Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

An Educational ERP System That Records the Students' Attendance in an Institution

[1] S.Santhi Priya,[2] G.Pavannadh,[3] K.Sai Sindhuja,[4] SK.Mansoor, [5] P.Brahmeswarao

[1]Assoc. Professor, Department of CSE- AI

[2,3,4,5] UG Scholar, Department of CSE- AI

Chalapathi Institute of Technology, Guntur, Andhra Pradesh, India-522016

ABSTRACT

The Automated Attendance Management System revolutionizes attendance tracking by leveraging machine learning and real-time facial recognition. Traditional methods, such as manual registers and standalone biometric systems, often lead to inefficiencies, errors, and security vulnerabilities. To overcome these limitations, the system integrates Open CV, deep learning models (CNNs), Python, and Streamlit to ensure accurate and seamless attendance recording. By continuously analyzing facial features and matching them against a stored database, it eliminates the risks of proxy attendance and manual entry errors, ensuring a secure and automated process. A key feature of the system is its real-time facial recognition capability, which processes live video feeds to detect and verify individuals instantly [21]. Machine learning models trained on diverse datasets enhance accuracy, adapting to variations in lighting, angles, and facial expressions. The system automatically marks attendance upon successful recognition and triggers alerts for unauthorized individuals or anomalies [20]. Additionally, it provides detailed analytics, including absentee trends, latecomer statistics, and department-wise attendance breakdowns. The system's interactive dashboard, powered by Streamlit, offers a user-friendly interface for monitoring attendance records, generating reports, and visualizing data insights in real time [23].

To ensure scalability and security, the system supports cloud-based storage for large-scale deployment and encryption protocols to protect biometric data. Future enhancements include mobile-based attendance tracking, multi-factor authentication, and AI-powered behavioral analytics to detect anomalies in attendance patterns [14]. By combining advanced face recognition technology with a robust architecture, the Automated Attendance Management System sets a new standard for attendance tracking across diverse environments.

***Keywords**: Open CV, deep learning models, monitoring attendance records, protect biometric and cloud-based storage.*

1. INTRODUCTION

The increasing reliance on technology in educational institutions and corporate environments has led to significant advancements in attendance tracking methods. Traditional attendance systems, such as manual registers and standalone biometric devices, often present inefficiencies, inaccuracies, and security vulnerabilities [10]. Manual processes require substantial administrative effort and are prone to errors, including proxy attendance, data loss, and incorrect markings. The demand for a robust and automated solution has become essential to ensure accuracy, security, and efficiency in attendance management. The Automated Attendance Management System leverages machine learning, real-time facial recognition, and database management to provide a highly accurate and secure attendance tracking system [2]. By integrating Open CV, deep learning models (CNNs), Python, and Streamlit, this system eliminates the challenges associated with traditional methods and enables seamless, contactless attendance recording with minimal manual intervention. The system captures and processes facial features in real time, authenticates individuals, and securely updates attendance records in a structured SQL database [3]. This approach significantly enhances accuracy, prevents

unauthorized access, and eliminates the need for manual record-keeping. Designed for scalability, the system can be effectively implemented across various domains, including educational institutions, corporate offices, public events, and healthcare facilities. In educational settings, it automates student attendance tracking, reduces the administrative workload of teachers, and ensures real-time attendance verification [20]. In workplaces, it helps organizations maintain accurate records of employee attendance while enhancing security and payroll efficiency [15]. Additionally, this system is valuable for event management and healthcare applications, where real-time identification and access control are essential.

While the system provides a highly efficient and secure attendance tracking mechanism, continuous improvements are essential to enhance its performance and adaptability. Future enhancements may include the integration of mobile applications to allow remote check-ins for hybrid workplaces and online learning [17]. Additional security layers such as multi-factor authentication can be implemented by combining facial recognition with QR codes or PIN-based verification. The introduction of GPS-based geo-fencing would further ensure that attendance is recorded only within designated locations, preventing misuse of the system. Advanced AI-driven analytics can also be incorporated to detect patterns in attendance behavior, enabling organizations to make informed decisions and optimize their workforce or student engagement strategies [18]. The Automated Attendance Management System represents a significant technological advancement in attendance tracking, offering a scalable, accurate, and efficient alternative to traditional methods. By leveraging real-time facial recognition, machine learning algorithms, and secure database management, it eliminates the need for manual intervention and reduces administrative burdens [11]. The contactless nature of the system also ensures hygiene and safety, particularly in post-pandemic environments where minimizing physical interaction is a priority [19]. As institutions and organizations continue to seek efficient solutions for attendance tracking, this system provides an innovative approach that aligns with modern technological advancements and automation trends [15]. Its adaptability across various sectors, combined with its potential for future enhancements, makes it a powerful tool for the digital transformation of attendance management systems.

The implementation of this system is based on an efficient architecture that ensures real-time data processing and secure record storage [14]. The facial recognition model is trained on a diverse dataset to account for different lighting conditions, facial angles, and variations in appearance, making it robust and adaptable for various real-world scenarios [17]. The integration of an SQL-based database allows for structured and organized storage of attendance records, enabling instant retrieval, report generation, and analytics for decision-making [19]. Administrators can monitor attendance trends through an interactive dashboard, where they can filter data by department, date, or individual records. The system also supports automated notifications, alerting authorities in case of absenteeism, irregularities, or unauthorized access attempts.

2. EXISTING SYSTEM

The primary objective of an attendance system is to maintain accurate records of an individual's presence, ensuring accountability and productivity. Traditionally, attendance was recorded manually using paper-based registers or logbooks, where individuals would sign their names or check-in through supervisors. While this method was simple and widely used, it had significant drawbacks, including errors, data loss, and manipulation [18]. With advancements in technology, the need for an automated and error-free attendance management system became evident, leading to the development of various digital solutions. Attendance tracking is essential in educational institutions, workplaces, and event management to ensure accuracy and accountability. Traditional methods, such as manual registers, are prone to errors and inefficiencies [19]. The demand for automation has led to digital attendance solutions that improve accuracy and security. Modern attendance systems use RFID, biometric authentication, and facial recognition to streamline processes. These technologies reduce

human intervention, enable automation, and integrate with HR and payroll systems. Advancements in machine learning and AI further enhance recognition capabilities, making attendance management more reliable [20]. Existing Attendance Management Methods early automated methods included RFID-based systems, where users scanned cards for attendance. While faster than manual tracking, they are vulnerable to card loss and misuse [21]. QR code-based systems offer similar functionality but still require manual effort. Biometric-based methods, such as fingerprint, iris, and facial recognition, provide higher security [22]. Fingerprint recognition is widely used but requires physical contact, raising hygiene concerns. Facial recognition, powered by computer vision, offers a contactless and secure alternative, making it suitable for large-scale use [23]. Challenges in Traditional Approaches Manual attendance tracking is time-consuming and prone to proxy attendance. It also requires constant supervision, making it inefficient for large organizations. Additionally, traditional systems lack automation and scalability, making it difficult to retrieve and analyze attendance records. These challenges have led to the adoption of biometric authentication, AI-driven facial recognition, and cloud-based storage for improved accuracy and security [21]. Research on automated attendance systems has explored various technologies. RFID systems reduce time but rely on external hardware. Fingerprint systems offer security but require physical contact, making them less practical in modern settings. Recent studies emphasize facial recognition-based attendance systems using Convolutional Neural Networks (CNNs). Cloud-based solutions further enhance scalability and automated reporting, improving attendance tracking efficiency.

Traditional attendance methods, including manual registers, RFID-based systems, and fingerprint scanners, have long been used but come with significant drawbacks [15]. Manual registers are error-prone and time-consuming, RFID cards can be lost or swapped, and fingerprint scanners require physical contact, raising hygiene concerns [18]. These systems lack real-time updates, scalability, and security, making it difficult to manage large attendance records efficiently [11]. Additionally, biometric methods may fail in poor environmental conditions, further limiting their reliability. A contactless, automated solution is needed to address these challenges.

3. PROPOSED SYSTEM

The Automated Attendance Management System overcomes these limitations by using facial recognition, real-time data processing, and cloud storage. Cameras or webcams capture facial images, which are processed using deep learning models to verify attendance instantly. This ensures a contactless, secure, and fraud-proof attendance tracking system [22]. The system integrates Open CV for image processing, CNNs for facial recognition, and SQL databases for efficient record management. An interactive dashboard allows administrators to monitor attendance in real time, improving decision-making and scalability for schools, offices, and events. Advantages of the Proposed System: The system's contactless nature eliminates hygiene concerns associated with fingerprint scanning and manual registers [13]. Facial recognition prevents proxy attendance, ensuring high accuracy in attendance tracking. Additionally, real-time updates and cloud-based storage enable instant access to attendance records. Machine learning models enhance recognition accuracy under varied lighting conditions, making the system secure, scalable, and highly efficient for modern institutions.

4. SYSTEM DESIGN

One of the primary concerns in attendance tracking is proxy attendance (buddy punching), where an unauthorized person marks attendance on behalf of someone else. Facial recognition minimizes this risk through advanced security techniques [21]. Liveness Detection & Anti-Spoofing Blink Detection & Micro-Movement Analysis Ensures real-time facial movements to detect live individuals.3D Depth Sensing Uses infrared-based depth analysis to prevent spoofing with printed

photos or mobile screens [10]. Texture & Reflection Analysis – Identifies flat surfaces to distinguish between real faces and fake images/videos. Multi-Face Recognition Prevention Ensures one-person-per-frame detection to prevent multiple users from marking attendance simultaneously [23]. Rejects images with overlapping faces or suspicious patterns using bounding box verification [20]. Secure Attendance Logging Uses tamper-proof database storage with cryptographic hashing (SHA-256, AES) to prevent attendance record modification. Blockchain-based logging ensures immutability and verification of attendance records [17]. Data Encryption & Privacy Policies Facial recognition systems handle sensitive biometric data, requiring strong encryption, anonymization, and policy enforcement to protect user privacy [14]. End-to-End Data Encryption AES-256 & RSA Encryption – Secures facial recognition data during transmission and storage. Secure Socket Layer (SSL/TLS) – Protects real-time communication between the system and cloud databases. Hashed & Salted Facial Data – Instead of storing raw images, facial embeddings are encrypted before storage.

Compliance with Privacy Laws: Ensures adherence to global data protection laws like: General Data Protection Regulation (GDPR – Europe) California Consumer Privacy Act (CCPA – USA) Personal Data Protection Bill (India) Provides user consent mechanisms, allowing individuals to opt-in or request data deletion. Access Control & Anonymization Role-Based Access Control (RBAC) – Restricts system access to authorized personnel (e.g., only admins can edit records). Facial Data Masking – Stores only feature embeddings instead of complete facial images to enhance privacy. Data Expiry & Automatic Deletion – Implements a data retention policy to delete old records after a predefined period. Multi-Factor Authentication (MFA) to enhance security, Multi-Factor Authentication (MFA) ensures that only authorized individuals can access or modify attendance records. Authentication Methods Facial Recognition + PIN or Password – Users must verify identity with an additional PIN/password for access. Facial Recognition + QR Code Scanning – A unique QR code is generated and scanned along with face recognition. Facial Recognition + NFC or RFID Cards Combines biometric verification with physical ID validation. one-Time Password (OTP) Verification. OTP-based verification ensures secure logins for new device access or attendance modifications. OTPs can be sent via SMS, email, or authentication apps (Google Authenticator, Twilio). Adaptive Authentication Uses AI-based risk assessment to dynamically adjust security levels based on User behavior patterns (e.g., login from a new device triggers additional verification). Geo-location verification (e.g., attendance can be marked only within the organization's premises).

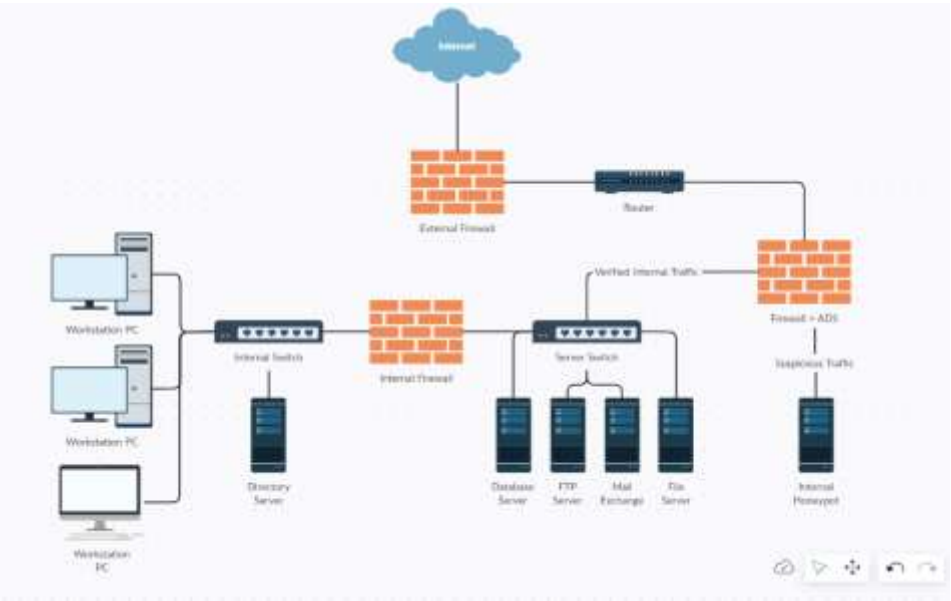

Fig1: System Design

4.1. System Components and Features:
Rule Configuration: Define inbound and outbound rules for traffic based on customizable criteria.
Packet Inspection: Inspect packets against rules to block or allow traffic dynamically. Traffic Visualization: Real-time dashboards enhance monitoring of rule effectiveness and traffic trends [17]. Dynamic Rule Prioritization: Optimize rule execution to minimize resource consumption and maximize efficiency. Advanced Logging: Maintain detailed logs of all network activity for security audits and threat analysis [22].

5. CONCLUSION

Through this paper, the following key findings were observed accuracy & Efficiency – The use of Convolutional Neural Networks (CNNs) significantly improves facial recognition accuracy compared to traditional methods. Automation & Time-Saving – Reduces the manual workload for attendance tracking, allowing instant authentication [8]. Security & Anti-Fraud Mechanisms. The system prevents proxy attendance using liveness detection and multi-factor authentication. Scalability & Adaptability supports cloud-based deployment, mobile integration, and multi-location attendance tracking. Impact on attendance management [6]. The introduction of facial recognition-based attendance systems has a significant impact on how organizations handle attendance records. Improved Accuracy & Fraud Prevention eliminates human errors, proxy attendance, and data manipulation [2]. AI-based pattern recognition ensures real-time validation. Increased Productivity & Efficiency reduces manual effort by automating attendance logging and reporting. Cloud-based integration enables remote access to attendance data. Cost-Effectiveness & Scalability saves costs by removing dependency on RFID cards, fingerprint scanners, and manual record-keeping. Can be expanded to multiple locations and institutions without additional infrastructure requirements.

.

REFERENCE

[1] S Deepajothi, Kalyankumar Dasari, N Krishnaveni, R Juliana, Neeraj Shrivastava, Kireet Muppavaram, “Predicting Software Energy Consumption Using Time Series-Based Recurrent Neural Network with Natural Language Processing on Stack Overflow Data”, 2024 Asian Conference on Communication and Networks (ASIANComNet), Pages:1-6, Publisher: IEEE.

[2] "Predicting Customer Churn with Machine Learning – A Systematic Review": https://arxiv.org/abs/2001.01537,

[3] Kalyankumar Dasari, Mohmad Ahmed Ali, NB Shankara, K Deepthi Reddy, M Bhavsingh, K Samunnisa, “A Novel IoT-Driven Model for Real-Time Urban Wildlife Health and Safety Monitoring in Smart Cities” 2024 8th International Conference on I-SMAC, Pages 122-129.

[4] "Deep Learning for Customer Retention in Subscription-Based Services": https://www.sciencedirect.com/science/article/pii/S095741742100587X.

[5] Dr.D.Kalyankumar, Muhammad Shaguftha, Putti Venkata Sujinth, Mudraboyina Naga Praveen Kumar, Namburi Karthikeya, “Implementing a Chatbot with End-To-End Encryption for Secure and Private Conversations”, IJMTST, Vol: 10, Issue: 02, Pages:130-136, 2024.

[6] Kommineni, K. K., Pilli, R. B., Tejaswi, K., & Siva, P. V. (2023). Attention-based Bayesian inferential imagery captioning maker. Materials Today: Proceedings.

[7] Kalyan Kumar Dasari, K Dr , "Mobile Agent Applications in Intrusion Detection System (IDS)ʻ- JASC, Vol: 4 Issue : 5, Pages: 97-103, 2017.

[8] V.Monica, D. Kalyan Kumar, "BACKGROUND SUBTRACTION BY USING DECOLOR ALGORITHM", IJATCSE, Vol. 3 , No.1, Pages : 273 – 277 (2014).

[9] Netflix Prize Dataset (User behavior and ratings): https://www.netflixprize.com

[10] Kaggle : Customer Churn Prediction Datasets: https://www.kaggle.com/datasets

[11] Kalyan Kumar Dasari & Dr, K Venkatesh Sharma, "A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework", JASRAE, vol : 11, Pages: 209-214, 2016.

[12] Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao, GanugapantaVenkata Pavan Reddy, "Build a Tool for Digital Forensics to Analyze and Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.

[13] Dr.D.Kalyankumar, Kota Nanisai Krishna, Gorantla Nagarjuna, PuvvadaVenkata Naga Sai Jagadesh Kumar, Modepalli Yeswanth Chowdary, "Email Phishing Simulations Serve as a Valuable Tool in Fostering a Culture of Cyber security Awareness", IJMTST, Vol: 10, Issue: 02, Pages:151-157, 2024.

[14] Dr.D.Kalyankumar, Panyam Bhanu Latha, Y. Manikanta Kalyan, Kancheti Deepu Prabhunadh, Siddi Pavan Kumar, "A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System", IJMTST, Vol: 10, Issue: 02, Pages:110-116, 2024.

[15] Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun (2024). https://doi.org/10.1007/s11277-024-11635-w

[16] Kumar, K. K., Kumar, S. G. B., Rao, S. G. R., & Sydulu, S. S. J. (2017, November). Safe and high secured ranked keyword searchover an outsourced cloud data. In 2017 International Conference on Inventive Computing and Informatics (ICICI) (pp. 20-25). IEEE.

[17] Dr.K.Sujatha, Dr.Kalyankumar Dasari , S. N. V. J. Devi Kosuru , Nagireddi Surya Kala , Dr.

Maithili K , Dr.N.Krishnaveni, " Anomaly Detection In Next-Gen Iot:Giant Trevally Optimized Lightweight Fortified Attentional Convolutional Network," Journal of Theoretical and Applied Information Technology, 15th January 2025. Vol.103. No.1,pages:22-39.

[18] Kalyankumar Dasari*, Dr. K. Venkatesh Sharma, "Analyzing the Role of Mobile Agent in Intrusion Detection System", JASRAE, vol :15, Pages: 566-573,2018.

[19] Kalyan Kumar Dasari&amp, M Prabhakar, "Professionally Resolve the Password Security knowledge in the Contexts of Technology", IJCCIT, Vol:3, Issue:1, 2015.

[20] Kommineni, K. K. ., & Prasad, A. . (2023). A Review on Privacy and Security Improvement Mechanisms in MANETs. International Journal of Intelligent Systems and Applications in Engineering, 12(2), 90–99. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4224

[21] S Neelima, Kalyankumar Dasari, A Lakshmanarao, Peluru Janardhana Rao, Madhan Kumar Jetty, "An Efficient Deep Learning framework with CNN and RBM for Native Speech to Text Translation", 2024 3rd International Conference for Advancement in Technology (ICONAT), Pages: 1-6,Publisher :IEEE.

[22] A Lakshmanarao, P Bhagya Madhuri, Kalyankumar Dasari, Kakumanu Ashok Babu, Shaik Ruhi Sulthana, "An Efficient Android Malware Detection Model using Convnets and Resnet Models", 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Pages :1-6, Publisher :IEEE.

[23] Churn Prediction in Subscription- Based Busi ness es Using Machine Learning", https://www.science "Customer direct.com/science/article/pii/S18770509193155.