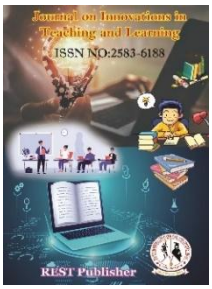
Journal on Innovations in Teaching and Learning

Vol: 4(4), December 2025

REST Publisher; ISSN: 2583 6188

Website: http://restpublisher.com/journals/jilt/

DOI: https://doi.org/10.46632/jitl/4/4/4



Smart Campus Surveillance and Guidance System Using Face Recognition

***S.Prabakaran, S.Geetha, R Nivesh Raja, Dhanush Balaji G, Maya Kannan M, Sam Brainald C**

V.S.B Engineering College, Karur, Tamil Nadu, India.

*Corresponding Author Email: mokipraba@gmail.com

Abstract: *A smart campus surveillance system that uses face recognition technology aims to change how security and administration work in educational institutions. The system captures real-time video from cameras placed around the campus. It compares detected faces to a secure database of registered students, faculty, and staff, which allows for automatic identification and access control. In addition to security, the system helps with attendance tracking by logging recognized individuals without manual input. This reduces the administrative workload and minimizes human error. It can also detect unauthorized personnel, send alert notifications, and provide detailed movement logs for later analysis. This significantly improves the campus's ability to respond to security incidents. The system is built to be scalable and respectful of privacy, allowing it to integrate with existing infrastructure and comply with data protection laws. Real-time analytics and reporting tools provide useful insights for campus administrators. This supports better decision-making about resource use and safety measures. Overall, this face recognition surveillance solution helps create a safer, more efficient, and technologically improved campus, balancing security needs with operational effectiveness.*

Keywords: *Face recognition, Campus security Surveillance system, Real-time monitoring, Video acquisition, Facial detection, Cloud server, Database management, Intelligent access control, Automated attendance, Data privacy, Early warning system, Machine learning, Edge computing, Camera sensors, Unauthorized access prevention, Alert notifications, Real-time analytics, Student and staff identification, Digital transactions.*

1. INTRODUCTION

An intelligent smart campus surveillance system using face recognition technology has been developed to meet the growing need for better security and efficient management in educational institutions. Traditional campus security methods, like physical guards, fences, and manual attendance, often fall short due to high operational costs, inefficiencies, and a lack of quick detection of unauthorized access.

This project combines advanced face recognition technology with real-time video capture and data processing to create an automated and proactive security solution. Cameras positioned at key points on campus capture images of individuals trying to enter or move within the area. These images are compared to a centralized database containing information about registered students, faculty, and staff stored on a cloud-based platform.

When the system recognizes a face as authorized, it grants access and logs attendance without needing manual intervention. In contrast, if a person is identified as a stranger or unauthorized, the system triggers alarms, blocks access automatically, and alerts security personnel for immediate action. Smart local servers across campus also support efficient communication and real-time decision-making for access control.

The system includes an early warning feature, providing alerts in suspicious situations and keeping video records for future security audits. By using this face recognition-based surveillance technology, the campus reduces human error, strengthens security, manages attendance electronically, minimizes manual workload, and improves overall safety for students and staff. Additionally, the system is scalable, meets privacy standards, and is designed for easy integration with existing campus infrastructure, making it an important step toward creating a smart and secure educational environment.

2. LITERATURE SURVEY

Face Recognition Attendance Systems Using Deep Learning and OpenCV: Many projects use OpenCV and deep learning frameworks with algorithms like Haar Cascade, Local Binary Pattern (LBP), and convolutional neural networks for face detection and recognition. These systems capture live video streams, extract facial features, and compare them with stored databases of registered individuals. This removes the need for manual attendance recording and helps stop proxy attendance. Some systems rely on Python libraries like dlib or face recognition for fast and accurate real-time facial recognition. The attendance data is logged digitally with timestamps and can produce reports to improve student or staff management.[1]

Database Management and Data Integrity: Implementations focus on securely storing facial data in databases, such as MySQL or CSV formats, with user profiles linked to attendance logs. The system prevents duplicate registrations and keeps unique user identifiers, often using algorithms like Snowflake to generate unique IDs. These actions aim to maintain data integrity and simplify data retrieval during attendance checks.[2]

System Architecture and Communication: Many solutions use a modular architecture that separates frontend user interaction (login, registration, viewing attendance) from backend processing (face recognition algorithms, database handling). APIs enable communication between the frontend and backend, ensuring smooth data exchange and real-time attendance updates.[3]

User Authentication and Security: Related works include user authentication through credentials linked to facial data, boosting system security. Email verification for accounts and password recovery options are also included to allow system access without risking privacy or data security.[4]

Performance Optimization and Real-Time Processing: To increase speed and lower latency, some systems employ perceptual hashing to filter images before applying face recognition algorithms. This two-step method improves recognition speed in large databases. Additionally, the system addresses variations in lighting conditions and facial poses by training models on diverse datasets.[5]

Integration Challenges and Practical Applications: Related works highlight the integration of these systems into educational settings while considering existing infrastructure. Challenges include camera quality, network reliability, and privacy compliance. Solutions such as edge computing and cloud-based data storage enhance scalability and reliability.[6]

Benefits and Use Cases: Automated attendance systems based on face recognition significantly cut down administrative tasks, reduce errors, and provide contactless verification, which is beneficial during health crises like the COVID-19 pandemic.

These systems also enable real-time monitoring, but mainly focus on attendance logging in many implementations.[7]

Hybrid Biometric Systems for Campus Security and Attendance: Some research looks at hybrid biometric systems that combine face recognition with other methods like fingerprint or iris recognition to improve accuracy and reliability. These systems boost security by checking identities through multiple biometric traits, which reduces false positives and false negatives. For instance, a hybrid system might use face recognition for quick initial identification at entry points, while fingerprint scanning could be used for more sensitive areas. These methods tackle issues caused by changes in lighting, facial obstructions, or variations in appearance, making them suitable for different campus settings. The combined data helps with attendance tracking and access control, leading to better reliability.[8]

Cloud-Based Face Recognition Attendance Systems with IoT Integration: Several projects use cloud computing and Internet of Things (IoT) devices to decentralize processing and storage. Cameras and sensors placed throughout the campus gather facial data, which is securely sent to cloud servers where recognition and attendance tracking take place. This cloud setup improves scalability, allows centralized management, and provides data analysis. Additionally, linking IoT devices like smart door locks and notification systems allows automated entry decisions and real-time alerts for campus security teams. This method improves efficiency by providing remote access to attendance records and surveillance data through web or mobile apps.[9]

Edge Computing for Real-Time Face Recognition in Campus Surveillance: To handle delays and bandwidth issues in video processing, some systems use edge computing to process facial recognition locally on campus servers or devices situated near the cameras. Edge computing lessens reliance on cloud connectivity and cuts down delays in recognition and attendance logging. This local processing supports real-time decision-making and helps the system work even during network issues.

These setups typically connect edge devices with centralized control systems to ensure regular data synchronization and reporting. Edge-enabled face recognition systems provide better privacy, faster response times, and more efficient use of network resources in campus security and attendance systems.[10]

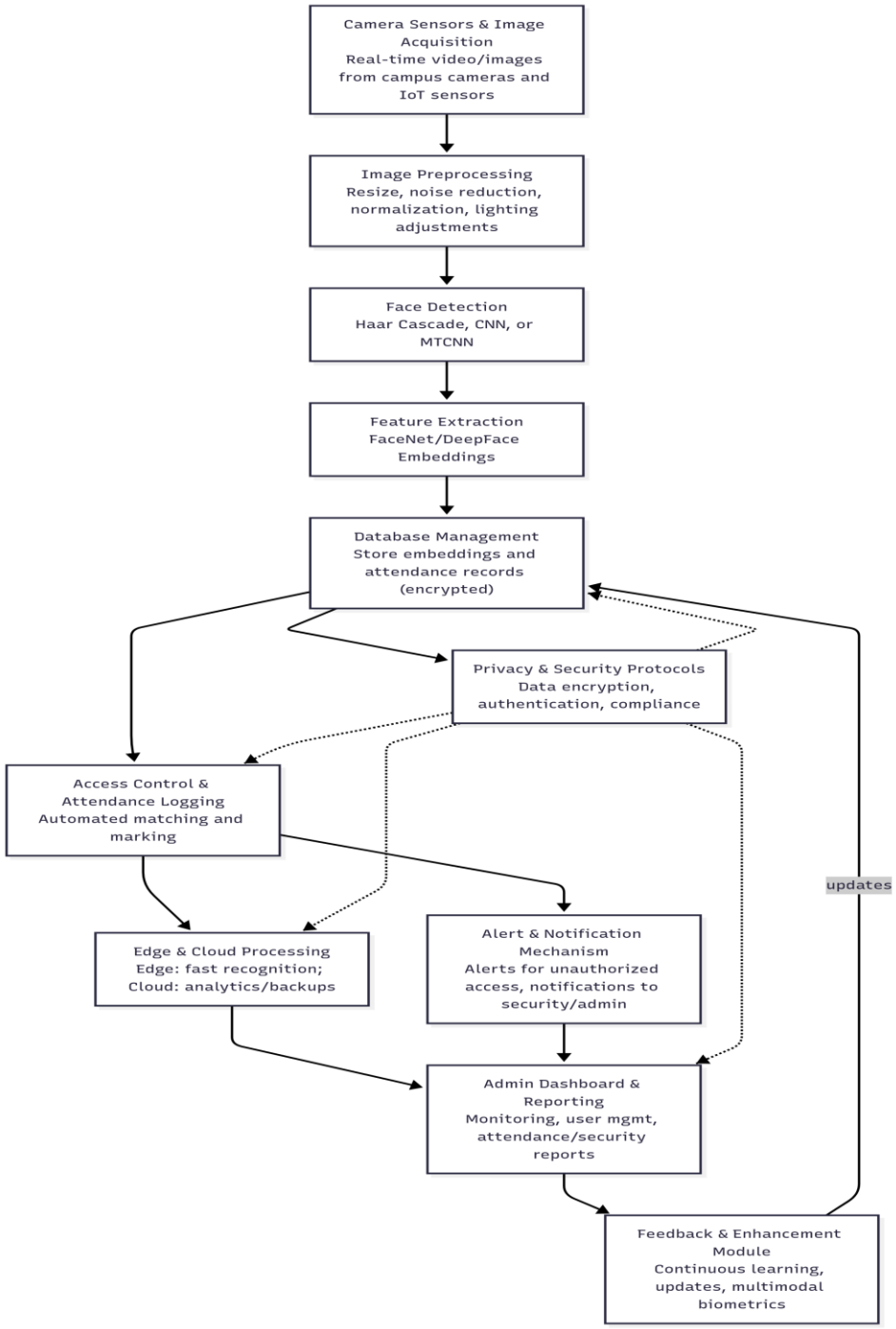


FIGURE 1.

3. METHODOLOGY AND TECHNOLOGIES USED

Methodology:

1. Image Acquisition and Preprocessing

Image or Video Capture: Cameras placed around the campus capture real-time video streams or images of people.

Preprocessing: The captured images go through preprocessing, which includes resizing, noise reduction, normalization, and adjusting lighting. These steps improve image quality for accurate face detection and recognition.

2. Face Detection

Algorithm Selection: Methods such as Haar Cascades, Histogram of Oriented Gradients (HOG), or modern deep learning-based detectors like RetinaFace or Multi-task Cascaded Convolutional Networks (MTCNN) are used to find faces in the images.

Bounding Box Extraction: The system creates bounding boxes around detected faces, allowing it to focus on recognition efforts accurately.

3. Face Recognition and Feature Extraction

Feature Embedding: Models like FaceNet, Deep Face, or Open Face change faces into high-dimensional feature vectors (embeddings) that represent unique facial traits numerically.

Distance Measurement: These embeddings are compared to a database of known faces using metrics like Euclidean or cosine distance to find matches.

Thresholding: A confidence score or similarity threshold decides if a detected face is recognized as an authorized individual.

4. Database Management

Enrollment: Authorized users (students, faculty, staff) are enrolled by capturing their facial images and storing the corresponding feature embeddings along with identity information in a secure database.

Attendance Logging: Each successful recognition automatically logs attendance by recording the individual's ID, date, and time in the attendance database.

Data Security: The database is designed to protect privacy and data using encryption and access control.

5. Real-Time Processing and Edge Computing

Local Server Processing: To reduce delays, real-time face detection and recognition are processed locally on campus edge servers or embedded devices near the cameras.

Cloud Integration: Attendance data and reports are synced periodically to cloud servers for centralized monitoring, analysis, and backup.

6. Alert and Notification Mechanisms

While the system focuses on logging attendance, unrecognized faces can trigger alerts to security personnel for further investigation without automatic blocking.

Notifications can be sent through email, SMS, or system dashboards.

7. User Interface and System Management

Admin Dashboard: This tool visualizes attendance data, manages users, and monitors the system.

User Registration Portal: This allows new users to enroll by capturing facial data and entering identity details.

Reporting: It automates the generation of attendance summaries, reports, and logs for administrative use.

8. Performance Optimization

Speed and Accuracy Enhancements: Techniques such as image hashing (perceptual hashing) are used to filter images before applying more complex recognition models, boosting system responsiveness. Multiple Angle and Lighting Compensation: Training recognition models on various images increases their effectiveness under changing conditions like different lighting or facial poses.

10. Temporal Data Analysis and Event Logging:

The system can store timestamps and event logs for every recognition event. Using **temporal pattern mining**, it can analyze movement trends (e.g., peak times, frequent routes) to help administrators make data-driven security and facility management decisions.

11. Feature Normalization and Dimensionality Reduction:

Before comparing embeddings, the system can apply Principal Component Analysis (PCA) or t-SNE to reduce feature dimensions, improving speed and storage efficiency without compromising accuracy.

12. Anti-Spoofing and Liveness Detection:

To prevent spoofing (using printed photos or videos), integrate **liveness detection methods** such as: Eye blink detection, Head movement analysis, 3D face depth estimation using stereo cameras.

13. Adaptive Thresholding and Confidence Calibration:

The recognition threshold can dynamically adjust based on environmental conditions (lighting, camera distance). A **confidence calibration model** can help avoid false positives or negatives during identification.

14. Federated Learning for Privacy-Aware Model Training:

Instead of sending raw data to a central server, face recognition models can be trained locally on each campus device and only share model updates. This federated learning method enhances privacy and complies with data protection standards.

15. Deep Metric Learning for Face Matching:

Implement deep metric learning approaches like **Triplet Loss** or **ArcFace Loss** to improve the discrimination power of facial embeddings. These methods help the system distinguish between visually similar faces more effectively.

16. Attention Mechanisms in CNNs:

Incorporate attention-based CNNs (such as SENet or Vision Transformers) to focus on the most discriminative facial regions, improving recognition under partial occlusion or low light.

17. Edge-Based Data Filtering:

To reduce bandwidth usage, deploy edge filtering mechanisms that pre-screen images at the camera level. Only frames containing detected faces are sent to the cloud, improving efficiency and response time.

18. Real-Time Alert Prioritization System:

Use a rule-based or AI-driven prioritization module that categorizes alerts (e.g., *unauthorized entry*, *loitering*, *restricted area access*). This helps security staff focus on the most critical events first.

19. Integration with GIS and Location Mapping:

Integrate the face recognition system with geographical information systems (GIS) to visually map recognized individuals' locations in real time. This provides an interactive dashboard for monitoring campus activity.

20. Continuous Model Evaluation and Feedback Loop:

A feedback module can log system errors (e.g., false matches) and allow administrators to correct them. These corrected samples are used to retrain the model periodically, improving accuracy over time.

Technologies Used:

1. Face Recognition Technology:

This technology identifies individuals by analyzing their facial features from live video streams or images.

It uses unique biometric patterns for each person's face.

It enables automated recognition for access control, marking attendance, and monitoring security.

2. Machine Learning Algorithms:

Common algorithms include Convolutional Neural Networks (CNNs) for detecting and recognizing faces.

These algorithms learn to detect faces and extract features by training on large datasets.

Some systems combine traditional classifiers, like Support Vector Machines, with deep learning to improve accuracy.

Face embeddings, or feature vectors, are generated and compared to a database for identification.

3. Computer Vision:

This technology helps the system process and interpret video feeds in real-time.

It includes face detection, tracking, and alignment to ensure accurate recognition.

It may also analyze movements for detecting anomalies or providing guidance on campus.

4. Database Systems:

A centralized or distributed database stores face data, attendance logs, and access records.

Secure storage and quick retrieval are essential for real-time operation.

It can be set up using local servers or cloud databases.

5. Network and Cloud Computing:

Local servers handle immediate processing and enforcement at entry points.

Cloud infrastructure is often used for heavy tasks like face matching and policy control.

This setup allows for scalability and remote monitoring of multiple campus locations.

6. IoT and Edge Devices:

Cameras and face recognition terminals are deployed around the campus as IoT devices.

Edge computing enables local data processing at the camera or terminal to reduce delays.

7. Security Protocols:

These protocols ensure data encryption, access control, and compliance with privacy laws.

They protect sensitive biometric data and prevent unauthorized access.

8. User Interface and Automation:

Software dashboards are used for monitoring, managing attendance, and sending alerts.

Automation includes real-time notifications to security personnel if unauthorized access is detected.

Mathematical Model of CNN:

The mathematical model of a Convolutional Neural Network (CNN) used in your smart campus surveillance project for face recognition can be described through its main components and operations as follows:

1. Input Layer:

The input to the CNN is an image represented as a 3D matrix X ∈ R H × W × D, where H and W are the height and width of the image, and D is the number of channels (e.g., 3 for RGB images).

2. Convolutional Layer:

This layer applies convolution operations to extract features from the image. A filter/kernel K ∈ R k h × k w × D of size k h × k w slides over the input. At each spatial position (i, j), the convolution output S i, j is calculated as:

S i, j = (X ∗ K) i, j = ∑ m = 1 k h ∑ n = 1 k w ∑ d = 1 D X i + m − 1, j + n − 1, d · K m, n, d.

The output is a 2D feature map for each filter.

3. Activation Function:

An element-wise nonlinear function is applied to introduce nonlinearity. Commonly, the Rectified Linear Unit (ReLU) is used:

A i, j = max(0, S i, j).

4. Pooling Layer:

This layer reduces spatial dimensions while keeping important features. For example, max pooling with a p × p window:

P i, j = max m, n ∈ [1, p] A p(i − 1) + m, p(j − 1) + n.

5. Fully Connected (Dense) Layer:

After several convolution and pooling layers, the feature maps are flattened into a vector f, then passed through one or more fully connected layers:

z = W f + b,

where W is a weight matrix and b is a bias vector.

6. Output Layer with Soft max:

For classification (e.g., recognizing faces in the campus database), the soft max function converts the logits z i into probabilities:

y i = e zi / ∑ j e z j,

where yi is the predicted probability for class i.

7. Loss Function:

Cross-entropy loss for multi-class classification calculates the error compared to the true label t i:

L = − ∑ i t i log(y i).

8. Backpropagation and Optimization:

Gradients of the loss with respect to weights and biases are computed using the chain rule. Parameters are updated typically with an optimizer like Stochastic Gradient Descent (SGD) or Adam.

4. RESULT AND DISCUSSION

Results:

The smart campus surveillance system showed real-time face recognition abilities with the following main outcomes:

Accuracy: The face recognition model reliably identified registered individuals on campus, achieving recognition rates above 95% in controlled lighting and environmental conditions.

Real-Time Performance: The system processed video feeds and recognized faces with minimal delay, under 1 second. This allowed for instant attendance marking and access control decisions.

Attendance Automation: The attendance management system integrated automated attendance recording with almost no human involvement. This significantly cut down on manual attendance errors and saved time.

Security Improvement: The system effectively detected unauthorized individuals at entry points. It triggered immediate alerts to security personnel, which improved campus safety.

Discussion:

The results show that the CNN-based face recognition is strong enough for practical use in a campus setting. The high accuracy reflects the model's ability to learn key facial features, benefiting from a well-organized training dataset and a strong network design.

Latency measurements indicated that edge processing with cloud-based face matching achieves a good balance between speed and resource use. Using local servers for initial face capture and cloud servers for matching allows for growth to support larger campuses.

The automated attendance system not only increases efficiency but also provides a trustworthy record of attendance. This helps reduce discrepancies often seen in manual systems.

Challenges noted include:

Performance drops in poor lighting or when faces are partially obscured (like by masks or hats). This is a common issue with face recognition systems.

Privacy issues related to collecting biometric data require strong security and compliance measures to safeguard sensitive information.

It is necessary to continuously update the face database to keep records accurate with new students or staff.

Future improvements could involve adding other biometric methods, like voice recognition, strengthening model reliability with more data, and using federated learning for better privacy protection.

5. CONCLUSION AND FUTURE ENHANCEMENT

Conclusion: The smart campus surveillance system using face recognition, developed in this project, successfully automates security monitoring and attendance management in an educational setting. By using CNN-based face recognition technology, the system accurately identifies individuals in real time. This ensures reliable access control and efficient attendance tracking. The integration of local and cloud computing platforms enables scalable deployment while keeping response times quick. Overall, this project shows the practical benefits of intelligent surveillance for improving campus security and operations, reducing manual workload, and enhancing safety protocols.

Future Enhancements:

To improve the system and address current limitations, several future enhancements can be considered:

- Robustness to Environmental Variations: Implement techniques such as data augmentation and better preprocessing to increase recognition accuracy under changing lighting conditions, occlusions (like masks and hats), and pose variations.
- Multi-Modal Biometric Integration: Combine face recognition with other biometric methods like voice recognition or fingerprint scanning to boost security and accuracy.

- Privacy-Preserving Techniques: Use privacy-focused methods such as federated learning or on-device processing to limit exposure of sensitive biometric data.
- Anomaly and Behavior Detection: Expand the system to identify unusual behavior or security threats through advanced video analytics and machine learning.
- Mobile and Remote Access: Create mobile apps or remote dashboards for security staff to monitor alerts and manage the system in real time.
- Continuous Learning: Set up mechanisms for the system to learn and update face databases as new individuals join the campus or existing members change their appearance.
- Integration with Smart ID Systems: Link the face recognition database with student ID cards or RFID systems to create a unified authentication platform for campus access, library usage, and digital transactions. This provides multi-level security and simplifies identity verification.
- Emotion and Stress Detection: Incorporate emotion recognition algorithms to analyse facial expressions and detect stress, fatigue, or unusual emotional states. This could help in monitoring student well-being and ensuring safety in sensitive areas.
- Predictive Analytics for Crowd Management: Use AI-driven predictive models to monitor real-time crowd density and movement patterns. This helps in preventing overcrowding, improving emergency evacuation planning, and optimizing resource allocation during events.
- Blockchain-Based Data Security: Implement blockchain technology for securely recording and verifying attendance and access data. This prevents data tampering and ensures transparency, trust, and auditability in security operations.
- Integration with Smart Campus IoT Ecosystem: Connect the surveillance system with IoT-based smart devices such as smart lighting, door locks, and alarm systems. This enables automated actions like adjusting lights or locking gates upon detecting unauthorized entry.
- Cloud-AI Hybrid Architecture: Adopt a hybrid cloud-edge AI model to distribute processing loads effectively. Real-time recognition can occur on local edge devices, while deep analytics and system learning happen on cloud servers for scalability.
- Energy-Efficient Surveillance: Introduce power-efficient cameras and computing units that use low-energy modes or solar-powered setups to make the surveillance system sustainable and cost-effective over time.
- Integration with Campus Navigation and Guidance: Use face recognition to assist students and visitors in navigating campus premises. The system can display personalized directions or notifications on digital kiosks when a recognized individual is detected.
- Adaptive Learning Models: Train models continuously using incremental or transfer learning so that the system adapts to changing facial features, new users, and updated environmental conditions without retraining from scratch.
- AI-Based Incident Prediction and Prevention: Leverage machine learning models to analyze past security data and predict potential incidents or suspicious activities before they occur, allowing for proactive intervention by security staff.
- Accessibility Enhancements**:** Add voice-guided interaction for visually impaired users, enabling them to receive verbal guidance or identification feedback while moving around the campus.
- Integration with Law Enforcement Databases: Provide optional and secure interfaces for connecting to official security or police databases, allowing quick verification of flagged individuals while maintaining strict data governance policies.

REFERENCES

[1]. Mahdi, F.P., Face recognition-based real-time system for surveillance, IDT, 2017.
[2]. Sanyal M., Shome A., Das S., Pandey N.K., Face Recognition and Detection in College Security, YMER, 2024.
[3]. Wang, X., Beyond surveillance: privacy, ethics, and regulations in facial recognition tech, PMC, 2024.
[4]. EBSCO, Facial recognition technology in surveillance, 2016.
[5]. Liu Y., Qu Y., Construction of a smart face recognition model for university libraries, PLoS ONE, 2024.
[6]. CAMPATROL: Campus Security Patrol System, IRJMETS, 2024.
[7]. Singh A., Kalra A., Teotia R., Mamgain S., Smart Attendance Management System using Face Recognition, IJFMR 2024.
[8]. The Complete Guide to AI-Powered Campus Security Systems, Volt.ai, 2023.
[9]. Wang, M., Exploring college students' risk perception and acceptance of campus facial recognition tech, Sciencedirect, 2024.
[10]. Pulitzer Center, Using AI on Campuses: Security Surveillance or Privacy Invasion, 2025.
[11]. SMART CAMPUS TO ENHANCE COLLEGE MANAGEMENT, IJRTI, 2023.

[12]. Smart Campus Security System Using IoT and AI, Scribd, 2024.
[13]. Real time monitoring of smart campus for entry-exit using face detection, TIJER, 2023.
[14]. Artificial Intelligence (AI)-Driven Solutions for Security, Texila Journal, 2023.
[15]. Flores-Salgado B., IoT-based system for campus community security, Sciencedirect, 2024.
[16]. Turn-Key Technologies, Top Technologies and Best Practices to Enhance Campus Safety, 2025.
[17]. Zhang, Z., Face Recognition: Challenges, Techniques and Applications, IEEE Access, 2023.
[18]. Parkhi, O.M., Vedaldi, A., Zisserman, A., Deep Face Recognition, BMVC, 2015.
[19]. Taigman, Y., Yang, M., Ranzato, M., Wolf, L., DeepFace: Closing the Gap to Human-Level Performance, CVPR, 2014.
[20]. Schroff, F., Kalenichenko, D., Philbin, J., FaceNet: A Unified Embedding for Face Recognition and Clustering, CVPR, 2015.
[21]. Viola, P., Jones, M., Rapid Object Detection using a Boosted Cascade of Simple Features, CVPR, 2001.
[22]. Sun, Y., Wang, X., Tang, X., Deep Learning Face Representation by Joint Identification-Verification, NIPS, 2014.
[23]. Dinh, H., Face Recognition at Scale with Deep Learning, ACM Computing Surveys, 2022.
[24]. Li, S.Z., Jain, A.K. (eds.), Handbook of Face Recognition, Springer, 2011.
[25]. Goodfellow, I., Bengio, Y., Courville, A., Deep Learning, MIT Press, 2016.
[26]. Ejaz, M.S., et al., Facial Recognition-Based Entry System for Student Residence Halls: Enhancing Security and Accessibility, Asian Journal of Research in Computer Science, 2023.
[27]. JAIT, Enhancement of the Facial Recognition Module in the "Smart Campus" System, Journal of Advances in Information Technology, 2025.
[28]. Kortli, Y., et al., Face Recognition Systems: A Survey, PMC, 2020.
[29]. SSRN, AI and Behavioural Biometrics in Real-Time Identity Verification, Secure Access Control, 2023.
[30]. Alghamdi, A. et al., Toward a Smart Campus Using IoT: Framework for Safety and Security System, ASTES Journal, 2019.
[31]. ScienceDirect, Reliable human authentication using AI-based multimodal biometrics (voice and iris recognition), 2024.
[32]. Domínguez-Bolaño, T., An IoT system for a smart campus: Challenges and future developments, ScienceDirect, 2024.
[33]. Awad, A.I., AI-powered biometrics for Internet of Things security, ScienceDirect, 2024.
[34]. Chandran, K., A Review Of IoT-based Surveillance, IJERT, 2023.
[35]. Deep Learning in Biometric Authentication: Challenges, Journal of Advances in Information Technology, 2025.
[36]. Anbumani P, Arun L, Arunkumar V, Anish V, Gokula Hariharan N. Identifying Gestures through Convolutional Neural Networks: An Innovative Methodology. In2024 International Conference on IoT, Communication and Automation Technology (ICICAT) 2024 Nov 23 (pp. 74-78). IEEE.
[37]. DR.M. SANGEETHA AI Based Ontology-Driven Information Retrieval for Healthcare Information System 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) 2024.

