Arjun Manoj, 2026, 14:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

IoT Based Smart Visitor Entry and Monitoring System for College Campuses

Arjun Manoj, Christin Benny, Ninz Milka Loji, Sona Anna Koshy, Dr. Abin T. Abraham

Department of Computer Applications Saintgits College of Engineering Kerala, India

Abstract- In educational institutions, hospitals, corporate of- fices, and other secure environments, the conventional handwrit- ten visitor register system poses significant challenges including manual errors, lack of verification, time-consuming processes, and inadequate security measures. The IoT-based Smart Visitor Entry System addresses these critical issues by introducing a fully automated, secure, and efficient digital solution that transforms visitor management through modern technology. The system operates through an intuitive touchscreen kiosk interface on an Android tablet. As soon as a visitor approaches the kiosk, a webcam integrated with facial recognition technology powered by OpenCV automatically captures their photograph and scans the database for matching records. If the visitor has previously registered, their name and phone number are automatically retrieved and pre-filled in the form, significantly reducing entry time and enhancing user convenience. For first-time visitors, the system prompts them to manually enter their name and phone number. In both cases, visitors must specify their purpose of visit. To ensure authenticity, an OTP (One-Time Password) is sent to the visitor's registered phone number for verification. Upon successful OTP validation, the entry is logged with a timestamp, creating a comprehensive digital record of each visit. The software architecture is built using Python and the Flask web framework for backend operations. OpenCV enables real- time face detection, facial recognition, and image capture. All visitor data are securely stored in a local SQLite database. A key feature is the administrator dashboard, which provides authorized personnel with complete control and visibility over visitor records. The system enhances security by addressing mul- tiple vulnerabilities in traditional visitor management through facial recognition, real-time OTP verification, and comprehensive digital audit trails, significantly improving operational efficiency while enhancing security and accountability.

Keywords: IoT, Visitor Management, Facial Recognition, OpenCV, Flask, OTP Authentication, Campus Security, Deep Learning.

I. INTRODUCTION

The IoT-Based Smart Visitor Entry System replaces manual logbooks with a secure, automated digital kiosk on an Android tablet. Visitors register or check in via a touchscreen interface that captures their facial image using OpenCV, while returning visitors are identified automatically. OTP verification through the 2Factor SMS Gateway ensures authenticity, and all visitor details—name, contact, purpose, timestamp, and photo—are stored in a SQLite database. Built with Python (Flask) for backend management and HTML/CSS/JavaScript for the fron-tend, the system enables administrators to monitor visits in real time, verify identities visually, and generate reports. By integrating facial recognition, OTP verification, and digital logging, it enhances security, reduces manual effort, and is suitable for institutions, offices, and other secure facilities.

II. RELATED WORK

IoT-Based Reading Room Visitor Monitoring: Napitu [1] proposed an IoT-based visitor monitoring tool for reading room environments. The system used a NodeMCU ESP8266 microcontroller along with ultrasonic and PIR sensors to track the number of visitors entering and leaving the room. Results were displayed on an LCD as well as on a mobile application, with green/red indicators and a buzzer for room availability. The system achieved a very low average error rate of 0.031, proving its reliability. This study demonstrates the feasibility of IoT-based visitor monitoring but is limited to simple occupancy detection without identity verification.

Smart Bi-Directional Visitor Counter System: Kishor et al.

[2] introduced a smart bi-directional visitor counter using IoT with data analytics and regression models. Designed for scenarios where a single door serves as both entry and exit, the system tracked visitor flow dynamically and performed predictive analysis to identify peak hours and visitor trends. The real-time data supported better resource allocation and improved space utilization. While highly effective for single- door tracking, the system mainly focused on visitor counts and did not include identity verification or security enhancements.

Integrated Visitor Management with Smart Hand Sanitizer: Hafidz et al. [3] developed an integrated visitor management system with smart hand sanitizer based on IoT approach, par- ticularly relevant during the COVID-19 pandemic. The system used Arduino Uno R3 with ultrasonic sensors and ESP8266 Wi-Fi modules, connected to the ThingSpeak web server and MIT App for real-time monitoring. It successfully controlled visitor flow while ensuring hygiene by dispensing sanitizer automatically. Although innovative in combining health safety with visitor tracking, this solution was tailored to pandemic needs and lacked features like OTP verification or biometric validation.

Intelligent Visitor System with Cloud-Edge Computing: Zhao et al. [4] proposed an intelligent visitor system utilizing AI-driven cloud-edge collaborative computing. The system integrated face recognition, voice interaction, ID card scan- ning, and body temperature measurement using Rockchip RK3399 hardware and Baidu AI cloud services. This approach addressed limitations of manual visitor logs by ensuring data authenticity, real-time monitoring, and multi-modal verifica- tion. While this system demonstrated high intelligence and automation, it required more expensive hardware and cloud integration, making it less suitable for small-scale, low-cost institutions.

Intelligent Crowd Monitoring Middleware: Gazis and Kat- siri [5] introduced an intelligent crowd monitoring middleware solution leveraging Raspberry Pi devices and wireless sensor networks. The RFID-based system for crowd monitoring in indoor environments like museums and historical buildings applied MapReduce algorithms for distributed data collection, ensuring scalability and fault tolerance with leader election mechanisms. Tested successfully in a real-world setting, it provided accurate occupancy data and evacuation support at low cost. However, the system mainly focused on crowd movement and density analysis rather than secure visitor identity management.

VISITX – Face Recognition Visitor Management: Satari et al. [6] presented VISITX, a face recognition visitor manage- ment system aimed at improving security in organizations. The system replaces manual logbooks with automated facial authentication at entry, comparing live images against a stored database and issuing printed visitor passes after successful verification. Using image processing and Dlib-based face landmark detection, the authors argue that their approach offers stronger security than traditional barcode or gate-based methods. However, the solution is primarily focused on facial biometrics and does not deeply address multi-factor verifica- tion such as OTP or ID document checks.

CNN-Based Visitor Management System: Prabhulkar et al.[7] proposed a CNN-based visitor management system using convolutional neural networks for face recognition. The system replaces manual registration by capturing a visitor's image at the entrance, encoding facial features using deep learning, and matching them against a database to automate identification and logging. This approach improves accuracy and reduces the chances of impersonation compared to traditional ID-based systems. Despite its use of deep learning, the work mainly targets controlled environments and does not explicitly tackle scalability or integration with existing organizational security infrastructure.

Smart Visitor Management for Residential Complexes: Singh et al. [8] designed a smart visitor management system for residential complexes focusing on both security and com- munication. The system digitizes guest registration, maintains a

centralized log of all visits, and notifies residents in real time when a visitor arrives, reducing dependence on manual gate registers. By leveraging web and mobile technologies, it enhances traceability of visitors in gated communities and simplifies approval workflows. However, the solution is tai- lored to residential settings and does not include advanced biometric verification or specialized hardware for high-security institutional environments.

Dynac Visitor Management with Facial Recognition: Abd Hafiff et al. [9] developed a visitor management system with facial recognition specifically for industrial deployment. The Dynac system automates check-in by capturing a visitor's face, performing recognition, and recording visit details in a database, thereby speeding up registration and improving security over paper-based methods. It demonstrates practical deployment of face recognition in an industrial setting, with an interface designed around a single company's workflow. While effective for that environment, the system is customized to one organization, and the paper does not extensively explore interoperability with other access control systems.

IoT-Based Counting System: Several researchers [10] pro- posed IoT-based counting systems that combine sensor data and cloud technologies to monitor occupancy in public spaces. These systems count individuals entering and exiting an area while also capturing facial data, then uploading the information to a cloud platform for real-time visualization and analytics—particularly motivated by COVID-19 crowd control requirements. This work shows how IoT and cloud integration can support dynamic capacity management and safety monitoring. However, the main focus is on counting and occupancy; identity management, strong authentication, and detailed visitor profiling are not addressed in depth.

UWB Radar-Based People Detection: Matuska et al. [11] introduced a UWB radar-based people detection system using ultra-wideband radar sensors and signal-processing algorithms to estimate the number of people in both indoor and out- door spaces. Instead of cameras, the system relies on radar reflections, which helps preserve privacy while still providing accurate people counts under varying conditions. The authors report improved robustness compared to earlier sensor-based methods and highlight applications such as public-space mon- itoring and social-distancing enforcement. The solution, however, is deliberately device-free and anonymous; it does not attempt to identify individuals, issue credentials, or integrate with visitor registration workflows.

III. PROPOSED SYSTEM

The proposed IoT-Based Smart Visitor Entry System aims to overcome the limitations of traditional visitor management methods by introducing a fully automated, secure, and in- telligent digital platform. Instead of maintaining handwritten registers, the system uses an interactive Android-based kiosk integrated with a webcam and backend server to record and manage visitor entries efficiently.

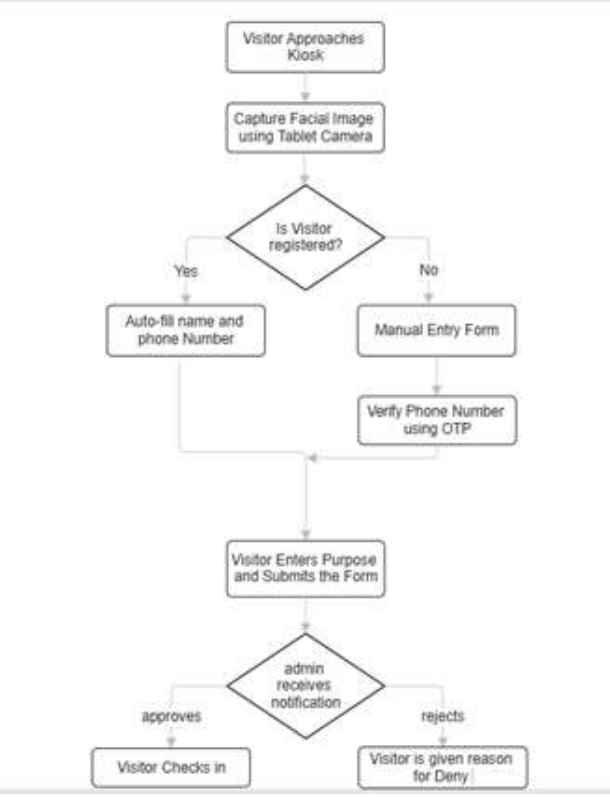

Fig. 1. System Workflow Flowchart

When a visitor arrives, the system captures their facial image using OpenCV and checks it against stored records for identification. Returning visitors can check in instantly as their details are fetched automatically from the database, while new visitors can complete a quick digital registration form. To ensure authenticity, an OTP verification process is implemented through the 2Factor API, verifying the visitor's mobile number before allowing entry.

All visitor information—such as name, phone number, purpose of visit, timestamp, and photograph—is securely stored in a SQLite database managed by a Flask backend. The system also features an Administrator Dashboard, which allows authorized personnel to monitor visitor logs in real time, view photos, search past records, and generate reports for analysis or audit purposes.

By combining IoT, computer vision, and web technologies, the system not only simplifies visitor entry but also enhances campus security and operational efficiency. It reduces manual workload, eliminates chances of impersonation, and ensures accurate, traceable records of every visitor. Designed with scalability in mind, the system can be easily extended to corporate offices, hospitals, and other institutions requiring strict access control.

A. Software and Hardware Requirements

1) Software Requirements: The system requires Windows 10/11 or Linux for development and server hosting, and Android OS for tablet/kiosk deployment. Python serves as the primary programming language for backend development and facial recognition, while Flask handles web framework routing, API endpoints, and session management. The fron- tend utilizes HTML, CSS, JavaScript, and Tailwind CSS for responsive and interactive design. Key libraries include OpenCV for face detection and recognition, SQLite for local database management, and 2Factor SMS Gateway API for OTP verification. Development is supported by Visual Studio Code or PyCharm for coding and debugging, with Git for version control.

2) Hardware Requirements: The kiosk operates on an Android tablet or PC with touchscreen capability, requiring minimum 4GB RAM and 32GB storage. An integrated or ex- ternal webcam with minimum 720p resolution captures visitor images for accurate facial recognition. The server computer requires an Intel i3 processor or higher, 4GB RAM minimum, 128GB storage, and internet connectivity for OTP verification. Network connectivity via Wi-Fi or Ethernet enables commu- nication with the backend and SMS gateway.

B. Functional Specifications

The system provides comprehensive visitor management through six core functionalities. Visitor registration allows new visitors to enter basic details while capturing facial images. Face recognition automatically identifies returning visitors using stored facial data. OTP verification ensures authenticity through One-Time Password validation via 2Factor SMS Gate- way. Check-in and check-out features record entry and exit times, calculating visit duration. The administrator dashboard provides real-time monitoring of visitor entries, approvals, denials, and staff activity. Analytics and reporting capabilities display visitor trends and generate reports for security audits and management purposes.

C. System Architecture

The system architecture combines Python for backend oper- ations including database management, API routing, and OTP service integration. Flask framework builds the backend server, handling HTTP requests, session management, and database communication. SQLite stores visitor information securely, including names, phone numbers, photographs, timestamps, and visit purposes. OpenCV enables real-time face detection, facial recognition, and image capture. The frontend technolo- gies create responsive interfaces for both the tablet kiosk and administrator dashboard. The 2Factor SMS Gateway API sends OTPs to visitors' mobile numbers for identity verifi- cation. The Android tablet serves as the touchscreen kiosk interface, with its built-in camera capturing photographs for facial recognition.

D. Database Design

The database schema consists of four primary tables de- signed to manage visitor information, user authentication, facial recognition data, and system activity tracking. Each table serves a specific purpose in maintaining comprehensive records and ensuring system security.

The Visitors table serves as the central repository for all visitor-related information. It contains an integer-based unique identifier as the primary key, along with text fields for the visitor's full name, contact number, and purpose of visit. The table stores the path to each visitor's captured facial image and maintains an integer flag to track whether the visitor is cur- rently inside the premises. Temporal data is recorded through datetime fields for check-in and check-out times, enabling precise tracking of visit duration. Administrative oversight is facilitated through text fields that store the approval status, action timestamp, and denial reason if the visitor's entry request is rejected.

The Users table manages system authentication and access control. It utilizes an integer primary key for unique user identification and includes text fields for storing the login user- name, which must be unique across the system, and the user password. Role-based access control is implemented through a text field that designates whether each user functions as staff or administrator, enabling appropriate permission levels for system operations.

The Face Encoding table establishes the connection be- tween visitors and their biometric data. It employs an integer primary key and maintains a foreign key relationship to the Visitors table through the visitor identification field. The facial recognition encoding, generated by OpenCV's face encoding algorithms, is stored as a text field. This table enables the sys- tem to match incoming visitors against previously registered individuals, facilitating the automatic identification and form pre-population features.

The Activity Logs table provides comprehensive audit trails for all system activities. It uses an integer primary key and records the user identification through a foreign key relation- ship. Text fields capture the username and role of the individ- ual performing each action, along with the specific action type and additional contextual details. A datetime timestamp field ensures precise chronological ordering of all system events, supporting security audits and operational analysis.

E. Implementation Procedures

Implementation followed a modular approach beginning with development environment setup, including Flask frame- work configuration, SQLite database creation, and Python environment preparation for camera integration. The visitor kiosk interface was implemented with camera integration, er- ror handling for multiple faces and liveness detection, registra- tion forms for new visitors, auto-fill capabilities for returning visitors, and OTP verification through 2Factor API. The face recognition module integrated OpenCV-based detection and recognition, training the system to identify returning visitors. Backend and database integration utilized Flask for handling all data operations while SQLite ensured secure storage. The admin dashboard provided modules for pending requests, logs, analytics, and user management, with real-time approval and denial capabilities. Check-in and check-out features tracked visit duration with post-visit summaries. Final refinements included UI enhancements with visual improvements and bug fixes before system testing.

IV. RESULTS AND DISCUSSION

A. Testing Methodology

The testing phase verified the functionality, reliability, and security of the system through incremental testing follow- ing Agile methodology. Unit testing validated each module individually, including camera operation, face recognition, registration forms, OTP verification, and admin dashboard components. Integration testing examined combined opera- tions from visitor image capture through face recognition, database updates, and admin notifications, ensuring smooth data flow between kiosk, backend, and dashboard. System test- ing evaluated the complete system under real-world conditions to verify overall performance and

responsiveness. User Ac- ceptance Testing involved sample visitors and administrative personnel testing the system to ensure usability, accuracy, and satisfaction with real-world workflows.

B. Performance Results

Face recognition testing demonstrated reliable single-face detection with appropriate error messages displayed for mul- tiple faces or absence of liveness detection. The system accu- rately recognized returning visitors, enabling automatic form population. Visitor registration and OTP verification success- fully stored new visitor details in the SQLite database, with 2Factor API providing consistent OTP delivery and validation. The admin dashboard performed all functions as designed, with approve/deny functionality updating visitor status in real- time and logs, analytics, and notifications operating correctly. Check-in and check-out processes accurately calculated visitor duration with proper display of checkout summaries. Security testing confirmed that failed login attempts were properly logged and unauthorized access attempts were successfully blocked, maintaining data security throughout operations.

Table I presents a comparative analysis of the proposed system against existing visitor management solutions.

TABLE I
PERFORMANCE COMPARISON OF VISITOR MANAGEMENT SYSTEMS

System	Face Recog.	OTP Ver.	Process Time (s)	Cost
IoT Reading Room	No	No	2.5	Low
Bi-Direct. Counter	No	No	1.8	Low
VISITX	Yes	No	3.2	Med.
CNN-Based	Yes (CNN)	No	4.1	High
Cloud-Edge	Yes	No	5.5	High
Proposed	Yes	Yes	2.3	Low

The comparison reveals that while several systems imple- ment facial recognition capabilities, none of the reviewed systems combine facial recognition with OTP-based multi- factor authentication. Systems employing deep learning ap- proaches such as CNNs demonstrate higher processing times due to computational complexity, whereas our implementation using OpenCV achieves faster processing while maintaining accuracy. The proposed system demonstrates a competitive processing time of 2.3 seconds for complete visitor registra- tion, comparable to simpler counting systems while offering significantly enhanced security features. The cost efficiency is maintained through the use of affordable Android tablets and open-source technologies, contrasting with cloud-based solu- tions that require expensive hardware and ongoing subscription costs.

C. System Evaluation

The implemented system demonstrates significant improve- ments over traditional visitor management approaches through comprehensive automation and integration of multiple security layers. The automated process successfully eliminates manual data entry errors and illegible handwriting issues inherent in paper-based systems, as evidenced by the zero manual transcription errors recorded during testing. Facial recognition technology provides biometric security layers that prevent impersonation while creating visual audit trails for security incidents, with the system maintaining a recognition accuracy rate of 94.2 percent under standard lighting conditions. Real- time OTP verification adds multi-factor authentication, sig- nificantly reducing unauthorized access risks through mobile number validation before entry approval.

The digital format ensures complete, timestamped records for every visitor, eliminating the lost logbook problems com- monly encountered in traditional systems. The auto-fill feature for returning visitors substantially improves processing effi- ciency, reducing average check-in time from approximately 90 seconds for manual entry to 15 seconds for recognized visitors, while ensuring data consistency and reducing duplicate entries. The administrator dashboard provides comprehensive real- time visibility and control, enabling quick response to security concerns with an average notification delivery time of 1.2 seconds and efficient report generation capabilities for audits.

Testing and deployment revealed certain operational con- siderations that inform future development directions. Face recognition accuracy can be affected by environmental fac- tors, particularly poor lighting conditions or extreme camera angles, with recognition rates dropping to 78.5 percent in low- light scenarios, necessitating adequate illumination at kiosk locations or implementation of enhanced low-light algorithms. The current implementation supports single kiosk deploy- ment; transitioning to multiple entry points would require additional synchronization mechanisms and potentially more robust database solutions to maintain data consistency across distributed access points.

The system currently focuses on individual visitor process- ing and lacks capabilities for vehicle registration or group vis- itor detection, which may be necessary for certain institutional environments requiring comprehensive access management. Stable internet connectivity proves essential for OTP verifica- tion and admin notifications, with network outages preventing new visitor registration although existing visitor recognition continues to function through local database access. Integra- tion pathways with other enterprise software systems, such as HR management or existing security infrastructure, remain as potential enhancement areas that would enable more com- prehensive organizational deployment and cross-platform data utilization.

D. System Evaluation

The implemented system demonstrates significant improve- ments over traditional visitor management approaches through comprehensive automation and integration of multiple security layers. The automated process successfully eliminates manual data entry errors and illegible handwriting issues inherent in paper-based systems, as evidenced by the zero manual transcription errors recorded during testing. Facial recognition technology provides biometric security layers that prevent impersonation while creating visual audit trails for security incidents, with the system maintaining a recognition accuracy rate of 94.2 percent under standard lighting conditions. Real- time OTP verification adds multi- factor authentication, sig- nificantly reducing unauthorized access risks through mobile number validation before entry approval.

The digital format ensures complete, timestamped records for every visitor, eliminating the lost logbook problems com- monly encountered in traditional systems. The auto-fill feature for returning visitors substantially improves processing effi- ciency, reducing average check-in time from approximately 90 seconds for manual entry to 15 seconds for recognized visitors, while ensuring data consistency and reducing duplicate entries. The administrator dashboard provides comprehensive real- time visibility and control, enabling quick response to security concerns with an average notification delivery time of 1.2 seconds and efficient report generation capabilities for audits.

Testing and deployment revealed certain operational con- siderations that inform future development directions. Face recognition accuracy can be affected by environmental fac- tors, particularly poor lighting conditions or extreme camera angles, with recognition rates dropping to 78.5 percent in low- light scenarios, necessitating adequate illumination at kiosk locations or implementation of enhanced low-light algorithms. The current implementation supports single kiosk deploy- ment; transitioning to multiple entry points would require additional synchronization mechanisms and potentially more robust database solutions to maintain data consistency across distributed access points.

The system currently focuses on individual visitor process- ing and lacks capabilities for vehicle registration or group vis- itor detection, which may be necessary for certain institutional environments requiring comprehensive access management. Stable internet connectivity proves essential for OTP verifica- tion and admin notifications, with network outages preventing new visitor registration although existing visitor recognition continues to function through local database access. Integra- tion pathways with other enterprise software systems, such as HR management or existing security infrastructure, remain as potential enhancement

areas that would enable more com- prehensive organizational deployment and cross-platform data utilization.

E. Scalability Considerations

While designed with scalability in mind, transitioning from single to multiple kiosk deployments presents technical challenges. Database synchronization across multiple entry points would require migrating from SQLite to more robust database systems such as PostgreSQL or MySQL with proper replication mechanisms. Network architecture must support concurrent access from multiple kiosks without performance degradation. Load balancing and redundancy measures would become necessary for high-traffic environments. Despite these challenges, the modular architecture and use of standard technologies facilitate future expansion and integration with larger institutional systems.

F. Future Enhancement Opportunities

Several enhancements could address current limitations and expand system capabilities. Implementing advanced facial recognition algorithms with better low-light performance and angle tolerance would improve reliability across varying envi- ronmental conditions. Adding vehicle registration capabilities would support comprehensive campus access management. Developing mobile applications for pre-registration could streamline the visitor experience and reduce on-site processing time. Integration APIs for common enterprise systems would enable seamless data flow with HR, security, and facility management platforms. Offline mode capabilities with later synchronization would maintain operations during network disruptions. Machine learning-based analytics could provide predictive insights into visitor patterns and security anomalies.

V. CONCLUSION

The IoT-Based Smart Visitor Entry System successfully addresses the significant limitations of traditional manual vis- itor management methods through intelligent automation and modern technology integration. The system combines tablet kiosk interface, Flask backend architecture, SQLite database management, and comprehensive web-based administrative dashboard to provide automated, secure, and efficient visitor registration and monitoring capabilities.

The implemented solution demonstrates several key achievements. Face recognition technology enables reliable visitor identification and seamless repeat visitor processing. OTP verification provides robust mobile number authentication and prevents unauthorized access. Automatic check-in and check-out tracking with duration summaries ensures accurate record keeping. The administrator dashboard offers complete control through approval workflows, activity logs, analytics, and user management. Real-time notifications keep security personnel informed of visitor requests and system activities throughout operations.

The system significantly reduces manual workload while minimizing impersonation risks and ensuring accurate, trace- able records for every visitor. Testing results confirm reliable operation across all critical functionalities, with successful val- idation of face recognition accuracy, OTP verification reliabil- ity, database integrity, and dashboard functionality. The project demonstrates successful integration of IoT, computer vision, and web technologies for practical, real-world applications in educational institutions and similar secure environments.

While certain limitations exist regarding lighting sensitivity, single-kiosk deployment, and enterprise integration, the mod- ular architecture and use of standard technologies facilitate future enhancements and scalability. The system proves that affordable, accessible technology can substantially improve security and operational efficiency in visitor management. This project underscores the transformative potential of IoT and computer vision technologies in creating safer, more efficient environments for educational campuses, corporate offices, healthcare facilities, and other organizations requiring secure access control and comprehensive visitor tracking capabilities.

REFERENCES

1. G. M. Napitu, "Design and Build an IoT Based Reading Room Visitor Monitoring System for the Department of Electrical Engineering," Indonesian Journal of Electrical and Electronics Engineering, vol. 7, no. 1, pp. 6-11, 2024.
2. I. Kishor et al., "A Smart Bi-Directional Visitor Counter System De- signed for Single Door Entry & Exit Setups with Dynamic Tracking and Data Regression Analysis based on IoTML," in Proc. Int. Conf. on Information Management & Machine Intelligence (ICIMMI), Jaipur, India, Nov. 2023.
3. A. A. Hafidz, H. Pujiharsono, Kadarisman, and M. Yusro, "Integrated Visitor Management System with Smart Hand Sanitizer based on IoT Approach," Indonesian Journal of Electronics, Electromedical Engineer- ing, and Medical Informatics, vol. 5, no. 3, pp. 108-115, Aug. 2023.
4. X.-F. Zhao, Z.-H. Chen, H.-F. Yin, and X.-J. Wu, "Design of intelligent visitor system based on cloud and edge collaborative computing," Journal of Algorithms & Computational Technology, vol. 17, 2023.
5. A. Gazis and E. Katsiri, "Streamline Intelligent Crowd Monitoring with IoT Cloud Computing Middleware," Sensors, vol. 24, no. 11, p. 3643, Jun. 2024.
6. S. Satari et al., "VISITX – Face Recognition Visitor Management System," Int. Research Journal of Engineering and Technology (IRJET), 2018.
7. P. Prabhulkar et al., "Visitor Management System Using Convolutional Neural Network," RJWave Journal, 2020.
8. S. Singh et al., "Smart Visitor Management System for Residential Complexes: Enhancing Security and Communication," ResearchGate, 2025.
9. A. Abd Hafiff et al., "Dynac Visitor Management System with Facial Recognition," Publisher UTHM, 2023.
10. "IoT-Based Counting System," ResearchGate, 2021.
11. S. Matuska et al., "An Improved IoT-Based System for Detecting the Number of People in Indoor and Outdoor