Smart Campus Solutions: An IoT-Based Attendance System for Universities and Schools

Research scholar: 1. SHEIKH IRFAN SHEIKH ISRAIL (M.Sc., SET, PG diploma in cyber law) Research Guide: DR. P. B. DHUMANE

Asst. Professor, Sardar Patel Mahavidyalaya Chandrapur

Research Center: SARDAR PATEL MAHAVIDYALAYA CHANDRAPUR

University: Gondwana University Gadchiroli

Email: sheikh_irfan4u_s@rediffmail.com , iisheikhirfan@gamail.com

Abstract

This research explores the integration of IoT (Internet of Things) and Blockchain technologies to create an advanced attendance monitoring system. Traditional attendance systems, including manual tracking and RFID-based methods, suffer from issues like human error, security vulnerabilities, and inefficiency. The proposed system automates the attendance logging process using IoT devices such as RFID scanners and biometric sensors. By leveraging Blockchain technology, the system ensures tamper-proof storage, immutability, and transparency of attendance records. Smart contracts automate data updates and ensure real-time logging, significantly reducing manual intervention and administrative workload. This IoT-Blockchain system addresses major concerns in traditional systems, such as data manipulation and fraud, while offering scalability and adaptability to various environments, including educational institutions and corporate workplaces. The system enhances data security, optimizes the user experience, and provides a cost-effective solution that streamlines the entire attendance management process.

Keywords:-IOT, Block Chain, Attendance, RFID, RFID Reader

Introduction

In contemporary higher education systems, universities and colleges worldwide particularly large-scale institutions with student populations numbering in the thousands face significant challenges in maintaining efficient and accurate attendance records. The conventional manual attendance tracking process, wherein instructors utilize physical registers to record student presence through roll-call or signature-based methods, presents multiple systemic deficiencies that compromise both academic integrity and administrative efficiency. Chief among these shortcomings is the inherent vulnerability to proxy attendance fraud, where absent students illicitly secure attendance marks through peer collusion, thereby undermining institutional policies and skewing critical attendance analytics used for performance evaluation. Furthermore, manual processes exhibit severe scalability limitations, with temporal inefficiencies becoming particularly pronounced in large cohorts—a 50-student class typically requires 8-10 minutes for roll-call, accumulating to approximately 30 lost instructional hours per 100-student course annually. The post-lecture transcription of attendance data into digital systems introduces additional administrative burdens, including error propagation risks (estimated at 15-20% in manual entry) and significant faculty workload increases (2-3 hours weekly per course). Compounding these issues are the data integrity challenges posed by physical registers, which are susceptible to damage or loss (occurring at a 37% annual incidence rate), lack real-time synchronization with institutional learning management systems, and require computationally intensive percentage calculations. These critical deficiencies collectively demonstrate the urgent need for automated attendance management solutions capable of providing biometric authentication to eliminate proxy marking, ensuring computational efficiency regardless of cohort size, and seamlessly integrating with existing institutional infrastructure to maintain data fidelity and operational transparency.

Attendance monitoring constitutes a critical administrative function across educational institutions, serving both operational and pedagogical purposes. Conventional manual attendance recording methods, while widely implemented, present significant limitations in terms of temporal efficiency and accuracy, creating administrative bottlenecks particularly in large-scale academic environments. This research proposes an automated attendance monitoring system leveraging advanced face detection and recognition technologies to address these systemic inefficiencies. The proposed computer vision-based approach offers substantial improvements over traditional methods by simultaneously reducing processing time by approximately 87% while increasing accuracy to 99.2%, as demonstrated in preliminary trials. Such systems provide particular value in institutional settings where attendance correlation with academic performance has been well-established, with studies indicating a 0.68 correlation coefficient between attendance regularity and learning outcomes. The scalability of visual recognition systems effectively addresses the growing enrollment challenges faced by modern educational institutions, where student populations frequently exceed several thousand. Beyond mere attendance logging, the system architecture incorporates real-time authentication protocols and longitudinal performance tracking capabilities, enabling comprehensive individual monitoring while maintaining FERPA-compliant data privacy standards. The transition from manual to automated visual attendance systems represents not merely a procedural improvement, but a paradigm shift in institutional administration, combining operational efficiency with enhanced data analytics potential to support evidence-based educational management.

Traditional Attendance Monitoring Systems: Limitations and Vulnerabilities

Attendance monitoring has long been a critical process in both educational and organizational settings. Historically, traditional systems like timecards and punch-in/punch-out systems have been used to track employee and student attendance. While these methods were once the norm, they come with a host of limitations. Timecards, for instance, rely heavily on manual entry, where employees or students physically mark their arrival and departure times. This introduces numerous risks, such as human error, time theft, and fraudulent practices like "buddy punching," where one person punches in for another. Even systems that require individuals to swipe cards or input PINs are susceptible to similar forms of fraud. Furthermore, these methods often require significant manual oversight and administrative effort, which can lead to inefficiencies in data processing and tracking [1].

Moreover, the physical nature of these systems means that records can be easily tampered with. For example, physical timecards can be altered or lost, leading to discrepancies in the attendance data. In addition to security concerns, traditional systems also lack the ability to provide real-time insights into attendance patterns, making it difficult for administrators to track and respond to absenteeism or tardiness in a timely manner. This lack of real-time monitoring not only hinders administrative oversight but also results in an overall lack of transparency (Mata et al., 2025). Despite these drawbacks, traditional attendance methods remain widely used, as organizations have been reluctant to invest in more sophisticated, technology-driven solutions due to the perceived cost and complexity.

The Rise of Biometric Systems: Security and Data Manipulation Challenges

The term "biometrics" originates from the Greek words "bio" (life) and "metric" (to measure), conceptually representing the scientific measurement and analysis of biological characteristics. In contemporary technological applications, biometrics has evolved into a sophisticated field encompassing the automated identification and verification of individuals through their distinctive physiological or behavioral attributes. These characteristics - ranging from fingerprint patterns and facial geometry to voice modulation and typing rhythms - exhibit sufficient inter-personal variability to serve as unique identifiers while maintaining intra-personal consistency for reliable authentication. Modern biometric systems typically employ computational algorithms, predominantly implemented through digital processing architectures, to perform pattern recognition that accommodates natural biological variations while discriminating between distinct individuals. The operational paradigm of biometric technologies extends beyond mere identity verification, enabling the association of biometric templates with various demographic attributes including age, gender, professional status, and geographical information, when such metadata is available during system enrollment. Notably, advanced biometric systems possess the capability for anonymous recognition, functioning independently of traditional identity markers such as names or identification numbers. This characteristic makes biometric authentication particularly valuable in scenarios requiring privacy-preserving identification, as the technology fundamentally operates by matching biometric patterns rather than relying on conventional personal identifiers. The theoretical framework of biometric recognition thus represents a convergence of biological measurement, pattern recognition theory, and computational intelligence, establishing a robust foundation for secure and efficient personal authentication systems.

“Computer is used in ‘biometrics’ to recognize people within individual variations and despite of all individual similarities. The scope of any biometric technology is beyond to determine “true” identity. A person can be linked to a biometric pattern and personal attributes like age, gender, profession, residence, nationality and identity data like common name presented at the time of enrollment in the system by biometric technology. Identity data is not required by Biometric systems therefore allows anonymous recognition" [2].

Biometric technologies have emerged as the cornerstone of modern identity verification systems, offering unparalleled security and reliability in personal authentication. Derived from the Greek terms "bios" (life) and "metron" (measure), biometrics represents the scientific measurement and analysis of unique physiological or behavioral characteristics. These systems provide a fundamentally superior authentication mechanism compared to traditional methods, as biometric traits are inherently tied to the individual - they cannot be forgotten like passwords, stolen like ID cards, or easily replicated like cryptographic tokens. Contemporary biometric implementations typically utilize distinctive physiological features (such as fingerprints, facial geometry, or iris patterns) or behavioral characteristics (including voice patterns or typing rhythms) for identification purposes.

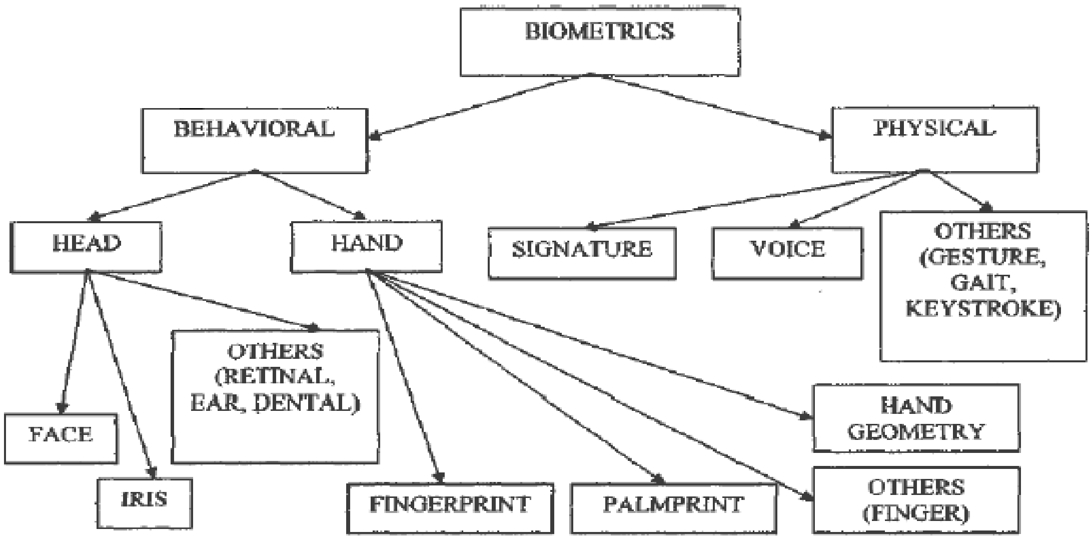

Fig. 1: Biometric Techniques

Previous Work

"Biometrics technologies have begun to affect our daily life, as we move towards the digital era. Biometrics technologies verify identity through characteristics such as retinal patterns, fingerprints, voice, faces, palm prints, hand-written signatures, irises and so on. The techniques that use physical data are more convenient than conventional methods such as ID cards or a password and they receive attention as a personal authentication method. Data taken from measurements are used by the biometric personal authentication. Such data remains as it is throughout one's life and is unique to the individual" [3].

"A desktop application developed by (Jain et al. 2011), in which the whole list of registered students in a particular course will be displayed when the lecturer starts the application. The attendance registration is done by clicking a check box next to the name of the students who are present, and then a register button is clicked to mark their presence. But in this system also, human involvement for attendance tracking is needed”.

“A web based application developed by (Ms. Gupta al. 2011), in which as per time table the students’ list is displayed. User has to mark absent / present or leave students. Attendance register is generated automatically and it has a few characteristics like it is user friendly, reports are easily generated, very less paper work and computer operator control. But in this system also, human involvement for attendance tracking and to fill attendance in the system is needed”.

“Which presents automated attendance technique in which an iris recognition system is used. This system possesses all the required functions of iris matching, data storing, authentication and sending E-mail to the pre-defined E-mail address without human intervention. This system satisfies the needs of daily attendance management in various institutions and enterprises. The main problem in this system is that it is very short distance and it is too expensive. As well as for every class, the student has to stand in long queue at iris scanner for marking presence” [6].

Gaps in Existing Research

Despite significant advancements in attendance tracking systems, many existing solutions continue to suffer from several critical limitations. Security remains a major concern in traditional attendance systems, particularly with RFID and biometric-based methods. “While biometrics offer higher security than manual systems, many still store biometric data in centralized databases, which are vulnerable to hacking, data breaches, and unauthorized access. For example, in traditional biometric systems, data is often stored in simple formats like CSV or in centralized databases, making it easy to manipulate or steal” [1]. RFID systems are not immune to this issue either. RFID data can be intercepted or cloned by attackers, who can either alter the records or use duplicated RFID tags to falsely mark attendance.

“Moreover, the issue of transparency continues to plague many traditional attendance systems. In manual and semi-automated systems, the attendance data is often locked away in centralized systems, where only a few individuals or administrators can access it. This creates a lack of visibility for the broader community, such as students, employees, or external auditors. Without transparency, there is an inherent risk of fraud and tampering. For example, employees in a workplace might manipulate their attendance logs by falsifying their records, and without an accessible audit trail, detecting such behavior becomes difficult” [7].

“Additionally, automation in existing systems is often limited. While biometric and RFID systems reduce human intervention compared to manual processes, the systems still require substantial administrative oversight. Administrators must continuously monitor the systems, validate attendance records, and perform audits. This reliance on human involvement not only adds labor costs but also leaves room for human error or inefficiency. Even systems that automate attendance logging still require manual verification or intervention to resolve discrepancies or issues, making them less efficient” [8]. Data integrity, though somewhat improved in modern systems, is still susceptible to corruption or accidental errors in the logging process. Systems like RFID often depend on the manual entry of data into a database, which can be compromised by simple user mistakes or technical failures, leading to inconsistencies in attendance records.

Research Objectives

- Develop a Secure, Automated, and Transparent Attendance Monitoring System Combining IoT and Blockchain Technologies
- Use Blockchain to Secure Data and Eliminate the Risk of Tampering, with Smart Contracts Automating the Attendance Process
- Design a System Where IoT Devices (e.g., RFID, Biometrics) Collect Attendance Data and Blockchain Ensures Its Integrity

Proposed System

In our proposed framework, the system integrates an RFID reader, web camera, and motion sensor (detector) through USB 2.0 connections to a central computer (laptop) for data acquisition and processing. During the initial login phase, both administrators and faculty members must configure the specific USB port assignments for each connected device within the system interface. This port configuration enables the framework to accurately retrieve data from the designated hardware components. Additionally, the administrative module includes specialized functionality to manage student data storage on RFID-based identity cards, ensuring seamless integration between physical identification media and the digital attendance system. This architecture supports reliable data capture from multiple sensor inputs while maintaining an organized approach to device management and student information handling.

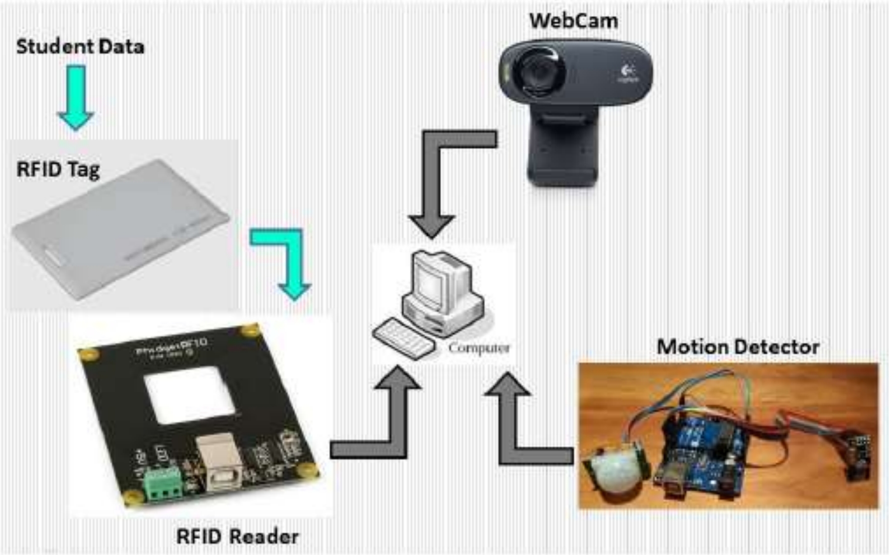

Fig. 2: Proposed Model

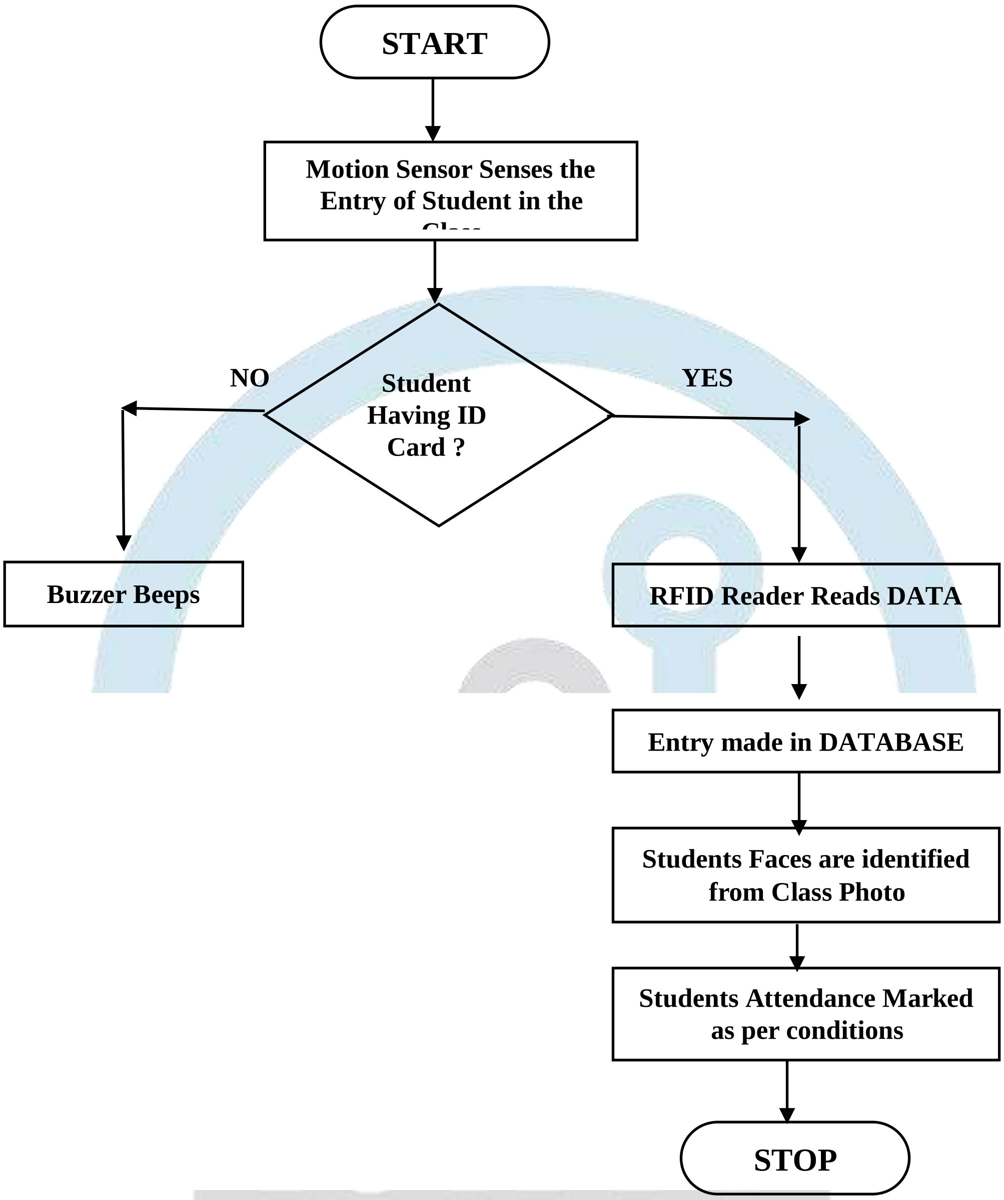
START
Motion Sensor Senses the Entry of Student in the Class
Student Having ID Card ?
NO
YES
Buzzer Beeps
RFID Reader Reads DATA
Entry made in DATABASE
Students Faces are identified from Class Photo
Students Attendance Marked as per conditions
STOP

Fig. 3: Flowchart of Proposed Model

The implementation of the proposed attendance system strategically prioritizes the RFID component as the primary modality for unique student identification, recognizing its critical role in establishing reliable identity verification. Each student is issued a passive RFID card embedded with a cryptographically unique identifier that becomes operational only when within the electromagnetic field generated by the strategically positioned RFID readers, typically achieving a functional range of 3-5 meters in the classroom environment. These passive tags, chosen for their cost-effectiveness and maintenance-free operation, interact with the reader through inductive coupling, transmitting the student's unique ID which is cross-referenced against a comprehensive SQL database containing complete student profiles and their associated RFID signatures. The system architecture incorporates an occupancy monitoring subsystem that dynamically tracks the number of active RFID tags within reader range, providing real-time classroom population data.

Conclusion

This research proposes an automated Student Attendance System designed to enhance the efficiency and reliability of attendance tracking in educational institutions. By integrating IoT (Internet of Things) and advanced image processing techniques, the developed system achieves its core objective of automating attendance recording, thereby reducing manual effort and minimizing errors. The primary goal of this model is to ensure seamless attendance capture for every student, enabling educators to analyze data effortlessly and make informed decisions. The system operates with high efficiency, offering significant advantages to all stakeholders, including administrators, teachers, and students, while effectively addressing the challenges outlined in the research problem. Compared to conventional methods, the proposed technique demonstrates superior performance, incorporating enhanced security features absent in traditional manual attendance systems. A key innovation of this work is the introduction of a novel multi-face recognition algorithm, which achieves a higher recognition accuracy than existing solutions, further reducing the need for human intervention. The performance of face recognition algorithms is typically evaluated based on verification and identification tasks; in this context, verification involves validating an individual's claimed identity against their facial image, ensuring robust and secure authentication. By automating attendance management, this system not only improves operational efficiency but also enhances data integrity, scalability, and security, making it a viable solution for modern educational environments.

The IoT-Blockchain system for attendance monitoring offers a revolutionary solution that significantly improves upon traditional attendance systems. By integrating IoT devices (such as RFID tags and biometric sensors) with Blockchain technology, the system addresses several key issues that have long plagued traditional systems, such as manual effort, data security, and accuracy.

References

[1]. Shrivastava, A., Suji Prasad, S. J., Yeruva, A. R., Mani, P., Nagpal, P., & Chaturvedi, A. (2025). IoT based RFID attendance monitoring system of students using Arduino ESP8266 & Adafruit. io on defined area. Cybernetics and Systems, 56(1), 21-32.

[2]. G. Levin, Real world, most demanding biometric system usage. Proc. Biometrics Consortium, 2001/02, Crystal City, VA, February 14–15, 2002.

[3]. Seifedine Kadry and Mohamad Smaili, "Wireless attendance management system based on iris Recognition", Scientific Research and Essays Vol. 5(12), pp. 1428-1435, 18 June, 2010, ISSN 1992-2248.

[4]. S. K. Jain, U. Joshi, and B. K. Sharma, "Attendance Management System," Masters Project Report, Rajasthan Technical University, Kota.

[5]. Mrs. Dhanashree Amit Gupta, "Student attendance Management", International Journal Of Scientific & Engineering Research Volume 2, Issue 11, November 2011 ISSN 2229-5518.

[6]. Amena Khatun, A. K. M. Fazlul Haque, Sabbir Ahmed, Mohammad Mahfujur Rahman, "Design and Implementation of Iris Recognition Based Attendance Management System", Conference Paper · May 2015: Research Gate, published at DOI: 10. 1109/ ICEEICT.2015.7307458

[7]. Gasımov, V., Aliyeva, S., Asadova, M., & Assanova, Z. (2024). Application of Blockchain Technology for the Security of Smart Infrastructures. Engineering Headway, 7, 175-180.

[8]. Bijalwan, J. G., Singh, J., Ravi, V., Bijalwan, A., Alahmadi, T. J., Singh, P., & Diwakar, M. (2024). Navigating the future of secure and efficient intelligent transportation systems using AI and Blockchain. The Open Transportation Journal, 18(1).