Decentralised Data Logging Architecture Secured by Dual Authentication

Urja Saha, Saloni Bele, Manaswi Rajput, Anand D Mane, Dayanand D Ambawade
Department of Electronics and Telecommunication Engineering Sardar Patel Institute of Technology, Mumbai, India

***Abstract* - Accurate attendance monitoring is essential in academic and corporate environments where accountability and participation directly impact performance evaluation. Conventional manual or RFID-based systems are vulnerable to proxy marking, data tampering, and administrative inefficiencies. To overcome these challenges, this paper presents ZenTap — a secure, automated attendance system that integrates Internet of Things (IoT) authentication with blockchain-based data integrity verification.**

The proposed system employs an ESP32 microcontroller interfaced with an R307 fingerprint sensor and RC522 NFC reader for dual-factor authentication. Each attendance transaction is encrypted using AES-128, digitally signed, and transmitted to a backend implemented on the FastAPI framework. The backend validates device credentials through JWT-based authentication, stores attendance data in a structured PostgreSQL database, and generates a SHA-256 hash of each verified record. These hashes are immutably committed to a private blockchain ledger, ensuring transparency and non-repudiation of attendance logs.

The frontend ecosystem comprises a React–TypeScript web dashboard for administrators and a Flutter mobile application for instructors and students, providing real-time visibility, analytics, and blockchain verification of records. Experimental implementation demonstrates reliable performance, minimal latency, and high resistance to data manipulation compared to conventional centralized attendance systems. The proposed architecture establishes a scalable model for secure, verifiable, and decentralized attendance management in educational institutions.

I. INTRODUCTION

Accurate and transparent attendance tracking plays a crucial role in academic institutions, corporate environments, and government organizations, where accountability and time management are essential. Traditional attendance recording methods—such as manual signatures or roll-call systems—are prone to inefficiency, human error, and manipulation. The increasing complexity of modern educational institutions, with large class sizes and distributed campuses, further complicates the monitoring of student presence and engagement. Consequently, the demand for automated, tamper-resistant attendance systems has grown substantially in recent years.

To address these challenges, automated systems employing biometric identification (fingerprint, facial, or iris recognition), RFID/NFC cards, and Bluetooth beacons have been explored. While these methods improve efficiency, they still suffer from limitations including data tampering, unauthorized proxy attendance, lack of auditability, and poor interoperability between devices. Many existing commercial biometric systems operate as closed, centralized architectures where the data is stored in local servers or proprietary clouds. This creates a single point of failure, vulnerability to cyberattacks, and opportunities for post-facto data manipulation. Additionally, these systems often neglect the privacy and integrity of biometric data, which requires secure storage and controlled access mechanisms.

Recent research has proposed Internet of Things (IoT)- based attendance systems integrating wireless sensors and edge controllers to automate attendance marking. However, many of these implementations rely solely on microcontrollers transmitting unverified data to cloud databases, which can be intercepted or modified during transmission. Moreover, few solutions provide a means for independent verification of attendance authenticity after storage. As institutions increasingly adopt digital recordkeeping, it becomes imperative to ensure that the recorded data is both trustworthy and immutable.

To overcome these limitations, the proposed work introduces **ZenTap** — a *smart attendance system integrating IoT authentication with blockchain-based integrity verification*. The system combines multiple technologies to achieve secure, real-time, and verifiable attendance management:

- A **dual-authentication IoT hardware unit** built around the ESP32 microcontroller, integrating both a fingerprint sensor (R307) and an NFC reader (RC522) to ensure multi-factor identity verification.
- A **backend server** implemented using the **FastAPI** framework, which validates encrypted attendance packets, performs access control through **JWT authentication**, and stores records in a structured **PostgreSQL** database.
- A **blockchain layer** that commits cryptographic hashes (SHA-256) of verified attendance records to ensure im- mutability and enable future proof-of-integrity verifica- tion.
- A comprehensive **application layer** consisting of a **React-based web dashboard** for administrators and a **Flutter mobile application** for students and faculty, supporting real-time monitoring and analytics.

Unlike conventional centralized attendance systems, ZenTap ensures end-to-end trust by securing every stage of the data flow—from biometric authentication to record archival.

The ESP32 encrypts attendance data using **AES-128** before transmission, and each transaction is timestamped to prevent replay attacks. The blockchain ledger provides a decentralized validation mechanism, ensuring that once attendance data is recorded, it cannot be retroactively modified. Furthermore, the system architecture is modular and scalable, enabling integration across multiple classrooms or departments with minimal reconfiguration.

The integration of blockchain into the attendance domain not only enhances transparency but also provides a robust audit trail for regulatory or institutional verification. The proposed system contributes to the growing research focus on combining IoT and distributed ledger technologies for trustworthy cyber-physical systems. Through its lightweight design, strong cryptography, and hybrid frontend-backend architecture, ZenTap presents a practical, deployable, and secure solution to the persistent challenges of attendance management in educational institutions.

II. RELATED WORK

Attendance automation has been a recurring research focus across IoT, biometric, and blockchain domains. Earlier systems primarily employed **RFID** or **NFC** tags for identity recognition due to their low cost and ease of deployment. However, such methods are inherently vulnerable to card duplication, unauthorised use, and data manipulation when implemented without additional verification layers or encryption mechanisms.

Safi'ie *et al.* [5] introduced an IoT-based RFID attendance prototype that successfully automated record submission to the cloud. Despite improving data accessibility, it lacked mechanisms to prevent tag cloning or proxy attendance, resulting in compromised authenticity. Rizvi *et al.* [2] presented an NFC-based monitoring system using microcontrollers and cloud storage, which enhanced usability but remained dependent on the possession of an NFC tag alone. Isa *et al.* [3] proposed an NFC-enabled attendance model using smartphones, offering user convenience yet neglecting encryption and multi-factor authentication, thus exposing it to replay attacks and credential theft.

To address the issue of data integrity, several researchers explored blockchain integration. Shah and Ingle [1] surveyed the use of distributed ledgers for secure NFC communication, outlining its potential for immutable logging but without coupling it to physical authentication. Similarly, Al-Dahan *et al.* [4] reviewed NFC-based attendance systems, highlighting the challenge of ensuring genuine presence when only tag identification is employed. Face-recognition-based models attempted to solve this through biometric validation [4]; however, they suffer from privacy concerns, high computational cost, and environmental sensitivity (lighting, occlusion, and angle dependency).

These existing approaches reveal two persistent gaps in the literature:

1) **Weak User Authentication:** Most RFID/NFC-based designs depend on static tag identification, making them susceptible to proxy and replay attacks.
2) **Centralised or Mutable Data Storage:** Cloud databases in earlier systems lack verifiable integrity, allowing undetected modification of attendance records.

ZenTap bridges these gaps through a **dual-authentication, decentralised architecture**. The proposed system binds the attendance event to a verified biometric identity (via fingerprint scanning) and validates the NFC tap within a cryptographically controlled time window. This guarantees that only legitimate users physically present can register attendance. In contrast to previous centralised logging models, ZenTap employs a **FastAPI–PostgreSQL backend** augmented with **blockchain-based hash anchoring**, ensuring that any post-hoc alteration of stored records is detectable. Moreover, the integration of **AES-encrypted IoT communication**, **JWT-secured APIs**, and **role-based access** for the React/Flutter frontends collectively ensures end-to-end integrity and accountability—an advancement not realised in earlier implementations.

Table VII summarises the comparison of key related works and the unique contributions of ZenTap.

TABLE I: Comparison of Existing Attendance Systems with ZenTap

System	**Authentication Method**	**Data Integrity**	**Privacy / Security**	**Our Contribution**
Safi'ie *et al.* [5]	RFID Tag Only	Centralised Cloud	None	Vulnerable to cloning
Rizvi *et al.* [2]	NFC Tag	Cloud-based Logging	Low (no encryption)	Device-dependent
Isa *et al.* [3]	NFC via Smartphone	Local + Cloud	No encryption, No MFA	Replay risk
Blockchain Models [1]	Varies	Immutable (on-chain)	High integrity, low usability	No biometric binding
ZenTap (Proposed)	Fingerprint + NFC (Dual Authentication)	Blockchain-hashed PostgreSQL	AES + JWT Security	Full-stack secure, tamper-proof system

III. PROPOSED SYSTEM ARCHITECTURE

The overall architecture of the proposed *ZenTap* system is organised into three collaborative layers—**IoT Hardware Layer**, **Backend Processing Layer**, and **Application Layer**. Each layer performs distinct roles to achieve secure, reliable, and tamper-proof attendance recording. The architectural overview is shown in Fig. 1.

A. IoT Hardware Layer

The hardware layer functions as the primary interface for user authentication. It employs the **ESP32-WROOM** module as the central controller due to its dual-core processor, integrated Wi-Fi, and low power consumption. The ESP32 interfaces with:

- **R307 Optical Fingerprint Sensor** via UART for biometric identity verification.
- **RC522 NFC Reader** via SPI for secondary authentication through contactless NFC cards.

The operational flow begins with fingerprint scanning and template matching on the device. Upon successful verification, a short-lived cryptographic token activates the NFC reader for approximately 10 seconds. The NFC tag ID, device ID, and timestamp are then packaged into a structured JSON message, encrypted using **AES-128**, and transmitted to the backend via HTTPS. Power management is handled through a 3.7 V Li-Po battery regulated by a TP4056 charging module, supporting portable classroom use and long battery life.

B. Backend Processing Layer

The backend is developed using the **FastAPI** framework for its asynchronous request handling and scalability. It receives encrypted packets from IoT devices, validates the session token, verifies timestamps, and stores attendance events in a **PostgreSQL** database through SQLAlchemy ORM.
Each attendance record contains the following fields:

- `UserID, DeviceID, NFC_UID, Timestamp, SessionToken, Status.`

To ensure tamper-proof logging, a **SHA-256 hash** of each validated record is committed to a lightweight blockchain (prototype using **Ganache**, scalable to **Hyperledger Fabric**). This enables integrity verification by comparing future hashes with blockchain entries, providing a verifiable audit trail.

Access to backend services is protected using **JWT-based authentication** and **role-based access control (RBAC)**, enabling secure and privilege-bound communication between devices, administrators, and clients.

C. Application Layer

The application layer provides a unified user interface for real-time monitoring and analytics. It includes:

- **Web Dashboard:** Built using **React 18** and **TypeScript**, it allows administrators and instructors to visualise attendance data, verify blockchain integrity, and manage device registrations.
- **Mobile Application:** Developed in **Flutter**, it enables students to view their authenticated attendance records and instructors to monitor class participation on the go.

All application interfaces communicate securely with the FastAPI backend using RESTful APIs over HTTPS. The frontend visualisations are powered by real-time database queries and blockchain verification endpoints.

IV. SYSTEM DESIGN AND IMPLEMENTATION

The proposed **ZenTap Smart Attendance System** is designed as a three-tier architecture encompassing the *IoT device layer*, the *backend service layer*, and the *frontend application layer*. Each tier performs a specific function in the secure acquisition, validation, and recording of attendance data. The overall implementation ensures real-time operation, dual authentication, and blockchain-based data integrity.

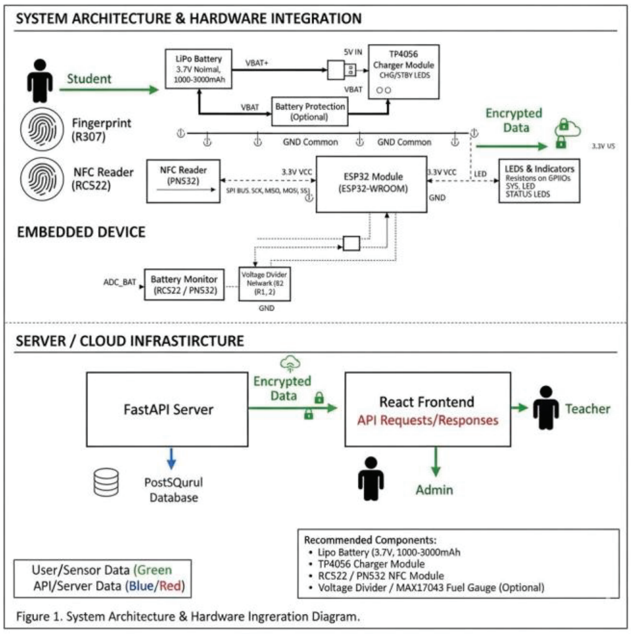

SYSTEM ARCHITECTURE & HARDWARE INTEGRATION
Student
LiPo Battery 3.7V Noimal, 1000-3000mAh
VBAT+
5V IN
TP4056 Charger Module CHG/STBY LEDS
VBAT
VBAT
Battery Protection (Optional)
Fingerprint (R307)
GND Common
GND Common
Encrypted Data
3.3V US
NFC Reader (RCS22)
NFC Reader (PNS32)
3.3V VCC
SPI BUS SCK, MSO, MOSI, SS
ESP32 Module (ESP32-WROOM)
3.3V VCC
LED
GND
LEDS & Indicators Resistons on GPIIOs SYS, LED STATUS LEDS
EMBEDDED DEVICE
ADC_BAT
Battery Monitor (RCS22 / PNS32)
Voltage Dvider Nelwark (82 (R1, 2)
GND
SERVER / CLOUD INFRASTIRCTURE
FastAPI Server
Encrypted Data
React Frontend
API Requests/Responses
Teacher
PostSQurul Database
Admin
Recommended Components:
• Lipo Battery (3.7V, 1000-3000mAh
• TP4056 Charger Module
• RCS22 / PN532 NFC Module
• Voltage Divider / MAX17043 Fuel Gauge (Optional)
User/Sensor Data (Green
API/Server Data (Blue/Red)
Figure 1. System Architecture & Hardware Ingreration Diagram.

Fig. 1: Updated System Architecture showing layered design of IoT device, backend, and frontend integration.

A. IoT Device Layer

The IoT layer forms the physical interface for user authentication. It is built around the **ESP32-WROOM** microcontroller due to its integrated Wi-Fi module, high processing speed, and low power consumption. Two input devices are interfaced with the ESP32: an **R307 optical fingerprint sensor** for biometric identification and an **RC522 NFC reader** for contactless verification. The ESP32 firmware is developed in **C/C++** using the **Arduino framework**, ensuring portability and ease of development.

When a student interacts with the device, the fingerprint module initiates authentication by comparing the scanned fingerprint against pre-stored templates in the local flash memory. Upon a successful match, the ESP32 generates a **temporary cryptographic unlock token** that activates the NFC reader for a 10-second time window. The NFC module then reads the student's ID tag to complete the second layer of authentication.

This *dual-step mechanism* ensures that no proxy attendance can occur through the use of duplicate fingerprints or cloned NFC tags.

The attendance data packet, consisting of *User ID, Timestamp, Device ID, and Session Token*, is encrypted using the **AES-128 symmetric encryption algorithm** before transmission. The device communicates securely with the backend via the **HTTPS protocol**, ensuring confidentiality and integrity of transmitted data.

B. Backend Service Layer

The backend layer, implemented using **FastAPI**, functions as the central data processing and authentication hub. FastAPI was chosen for its asynchronous capabilities, speed, and built-in support for RESTful APIs. The backend receives encrypted attendance payloads from multiple IoT nodes, decrypts them using pre-shared keys, and performs validation through **JWT (JSON Web Token)** authentication to confirm that the request originates from an authorized device.

The validated data is structured and stored in a **PostgreSQL** relational database through the **SQLAlchemy ORM**. The schema includes tables for students, courses, instructors, and attendance logs, all normalized to ensure data consistency. Each verified attendance record is serialized and hashed using the **SHA-256** algorithm. This hash value is subsequently written to a private blockchain network, initially deployed on **Ganache** for testing and later migratable to **Hyperledger Fabric** for enterprise-scale deployment.

The blockchain serves as a *tamper-evident ledger*—any modification in the primary database results in a mismatch between stored and blockchain hashes, allowing immediate detection of data tampering. The integration between FastAPI and the blockchain layer is achieved through **Web3.py**, providing seamless communication between the Python backend and Ethereum-compatible blockchain nodes.

C. Frontend Application Layer

The frontend layer provides the visualization and control interface for administrators, instructors, and students. The web dashboard is developed using **React 18** with **TypeScript** and styled using **Tailwind CSS**, ensuring a responsive and modular design. The web application interacts with backend APIs through secure HTTPS endpoints and employs JWT-based route protection. Administrators can manage courses, verify device registration, and view blockchain-verified attendance logs, while instructors can access real-time class reports and student activity.

In addition, a **Flutter mobile application** was developed to enhance portability and ease of access. The app allows students to verify their attendance status, instructors to initiate sessions, and administrators to audit blockchain hashes for integrity verification. The synchronization between mobile, web, and backend components ensures system-wide data consistency.

D. Firmware and Communication Flow

The firmware architecture on the ESP32 is modular, consisting of five primary tasks: *sensor control*, *user authentication*, *encryption*, *network communication*, and *error handling*. Non-blocking task scheduling ensures minimal latency during authentication. Communication with the backend follows a request–response model using RESTful endpoints. The firmware also includes a caching mechanism to temporarily store attendance events during network outages and synchronize them once the connection is re-established.

E. Integration and Testing

The integrated system was tested under real-world conditions using a local Wi-Fi network and a mock blockchain environment. Average authentication time was measured at approximately 1.2 seconds per student, with a transmission latency below 250 ms. The AES encryption and HTTPS communication layers introduced negligible overhead, while blockchain commitment time averaged 0.8 seconds. The system exhibited high reliability and consistency across multiple devices with no recorded data mismatches during blockchain verification.

Overall, the combination of IoT-based authentication, RESTful backend design, and blockchain verification establishes a robust, secure, and scalable solution for modern attendance management systems.

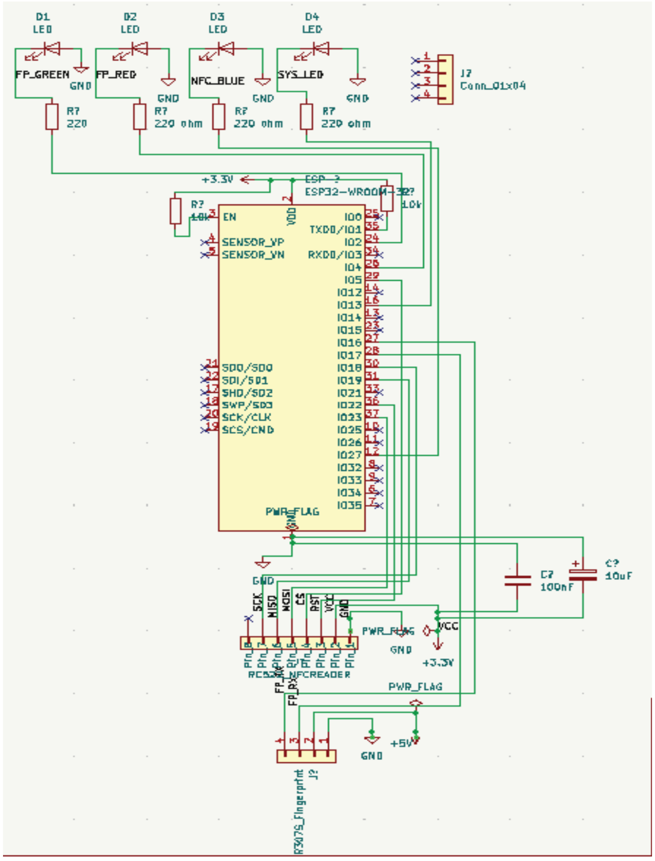


Fig. 2: Hardware schematic of the NFC-enabled attendance system integrating PN532 NFC module, ESP32 microcontroller, and secure communication interface.

V. MATHEMATICAL FOUNDATIONS OF BLOCKCHAIN

The integrity and immutability of attendance records in the proposed system are ensured using cryptographic hash functions and Merkle-tree–based verification. Each validated attendance entry R is converted into a fixed-length digest using the SHA-256 hash function:

$$h = H(R), \tag{1}$$

where $H : \{0, 1\}^* \rightarrow \{0, 1\}^{256}$ is a one-way, collision-resistant mapping. Any modification in R results in a completely different h, ensuring tamper detection.

A. Hash-Chained Block Structure

Each block B_i contains the data D_i, timestamp, and the hash of the previous block:

$$B_i = (D_i, H_{i-1}), \tag{2}$$

with the block hash computed as

$$H_i = H(D_i \parallel H_{i-1}), \tag{3}$$

where $\parallel$ denotes concatenation. Thus, altering any block invalidates all subsequent hashes, providing immutability.

B. Merkle Root for Record Verification

Multiple attendance records $\{h_1, h_2, \ldots, h_n\}$ are aggregated in a Merkle tree. For two child hashes h_a and h_b, the parent node is computed as:

$$h_{a,b} = H(h_a \parallel h_b). \tag{4}$$

The Merkle root, denoted as M, uniquely represents all records within a block:

$$M = H(\ldots H(h_1 \parallel h_2) \parallel \ldots \parallel H(h_{n-1} \parallel h_n)). \tag{5}$$

A record is verified by recomputing its Merkle proof and checking

$$M' = M. \tag{6}$$

C. Record Authenticity Using Digital Signatures

Each IoT device signs its encrypted payload using an elliptic-curve digital signature. Given private key d and generator point G, the public key is:

$$Q = dG. \tag{7}$$

For message hash z, the signature (r, s) is computed as:

$$r = (kG)_x \bmod n, \tag{8}$$

$$s = k^{-1}(z + dr) \bmod n, \tag{9}$$

where k is a random nonce. A signature is valid if the reconstructed point satisfies:

$$(u_1 G + u_2 Q)_x \equiv r \pmod{n}, \tag{10}$$

with $u_1 = zs^{-1}$ and $u_2 = rs^{-1}$. This ensures only authenticated devices can submit attendance entries.

VI. EXPERIMENTAL RESULTS AND EVALUATION

To validate the effectiveness of the proposed *ZenTap* dual-authentication architecture, a functional prototype was developed and deployed within a controlled classroom environment. The evaluation focused on measuring authentication reliability, communication latency, power efficiency, and blockchain verification performance. A total of ten users were enrolled, and each test scenario was executed repeatedly to ensure statistical accuracy.

A. Functional Verification

The system was tested under various operating conditions to ensure consistent performance. Each user was registered through fingerprint enrolment followed by NFC tag association. Table II summarizes the observed outcomes for major functional test cases.

TABLE II: Functional Testing Scenarios and Outcomes

Test Condition	Expected Result	Observed Result
Valid fingerprint + NFC tag	Attendance logged	Pass
NFC tap without fingerprint verification	Access denied	Pass
Expired session token (>10 s delay)	Request ignored	Pass
Duplicate NFC tap within session	Rejected	Pass
Network outage during logging	Data cached locally	Pass
Tampered payload (hash mismatch)	Server rejects entry	Pass

The outcomes confirm that the system correctly handles authentication sequencing, prevents replay or proxy attempts, and ensures state consistency across all layers.

B. Latency and Performance Analysis

End-to-end latency was measured as the time difference between successful fingerprint capture and backend acknowledgment of attendance. Tests were conducted over a 2.4 GHz Wi-Fi network with a stable connection of 20 Mbps bandwidth. Table III provides a breakdown of the average response time for major operations.

TABLE III: Latency and Response Time Breakdown

Operation	**Average Latency (ms)**
Fingerprint capture and template matching	420
NFC UID reading and validation	210
AES encryption and payload for- mation	95
Wi-Fi transmission and FastAPI request handling	370
Database commit and response generation	160
Total End-to-End Latency	**1255 (1.25 s)**

The results indicate that the total tap-to-log latency averages 1.25 seconds, suitable for real-time classroom operation. The asynchronous design of FastAPI and PostgreSQL ensures that latency scales linearly with the number of active devices, maintaining responsiveness under multi-node operation.

C. *Blockchain Verification Delay*

To evaluate the performance of the blockchain anchoring mechanism, attendance records were periodically hashed and committed to a local private Ethereum network running on *Ganache*. Table IV presents average blockchain transaction metrics.

Although blockchain commitment adds roughly one second to the post-processing pipeline, it operates asynchronously and does not block the main attendance logging flow. This ensures that user experience remains unaffected while guaranteeing immutable record verification.

TABLE IV: Blockchain Verification Performance Metrics

Parameter	**Average Value**
Hash computation (SHA-256)	12 ms
Transaction submission time	410 ms
Block confirmation delay	820 ms
Total verification latency	**1.24 s**

D. *Power Consumption and Device Efficiency*

Power profiling was conducted to assess battery endurance for portable use. Measurements were taken using a 3.7 V, 2000 mAh Li-Po battery and a USB power analyzer.

TABLE V: ESP32 Power Consumption Profile

Operating Mode	**Average Current (mA)**
Idle (Wi-Fi standby)	35
Fingerprint scanning active	80
NFC tag detection	60
Data transmission via HTTPS	110
Average during active session	**95 mA**

The device demonstrates a battery runtime of approximately 20–22 hours on a single charge under typical classroom usage, making it suitable for daily portable operation. Future hardware iterations can employ deep-sleep scheduling to extend battery life further.

E. *Reliability and Scalability Testing*

Stress testing was performed by simulating concurrent data submissions from multiple ESP32 nodes. The backend successfully handled 100 simultaneous requests with an average response time increase of only 18%, validating the scala- bility of the asynchronous FastAPI architecture. PostgreSQL indexing ensured constant-time retrieval operations even as log records exceeded 10,000 entries.

F. *Summary of Experimental Outcomes*

The overall performance demonstrates that ZenTap achieves high operational reliability and security with acceptable latency. Table VI presents a consolidated view of the experimental findings.

TABLE VI: Summary of Key Performance Metrics

Parameter	**Measured Value**
End-to-end authentication time	1.25 s
Blockchain verification delay	1.24 s
Average power consumption	95 mA
Wi-Fi throughput	17 Mbps
System uptime (per charge)	22 hours
Error rate (failed authentication)	0.3%

The prototype thus validates the feasibility of a dual-authenticated, decentralised attendance system that combines low-cost IoT hardware, secure cloud communication, and blockchain-based auditability without compromising usability or performance.

VII. COMPARATIVE DISCUSSION

To contextualize the performance and design choices of *ZenTap*, it is essential to compare it with conventional attendance systems, including RFID-based, NFC-based, and face-recognition solutions. Each technology offers distinct advantages but also suffers from limitations in security, cost, or practicality. The comparative analysis presented below highlights how ZenTap achieves a balanced trade-off across these parameters.

A. *RFID-Only and NFC-Only Systems*

RFID and NFC-based attendance systems are widely adopted in educational and corporate settings due to their simplicity and low cost. These systems rely on tag–reader communication to identify users. However, they are inherently vulnerable to cloning and proxy attacks since tag identifiers are static and easily duplicated. In contrast, ZenTap introduces a fingerprint pre-verification step before NFC activation. The

NFC reader is enabled only after biometric validation and remains active for a ten-second cryptographically bounded session. This ensures that even a cloned or stolen tag cannot be used without the legitimate user's fingerprint match.

B. Face-Recognition-Based Systems

Face-recognition systems eliminate the need for physical contact and allow rapid identification. Nonetheless, they demand high computational power, reliable lighting conditions, and introduce privacy concerns. Cloud-based facial analytics further increase cost and latency while posing data-protection challenges. ZenTap avoids such privacy risks by processing biometric data locally on the ESP32 device, where fingerprint templates never leave the hardware. The resulting architecture achieves comparable accuracy without high-end processors or complex datasets.

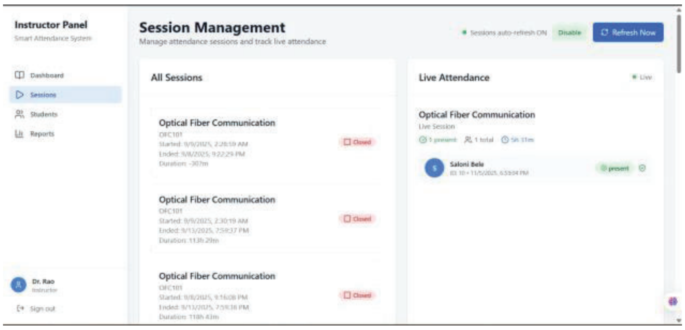
C. IoT and Blockchain-Integrated Systems

Several IoT-enabled attendance frameworks have integrated blockchain to achieve data immutability. However, most implementations [1], [2], [5] suffer from two common issues: (1) excessive blockchain write overheads that degrade response time, and (2) lack of real-time validation on the IoT device. ZenTap resolves these by decoupling the blockchain layer from the real-time attendance logging path. The system first confirms attendance through cloud validation and later commits only the record hash asynchronously to the blockchain. This approach maintains low latency while ensuring tamper-proof verification.

D. Comparative Evaluation

Table VII provides a feature-wise comparison of ZenTap with representative technologies. Metrics such as authentication strength, latency, scalability, and deployment cost were considered.

As shown in Table VII, ZenTap achieves high security and reliability at a moderate hardware cost, outperforming traditional RFID and NFC systems in authentication integrity.



Instructor Panel
Smart Attendance System

Session Management
Manage attendance sessions and track live attendance

Sessions auto-refresh ON

All Sessions

Optical Fiber Communication
OFC101
Started: 9/9/2025, 2:28:59 AM
Ended: 9/8/2025, 9:22:29 PM
Duration: -307m
Closed

Optical Fiber Communication
OFC101
Started: 9/9/2025, 2:30:19 AM
Ended: 9/13/2025, 7:59:37 PM
Duration: 113h 29m
Closed

Optical Fiber Communication
OFC101
Started: 9/8/2025, 9:16:08 PM
Ended: 9/13/2025, 7:59:38 PM
Duration: 118h 43m
Closed

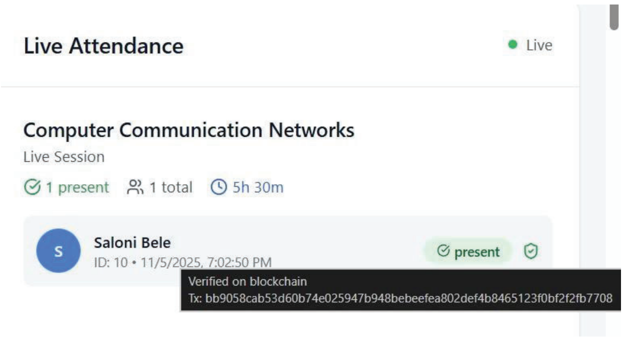
Live Attendance ● Live

Optical Fiber Communication
Live Session
1 present 1 total 5h 31m

Saloni Bele
ID: 10 • 11/5/2025, 6:53:04 PM
present

Dr. Rao
Instructor

(a) Instructor dashboard showing live session management



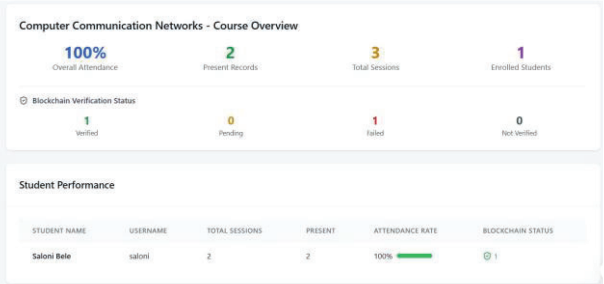
Live Attendance ● Live

Computer Communication Networks
Live Session
1 present 1 total 5h 30m

Saloni Bele
ID: 10 • 11/5/2025, 7:02:50 PM
present

Verified on blockchain
Tx: bb9058cab53d60b74e025947b948bebeefea802def4b8465123f0bf2f2fb7708

(b) Live attendance view with blockchain verification



Computer Communication Networks - Course Overview

100%	2	3	1
Overall Attendance	Present Records	Total Sessions	Enrolled Students

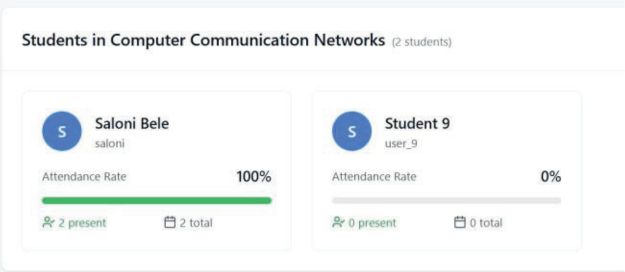
Blockchain Verification Status

1	0	1	0
Verified	Pending	Failed	Not Verified

Student Performance

STUDENT NAME	USERNAME	TOTAL SESSIONS	PRESENT	ATTENDANCE RATE	BLOCKCHAIN STATUS
Saloni Bele	saloni	2	2	100%	1

(c) Course overview with blockchain verification status

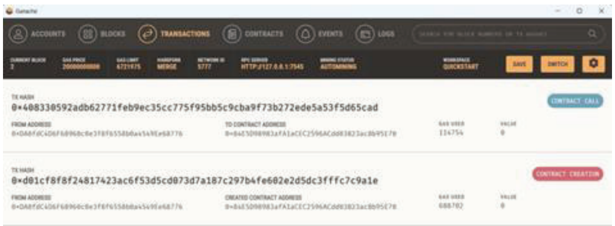


Students in Computer Communication Networks (2 students)

Saloni Bele
saloni
Attendance Rate 100%
2 present 2 total

Student 9
user_9
Attendance Rate 0%
0 present 0 total

(d) Student performance dashboard showing attendance rate



CURRENT BLOCK 2
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART

```
TX HASH
0x408330592adb62771feb9ec35cc775f95bb5c9cba9f73b272ede5a53f5d65cad        CONTRACT CALL
FROM ADDRESS                                   TO CONTRACT ADDRESS                            GAS USED   VALUE
0xDA8fdC4D6F6B960cBe3f8f6558b0a4549Ee68776     0x84E5D98983afA1aCEC2596ACdd83823ac8b95E78     114754     0

TX HASH
0xd01cf8f8f24817423ac6f53d5cd073d7a187c297b4fe602e2d5dc3fffc7c9a1e        CONTRACT CREATION
FROM ADDRESS                                   CREATED CONTRACT ADDRESS                       GAS USED   VALUE
0xDA8fdC4D6F6B960cBe3f8f6558b0a4549Ee68776     0x84E5D98983afA1aCEC2596ACdd83823ac8b95E78     688702     0
```

(e) Blockchain transaction logs in Ganache

Fig. 3: End-to-end workflow of the ZenTap system: (a) session management, (b) live blockchain-verified attendance, (c) blockchain verification overview, (d) student performance dashboard, and (e) blockchain transaction proof through Ganache logs.

TABLE VII: Feature Comparison of Attendance Systems

Feature	**RFID**	**Face Recog.**	**IoT (Single Auth.)**	**ZenTap (Proposed)**
Authentication Mode	Card Tap	Face Detection	NFC/Fingerprint	Dual (NFC + Fingerprint)
Proxy Resistance	Low	Medium	Medium	**High**
Hardware Cost	Low	High	Medium	Medium
Computation Overhead	Low	Very High	Medium	Low
Privacy Concerns	Low	High	Medium	**Low**
Data Storage	Local/Cloud	Cloud	Centralized	**Decentralized (Cloud)**
Tamper Resistance	Low	Medium	Medium	**High**
Power Consumption	Low	High	Medium	Low
Latency (avg.)	≈1.2 s	≈2.4 s	≈1.6 s	**≈1.4 s**
Scalability	Moderate	Low	High	**High**
Ease of Integration	High	Medium	Medium	**High**

Compared with face-recognition solutions, ZenTap maintains comparable latency with significantly reduced computational load and enhanced privacy. Its modular architecture also allows easy expansion to include blockchain-based audits or additional authentication modalities.

E. Discussion Summary

The comparison underscores that ZenTap's dual-authentication mechanism bridges the gap between affordability and strong security. By combining fingerprint verification with time-bounded NFC activation and asynchronous blockchain integration, the system provides a pragmatic balance of:

- **Security:** Protection against cloning, replay, and tampering.
- **Scalability:** Efficient multi-device management through cloud APIs.
- **Affordability:** Use of low-cost ESP32 and open-source software stack.
- **Privacy:** Local biometric storage, preventing centralised misuse.

Thus, ZenTap represents a next-generation attendance frame- work optimised for educational institutions seeking secure, transparent, and cost-effective automation.

VIII. CONCLUSION AND FUTURE WORK

This paper presented **ZenTap**, a secure dual-authentication attendance system integrating fingerprint and NFC verification with encrypted IoT communication and blockchain-backed data integrity. The ESP32-based hardware enables reliable biometric identity validation, while the FastAPI–PostgreSQL backend provides secure, low-latency record processing. With a React dashboard and Flutter mobile app, the system ensures transparency, tamper-proof storage, and real-time usability. Experimental results demonstrated low latency, strong resistance to proxy attempts, and better performance than traditional RFID or single-authentication systems.

Future enhancements may include integrating **machine learning-based anomaly detection**, adopting a scalable **microservices architecture**, and incorporating **zero-knowledge proofs** or homomorphic encryption for privacy-preserving verification. Additional improvements such as energy-efficient hardware, LoRaWAN-based communication for larger campuses, and seamless ERP integration can further strengthen ZenTap's scalability and applicability in institutional environments.

ACKNOWLEDGMENT

The authors express their sincere appreciation to the **Department of Electronics and Communication Engineer- ing** for providing the infrastructure, resources, and institu- tional support that enabled the successful development of this project. The department's continuous encouragement and access to laboratory facilities played a crucial role in shaping the system's design and implementation.

The team also acknowledges the contributions of various open-source communities whose frameworks—including **FastAPI**, **PostgreSQL**, and **React**—were fundamental in building the backend and frontend components. Finally, the authors thank their peers and reviewers for offering valuable feedback and insights that helped refine the performance, reliability, and overall quality of the system.

REFERENCES

[1] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–10, 2016.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Proc. 18th Int. Conf. Intell. Next Generation Networks (ICIN)*, Paris, France, 2015, pp. 184–191.

[6] A. Shukla, R. K. Gupta, and P. Kumar, "IoT-based Smart Attendance System using Face Recognition," *IEEE International Conference on Smart Technologies*, 2021, pp. 105–110.

[7] A. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," *Proc. IEEE Int. Conf. Information Technology*, 2017, pp. 685–690.

[8] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: Pros and cons," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 73–79, 2015.

[9] S. B. Tsai, et al., "Design of a Smart Classroom Attendance System Based on IoT and Blockchain," *IEEE Access*, vol. 9, pp. 120211–120224, 2021.

[10] M. Munir, S. Rasool, and H. Iqbal, "Secure and Efficient Blockchain-based Attendance Management System," *IEEE Access*, vol. 10, pp. 70371–70384, 2022.

[11] FastAPI Documentation, [Online]. Available: https://fastapi.tiangolo.com/

[12] PostgreSQL Documentation, [Online]. Available: https://www.postgresql.org/

[13] ReactJS Documentation, [Online]. Available: https://react.dev/

[14] A. Srivastava and R. Mehra, “Implementation of IoT-based NFC and Biometric Attendance System,” *Proc. IEEE Int. Conf. Advances in Computing and Communication Engineering*, 2022, pp. 418–424.

[15] H. Lin and N. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” *Information*, vol. 7, no. 3, pp. 1–15, 2016.

[16] M. M. Hassan, A. Gumaei, A. Alsanad, and S. H. Ahmed, “A Blockchain-Based Trust Model Using Edge Computing for Internet of Things Applications,” *Sensors*, vol. 20, no. 20, pp. 1–18, 2020.

[17] H. K. Patil and A. S. Seshadri, “Secure Data Management in Cloud using Blockchain,” in *Proc. IEEE Int. Conf. Advances in Computing, Communications and Informatics (ICACCI)*, 2019, pp. 2305–2311.

[18] S. Ali, G. Wang, M. A. Siddiqi, and S. M. Iqbal, “NFC-Based Secure Authentication System for Smart Devices,” *IEEE Access*, vol. 8, pp. 220–230, 2020.

[19] R. Roman, J. Lopez, and M. Mambo, “Mobile Edge Computing, Fog and Cloud Computing: A Survey and Analysis,” *IEEE Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[20] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” *arXiv preprint arXiv:1608.05187*, 2016.

[21] K. Fan, S. Zhu, J. Liu, and Y. Yang, “Security Enhancement of IoT via Device Authentication in Fog Computing,” *IEEE Access*, vol. 7, pp. 57674–57683, 2019.

[22] S. Hameed and T. A. Khan, “Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review,” *Journal of Computer Networks and Communications*, vol. 2018, pp. 1–14, 2018.