on the advantages and challenges that arise when moving towards smart campuses. The results have shown positive changes in efficiency, security, and privacy.

A. Interpretation of Results and Institution-wide Impact: The results have proven that the integration of MFA with decentralized identities improves the accuracy of records and increases the level of administrative efficiency.

Administrative Efficiency: The introduction of this system allowed for saving up to 60% of administrative time, which was previously devoted to handling traditional attendance activities.

Higher Accuracy: Automated identity validation has helped avoid human errors and increased trust in the records collected.

Privacy Acceptance: Although most students accept the idea of digital tracking to increase the effectiveness of their campus experience, they tend to be wary of having their private data accessed. In this regard, the framework is based on the Privacy by Design principle that uses SSI to give users control over their identities.

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

All in all, the framework combines efficiency and user privacy needs.

B. Comparison with Existing Systems: The USSCS system has many advantages over other existing campus identification systems.

1. Manual or Barcode Based Systems: These attendance methods are slow, unreliable, and prone to fraudulent activity.

From conventional methods, approximate reliability was increased to almost 99% authentication rate, Attendance process time greatly reduced

2. Basic RFID Based Attendance System: A basic RFID system enhances the speed but is susceptible to the following risks: Sharing of cards, Card cloning, Proxy attendance.

By using biometrics, proxy attendance was effectively blocked in USSCS during pilot implementation.

3. Traditional Centralized Biometric Systems: Biometric systems with centralized templates of sensitive biometric data are Single Points of Failure (SPOF) systems.

This can be mitigated in USSCS through the use of: Local card-based match on card process, Cryptographic hashes of biometric data, selectively revealing biometric data by implementing Zero-Knowledge Proof (ZKP).

C. Technical Limitations and Constraints: Though beneficial, some limitations persist.

1. Environmental Influences: Potential environmental influences that might impact the performance of fingerprint sensors include: Moisture, Dust, Injured fingers, Incorrect placement of fingers

These might contribute to an increased false rejection rate.

2. Computation Intensive Nature: The proof generation of zk-SNARK is computationally intensive thus it might strain the processor capacity and consume energy in a mobile environment.

3. Scalability Issues: While edge computing lessens the burden of network transmission, performance is likely to be hindered when the number of devices is extremely high due to excessive parallel processing demands.

4. Hygiene Factors: Touch-based fingerprint sensors may pose hygiene issues for campus-based students. The next generation of fingerprint sensors should incorporate non-contact biometric methods like face scanning or eye scanning.

D. General Discussion: From the pilot test results, USSCS emerges as a promising alternative to current campus identification methods. This system offers the following qualities: High authentication precision, Low administration overhead, Privacy protection, Anti-fraud measures, intelligent campus services management.

Nevertheless, in future enhancements, attention must be paid to scalability enhancement, efficient cryptography computation, and contactless biometrics implementation

6.1 Regulatory Compliance (DPDP ACT 2023)

The design of the USSCS system is based on the compliance of the Indian Digital Personal Data Protection (DPDP) Act 2023 and implementing regulations. Considering that educational establishments will handle private identity information, behavioural data, and biometric data, the regulatory compliance follows the principles of the Privacy by Design framework.

A. Notice and Informed Consent (Sect. 6): According to the provisions of the DPDP Act, the data collectors need to have clear notice and consent for personal data.

Notice with Privacy Statement: The USSCS mobile application gives a privacy statement with clear notification concerning the data collected (e.g., RFID UID, biometric hash, and GPS coordinates) and its purposes (attendance control, safety notifications, payments on campus).

Easy Process for Withdrawing Consent: The USSCS mobile application allows withdrawing consent at any point.

B. Protection of Minors (Sec. 9): The DPDP Act mandates that extra provisions must be in place for persons below 18 years old.

Consent from Guardian: This system allows a process by which guardians/parents can give consent before enrolling or processing minors' personal information.

Restriction on Behavioural Profiling & Advertisements: Behavioural profiling and advertisements are disabled for minors.

C. Data Minimization and Disclosed Attributes Only (Rule 10): The proposed framework minimizes data gathering to the minimal amount required for certain campus activities.

Proof System Using Zero Knowledge: Through the use of Non-interactive Zero-knowledge proof, students are able to prove status attributes without having to disclose their private data.

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

Biometric Privacy Protection: Fingerprints are stored in hashed template form to minimize the chances of being disclosed in case of any breach.

D. Rights of the Data Principal (Section 11): In USSCS, there are technological provisions which comply with the rights of users under the DPDP Act.

1. Right to Access: Students can view summaries regarding:

- Data processing operations, Authentication operations, Sharing permissions for services, Active identity credentials , via a secure dashboard interface.

2. Right to Correct and Delete: A person who qualifies may make requests for modification/deletion of their records after they graduate or withdraw from the institution or complete the purpose of education.

E. Reasonable Security Measures: Reasonable security measures within USSCS include:

- AES-256 protected storage technology, Use of ECIES to communicate securely, Edge computing for secure processing on ESP32-S3, Access control to identity records

The framework can be extended to include institutional procedures for incident management and notification, if required.

Compliance Conclusion

By using the elements of consent, data minimization, biometrics protections, right controls and strong encryption, the USSCS framework provides a pragmatic path toward privacy-compliant identity management in the smart campus.

6.2 Future Plan and Development

Future intelligent campus identity systems will likely become more advanced through innovations in artificial intelligence, connectivity, blockchain technology, and biometrics. The use of these technologies can lead to even greater levels of automation and protection in campus operations.

A. Shift Toward Agentic and Explainable AI: The next level of campus management might see the use of Agentic AI, where AI-based systems help with campus operations including administration and education-related activities.

Possible uses include: Efficient scheduling and timetabling, Automated processes for identity verification, Customized assistance for students, Validation of credentials for foreign students or exchange programs.

For ethical considerations, Explainable AI should be incorporated into future intelligent campus systems to ensure fairness and transparency in decision-making processes.

B. Modular Blockchain and Post-Quantum Security: Modular blockchains with distinct execution, consensus, and availability layers are likely to become the norm for future blockchain systems. This will help increase scalability and throughput for future university ecosystems.

Considering that student records are usually stored for long periods, future security updates must also take into account post-quantum cryptography solutions.

Examples include:

ML-DSA (Dilithium), a signature scheme, ML-KEM (Kyber), a key encapsulation mechanism.

Utilizing post-quantum cryptographic methods can offer long-term privacy and security.

C. Implementation of 6G and Digital Twin Environments: The advent of future communication technology like 6G could offer extremely low latency with high density of devices connected to the network.

Such technology could be used to create a campus digital twin, which is an advanced virtual representation of the campus, taking into account the sensors installed on the premises and the buildings themselves.

Possible advantages are: Simulation of evacuation plans, Optimized energy use, Maintenance scheduling, Crowd control

D. Enhanced Biometrics and Liveness Detection Systems: In light of advanced methods used to commit fraud through synthetic identity or AI-based spoofing attacks, biometric defenses should be enhanced further.

Some research opportunities may focus on: Detection of live fingerprints, faces, and irises, multi-spectral biometric scanning, Recognition algorithms resistant to deepfakes, Anti-adversarial testing of systems, Use of AI in anomaly detection

With these approaches, users can be separated from artificial biometric imposters.

Conclusion

The future of USSCS-like systems is dependent upon the incorporation of: Advanced automation, Decentralized identity management solutions, Quantum cryptography, Real-time digital university facilities, Sophisticated anti-spoofing biometric defenses

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 234-241, April-2026
https://doi.org/10.47001/IRJIET/2026.104034

These technologies will enable the creation of safe and intelligent digital environments for universities.

VII. CONCLUSION

The evolution from traditional campus identification systems to secure, versatile digital identities constitute a crucial step towards the fulfillment of the Smart Campus vision. The findings of this research reveal the potential of implementing IoT hardware (ESP32-S3), multi-factor biometric authentication, and the dual blockchain architecture zkEVM to drastically increase the efficiency of higher education institutions while maintaining students' privacy and data sovereignty.

As seen from the experiment, the USSCS is able to save up to 60% of time spent on administrative duties and reach the level of authentication accuracy of 99%. Moreover, the multi-layered authentication approach employed in the suggested model effectively eliminates frequent problems such as proxy attendance and unauthorized use of identity.

Apart from solving the issue of identity management, the incorporation of safety monitoring capabilities turns the student smart card into an active part of the safety infrastructure and makes it possible to monitor hazards on campus.

However, the success of any such systems largely depends on their strict adherence to the principles of Privacy by Design as well as legislative frameworks like India's DPDP Act 2023. A student-oriented approach to identity management based on decentralization will allow institutions to establish a sustainable, secure, and advanced campus environment.

REFERENCES

[1] B. O. Zarpellon, L. de Oro Arenas, E. P. Godoy, F. P. Marafão, and H. K. M. Paredes, “Design and Implementation of a Smart Campus Flexible Internet of Things Architecture on a Brazilian University," *IEEE Access*, 2024.

[2] L. Shihao, D. P. Dahnil, and S. Saad, "A Survey of Smart Campus Resource Information Management in Internet of Things," *IEEE Access*, 2025.

[3] N. Cavus, S. E. Mrwebi, I. Ibrahim, T. Modupeola, and A. Y. Reeves, “Internet of Things and its applications to smart campus: A systematic literature review,” *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 23, pp. 17–35, 2022, doi: 10.3991/ijim.v16i23.36215.

[4] Meghana, Inturi & Meghana, J.D.N.V.L. & Jayaraman, Ramesh. (2020). Smart Attendance Management System using Radio Frequency Identification.10451049.10.1109/ICCSP48568.2020.9182167.

[5] P. Yadav and R. Yadav, “Privacy in the digital age: A critical study of the DPDP Act 2023 and its implications,” *Faculty of Law, University of Lucknow*, 2023.

[6] Dieye, Mohameden & Valiorgue, Pierre & Gelas, Jean-Patrick & Diallo, El-Hacen & Ghodous, P. & Biennier, Frédérique & Peyrol, Eric. (2023). A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain. *IEEE Access*. PP. 1-1. 10.1109/ACCESS.2023.3268768.

[7] Chandru, Dhanush & Shekadar, Aparna & Chowdhury, Sumit. (2025). Automated Attendance System using RFID and IoT. *IRO Journal on Sustainable Wireless Systems*. 7. 257-277. 10.36458/jismac.2025.3.002.

[8] Muhammad Al Imran, Muhammad Fikry, & Sujacka Retno. (2025). Enhancing Academic Security with RFID-Based Smart Locks and Real-Time Attendance Tracking System. *Proceedings of International Conference on Multidisciplinary Engineering (ICOMDEN)*, 2, 00076.

[9] "Agentic AI in Education: State of the Art and Future Directions," *ResearchGate Technical Synthesis*, 2025.

[10] "A Comparative Analysis of Fast API and Django Frameworks for IoT," *IJSREM*, vol. 10, no. 3, 2026.

[11] "The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)," *The Gazette of India*, Aug 11, 2023.

Citation of this Article:

Aditi Bhadake, Snehal Khode, & Nikita Uphade. (2026). A Privacy Preserving Multi Factor Identity Framework for Smart Campuses Using Biometrics and Blockchain. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(4), 234-241. Article DOI https://doi.org/10.47001/IRJIET/2026.104034

****

