International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Survey on AI-Powered Smart Attendance Systems: Integrating Deep Learning, Computer Vision, and IoT for Enhanced Security and Reliability

Nisha P.K [1] ,Bhavana S Nair [2] ,Aswin Baburaj[3] ,Benson B Varghese [4] ,Aadithyakrishnan K H [5]

[1]*Asst Professor, Dept of CSE , Sree Narayana Gurukulam College of Engineering, Kochi, India*
nisha@sngce.ac.in
[2]*Student, Dept of CSE, Sree Narayana Gurukulam College of Engineering, Kochi, India*
bhavanasnair.1881@gmail.com
[3]*Student, Dept of CSE, Sree Narayana Gurukulam College of Engineering, Kochi, India*
aswinbaburaj004@gmail.com
[4]*Student, Dept of CSE, Sree Narayana Gurukulam College of Engineering, Kochi, India*
bensonbvarghese62@gmail.com
[5]*Student, Dept of CSE, Sree Narayana Gurukulam College of Engineering, Kochi, India*
aadhikalarikal619@gmail.com

Abstract - This project introduces an AI-powered smart employee attendance system that leverages deep learning, computer vision, and IoT technologies to offer a secure, contactless, and reliable solution for modern workplaces. Employees mark their attendance via a mobile application equipped with AI-based facial recognition, which verifies identity using live face data. To ensure authenticity and prevent location spoofing, the system integrates Bluetooth Low Energy (BLE) and Near Field Communication (NFC) modules within the office premises. These IoT components confirm the employee's physical presence, enabling multi-factor verification. The AI layer incorporates liveness detection to counter spoofing attempts and intelligent behavior analysis for detecting anomalies such as frequent late entries. With a seamless backend architecture, real-time validation, and admin dashboard support, the system redefines traditional attendance methods by making them automated, intelligent, and secure.

Key Words: Artificial Intelligence, Deep Learning, Computer Vision, Facial Recognition, Internet of Things (IoT), Smart Attendance, Security, Authentication, BLE, NFC.

1.INTRODUCTION

Automated attendance systems for campuses and workplaces have become a focal point for applying IoT, computer vision, and lightweight security protocols. Two research strands dominate the literature relevant to secure, contactless employee attendance: (i) authentication protocols and RFID based systems that emphasize low-cost secure identity verification; and (ii) vision-based biometric systems, predominantly using deep learning (CNNs) for face detection/recognition and edge deployment for real-time operation. This survey summarizes recent contributions, compares approaches, and highlights open problems for an AI-powered secure contactless attendance system.

A. Background

Attendance systems have also changed tremendously over the years. Originally, manual paper-based systems were very common in which the employees or students would sign physical books to denote their presence. Although easy, these systems were tremendously error-prone, involving misreporting, buddy-punching, and mismanagement of data. With the introduction of technology, early-day digital systems in the form of RFID cards, magnetic swipe systems, and biometric scanners were introduced. These systems provided more precision and efficiency than manual systems. Nevertheless, they also possessed considerable drawbacks: RFID and swipe cards were easily maliciously used or loaned out, while simple biometric systems occasionally malfunctioned under environmental pressures or were subjected to spoofing attacks. These problems revealed the requirement for more secure, automated, and smart attendance options with less human intervention but guaranteed reliability and integrity.

B. Problem Statement

In spite of improvements in digital attendance solutions, there are substantial security and reliability issues. Conventional solutions like RFID cards, magnetic swipes, and simple biometric scanners are easily tampered with. In, for instance, employees or students can evade the system by handing over ID cards or location spoofing, making attendance records inaccurate. Also, environmental noise, technical malfunctions, and spoofing efforts can further lower reliability. These vulnerabilities highlight the requirement for a stronger, automated solution that

blends secure identity verification with real-time monitoring, guaranteeing both authenticity and accuracy in attendance management.

C. Motivation

Current attendance systems are vulnerable to fraud, mistakes, and technology breakdowns, and therefore lack modern requirements. With the post-pandemic era comes the need for touchless solutions to maintain hygiene. Integrating AI-based facial recognition, liveness detection, and IoT-capable BLE/NFC sensors provides secure, automatic, and trusted attendance management for working environments and schools.

D. Contributions

This survey paper aims to:

1. Offer an exhaustive overview of current AI- and IoT-based attendance systems.
2. Critically examine their security and reliability weaknesses.
3. Suggest a conceptual design for a safe, smart, and touchless attendance solution.

2. RELATED WORKS

Throughout history, many technologies have been invented to automate attendance, each with its own advantages and some limitations. In this section, we take a look at four primary types:- RFID, biometric, mobile apps, and location-based systems , explaining how they operate, their strengths, and the security issues they encounter.

A. RFID Based System

RFID-based attendance systems utilize radio frequency signals to verify users, usually through smart cards or tags. For example, the IEEE paper "A New Mutual Authentication Protocol in Mobile RFID for Smart Campus" suggests a protocol that authenticates between readers and RFID tags. It mitigates most common attacks, such as replay, counterfeit, and Man-in-the-Middle (MTM) attacks, with encryption and mutual authentication. Although very effective at enhancing security, RFID systems remain susceptible to card-sharing and need proper protocol design to avoid exploitation.

B. Biometric Systems

Biometric attendance systems rely on fingerprints, iris scans, or facial recognition to identify an individual. They are more secure as they associate attendance with distinctive physiological features, minimizing impersonation. Some biometric systems, though, are contact-based, posing hygiene and privacy concerns. External conditions like lighting or finger damage can disrupt accuracy, and sophisticated spoofing attacks are still problematic.

C. Android/Mobile

Application-based Systems Mobile application-based attendance systems enable users to take attendance through smartphones, usually utilizing credentials or QR codes. They provide ease and live tracking of data but are susceptible to credential sharing, device tampering, and spoofed location data. Such weaknesses make it imperative to have more robust authentication and verification processes in app-based solutions.

D. Location-based Systems

Location-based attendance systems leverage GPS, Bluetooth, or Wi-Fi signals to verify a user's location. Although efficient for remote verification, they are vulnerable to spoofing attacks that simulate location. Moreover, signal interference or hardware limitations can compromise reliability. These factors point to the need to supplement location-based verification with additional secure authentication mechanisms for secure attendance management. From the reviewed literature, it is evident that while each approach, RFID, biometrics, mobile apps, and location-based systems, offers unique benefits, none is entirely foolproof. Security vulnerabilities, ease of manipulation, privacy concerns, and environmental constraints continue to challenge the reliability of these systems. This analysis motivates the development of an integrated, AI- and IoT based attendance framework that combines touchless verification, real-time location validation, and intelligent monitoring to overcome these limitations.

Table -1: summarizes and compares the advantages and limitations of the four main attendance system categories reviewed in this paper.

System Type	Benefits	Limitations
RFID-based	Fast, contact-less, widely used	Vulnerable to card-sharing, cloning; relies on secure protocols
Biometric	High security, unique ID, reduces impersonation	Hygiene concerns, environmental factors affect accuracy, privacy issues, spoofing possible
Mobile App-based	Convenient, real-time tracking, remote monitoring	Credential sharing, device tampering, and fake location data
Location-based	Confirms physical presence remotely, useful for distributed setups	Location spoofing, signal interference, hardware limitations

3. PROPOSED FRAMEWORK

Based on the literature review, a conceptual framework is proposed for an ideal intelligent attendance system that integrates Artificial Intelligence (AI) and Internet of Things (IoT) technologies. The framework aims to enhance the accuracy, reliability, and efficiency of attendance monitoring by combining real-time data acquisition with intelligent decision-making. IoT-enabled sensors and devices facilitate seamless data collection from multiple sources such as RFID tags, biometric scanners, or mobile applications. The collected data is then processed using AI algorithms for identity verification, anomaly detection, and pattern analysis, ensuring secure and automated attendance tracking. This integrated approach not only minimizes manual intervention but also supports scalability, remote access, and real-time analytics for effective management in educational and organizational environments.

A. Conceptual Diagram

The system can be visualized as interconnected modules:

- Mobile App (Front-End): Offers user interface for authentication, captures real-time facial data, and interacts with IoT modules.
- AI / Deep Learning Layer: Facilitates facial recognition, liveness detection, and behaviour analysis to provide safe and accurate verification.
- IoT Layer: Employed hardware devices like ESP32-CAM with BLE and NFC sensors to authenticate physical presence and avoid location spoofing.
- Backend System: Serves as the core repository for real-time validation, secure storage of data, and an admin interface to track attendance.

B. Component Roles

1. Mobile App: Streamlines user interaction and supports real-time data transfer.
2. AI Layer: Validates identity and keeps spoofing or falsification of attendance at bay.
3. IoT Layer: Verifies that the user is physically located at the appointed position.
4. Backend System: Maintains attendance records securely and offers administrative management.

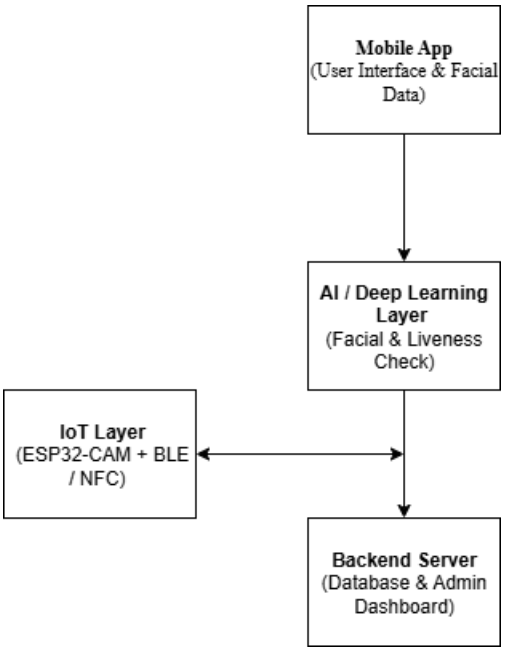

Fig -1:Conceptual framework of an AI-powered contactless attendance system integrating mobile app, IoT modules, and backend processing.

4. SECURITY AND PERFORMANCE ANALYSIS

A. Security Analysis

The suggested AI-driven, IoT-based attendance system works towards meeting the security limitations noticed in systems like RFID-only, QR code, and standalone facial recognition systems. Combining facial recognition with liveness detection and IoT-enabled physical presence verification (BLE/NFC), the system implements a multi-factor authentication system that is strongly resistant against prevalent security attacks.

- Resistance to Spoofing Attacks:
  Single-image facial recognition systems can be spoofed with images, videos, or 3D masks. The addition of liveness detection prevents any other than a live human face from authenticating successfully. Methods such as blink detection, micro-expression detection, or depth sensing add further strength to the system.

- Physical Presence Verification:
  BLE (Bluetooth Low Energy) beacons or NFC tags confirm that the user is on-site at the specified location. It guards against location spoofing, a weakness in GPS-based remote check-ins or attendance, making sure that attendance is recorded only when the user is present on-site.

- Multi-Layer Security:
  By integrating AI-driven biometric authentication with IoT presence confirmation, the system builds two separate layers of verification. Even when one layer is breached, the other still secures the system.

- Data Integrity and Confidentiality:
  Records of attendance, facial templates, and IoT indications are securely transmitted and stored through encryption protocols (AES, TLS, etc.). Role-based backend access control and access control keep unauthorized handling or access to sensitive data at bay.

- Comparison with Existing Systems:
  As opposed to RFID-based systems, which can be cloned or lost, or QR code systems, which are easy to replicate, the new system exploits the uniqueness of biometrics as well as location authentication, thus being tamper-resistant and extremely reliable.

B. Performance Metrics

The architecture is optimized to deliver high performance with security in mind while being practical for mass deployments like universities or corporate campuses.

- High Accuracy:
  Deep learning algorithms (e.g., CNNs, ResNet architectures) provide accurate facial recognition with accuracy rates above 95–98%, even with variations in illumination, pose, or facial expressions. Liveness detection also lowers the false acceptance rate (FAR).

- Fast Authentication:
  Through the utilization of edge computing from mobile devices and streamlined AI models, the system provides instant attendance marking, on average 1–3 seconds per user, to reduce delays in high-traffic spaces.

- Scalability:
  The backend infrastructure, either based on cloud or on-premise servers, is capable of supporting thousands of users at a time, with dynamic load balancing and optimized database management.

- Reliability and Redundancy:
  The two-layer verification eliminates both false negatives (genuine user marked absent) and false positives (incorrect user marked present). IoT modules ensure ongoing monitoring of location-based presence, offering uninterrupted tracking of attendance.

- Energy and Resource Efficiency:
  BLE and NFC modules are power-efficient, and light-weighted AI models guarantee low battery use on mobile devices, making the system viable for daily usage.

Combining AI and IoT in this architecture provides a safe, effective, and scalable attendance solution. In contrast to current methods, it addresses risks such as spoofing, cloning, or location forgery, yet still offers high performance regarding speed, accuracy, and user load.

5. FUTURE SCOPE

Future work can investigate the integration of other types of sensors, such as thermal cameras or motion sensors, to enhance verification abilities. Advances in AI models will potentially enhance recognition reliability in different conditions. The system can be generalized to other applications, such as secure access control, examination authentication, or employee monitoring. Improving the energy efficiency of mobile and IoT devices, adopting cloud-based deployment, and creating smarter attendance analytics are other paths for improving scalability, efficiency, and organizational understanding.

5.CONCLUSIONS

The combination of AI and IoT technologies offers a safe, dependable, and touchless smart attendance solution. By using facial recognition, liveness detection, and BLE/NFC-based presence authentication, the proposed system successfully eliminates weaknesses found in conventional and current digital attendance systems. The system offers high accuracy, real-time verification, and support for large-scale organizations, together with improved data integrity and fewer false positives and negatives. In all, the integration of deep learning, computer vision, and IoT sets a strong and smart solution for contemporary attendance management.

REFERENCES

[1] H. Tiwary, "Live Attendance System via Face Recognition," Int. J. Recent Advances in Science, Engineering and Technology (IJRASET), vol. 6, no. 4, pp. 3891–3897, Apr. 2018.

[2] N. Dalal and B. Triggs, "Histogram of oriented gradients for human detection," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 1, pp. 886–893, 2005.

[3] S. A. Korkmaz, A. Akçiçek, H. Bınol, and M. F. Korkmaz, "Recognition of the stomach cancer images with probabilistic HOG feature vector histograms by using HOG features," in Proc. IEEE Int. Symp. Intell. Syst. Informatics (SISY), pp. 339–342, 2017.

[4] A. L. Machidon, O. M. Machidon, and P. L. Ogrutan, "Face recognition using Eigenfaces geometrical PCA approximation and neural networks," in Proc. Telecommun. Signal Process. (TSP), 42nd Int. Conf., pp. 80–83, 2019.

[5] N. Faruqui, M. A. Yousuf, and M. F. K. Patwary, "Automatic examinee validation system using Eigenfaces," in Proc. Int. Conf. Advances in Sci. Eng. Robotics Technol. (ICASERT), pp. 1–7, 2019.

[6] V. R. P. Rao, C. A. H. Puwakpitiyage, D. A. Shafiq, F. Islam, D. O. D. Handayani, H. Yacoob, and T. Mantoro, "Design and development of facial recognition-based library management system (FRLMS)," in Proc. Int. Conf. Comput. Eng. Design (ICCED), pp. 119–124, 2018.

[7] K. Puthea, R. Hartanto, and R. Hidayat, "A review paper on attendance marking system based on face recognition," in Proc. Int. Conf. Inf. Technol. Inf. Syst. Elect. Eng. (ICITISEE), pp. 304–309, 2017.

[8] N. Suri, M. Marne, M. Ghotekar, and U. Pacharaney, "Design of facial features-based hospital admission using GSM," in Proc. Int. Conf. Inventive Comput. Technol. (ICICT), vol. 1, pp. 1–6, 2016.

[9] A. Geitgey, "Modern face recognition with deep learning," 2016.

[10] Codacus, "OpenCV face recognition," Nov. 2016.

[11] OpenCV, "Face detection using Haar cascades," 2016.

[12] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cogn. Neurosci., vol. 3, no. 1, pp. 71–86, 1991.

[13] L. Yongzhi, "Image feature extraction method and its application in face recognition," Ph.D. dissertation, Nanjing Univ. of Sci. and Technol., China, 2000.

[14] R. Guan, "Based on the study of landscape pattern evolution and monitoring technology in 3S Dalinuoer National Nature Reserve," M.S. thesis, Inner Mongolia Agricultural Univ., China, 2000.

[15] J. Qu, "Design and implementation of mobile phone attendance management system based on mobile

[16] J. Paziewski, R. Sieradzki, and R. Baryla, "Signal characterization and assessment of code GNSS positioning with low-power consumption smartphones," GPS Solutions, vol. 23, no. 4, pp. 98, 2000.