Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI-Powered Security and Attendance Management System Using Deep Learning and Facial Recognition

Ms. S. Hemavathi[1], Ms. Rekha Chakravarthi[2]

[1]*PG Student, M.Sc. (Computer Science), Sathyabama Institute of Science and Technology, Chennai-119,* hemavathis2002@gmail.com

[2]*Professor, Department of ECE,Sathyabama Institute of Science and Technology, Chennai-119,* rekha_2705@yahoo.co.in

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

This project presents a comprehensive AI-driven security and attendance management system, designed to leverage state-of-the-art deep learning and facial recognition technologies. By employing Convolutional Neural Networks (CNNs) and the YOLO v8 algorithm, the system achieves precise, real-time classification of individuals as either authorized or unauthorized when they attempt to access buildings or classrooms. The framework utilizes advanced facial feature mapping and high-speed image analysis, ensuring robust identity verification through seamless comparisons with a secure, pre-registered database. In academic environments, the system automates the process of attendance tracking with high accuracy, dynamically logging the presence of students and significantly reducing administrative workloads. It enhances the security infrastructure by integrating automated alert mechanisms; upon detecting unauthorized entry, the system sends instant notifications and issues security warnings to designated personnel, activating proactive threat mitigation protocols. The intelligent response suite includes real-time SMS and email alerts to ensure immediate action is taken. This innovative solution combines the efficiency of automated attendance systems with advanced security protocols, setting a new benchmark in smart building management. By integrating AI-driven facial recognition and automated response systems, it enhances operational efficiency, ensures reliable access control, and promotes a safer, more secure environment for academic and institutional use.

Keywords: AI-driven Security, Facial Recognition, Attendance Management, Deep Learning, Real-time Access Control.

INTRODUCTION

Modern security and attendance systems now require artificial intelligence (AI) since it provides improved accuracy and efficiency. By automating access control and identity verification, AI-powered systems—especially those that use face recognition and deep learning techniques—are completely changing security. At the core of these developments are deep learning algorithms, particularly Convolutional Neural Networks (CNNs), which allow facial recognition systems to evaluate images with high precision even in the presence of changing illumination and perspective. These systems can identify unwanted access in real time in security applications, alerting security staff right away and averting possible dangers (Şengönül et al., 2023). Similar to this, AI-driven attendance systems automate the roll-call procedure using facial recognition, removing human error and increasing productivity in settings including corporate offices and educational institutions (Sheikh et al., 2023). These systems can handle big populations with great accuracy since they are not only faster but also more scalable. Deep learning models get better over time by continuously learning from fresh data, which makes them more capable of managing a variety of situations and guaranteeing long-term dependability (Jang et al., 2023). As a result, facial recognition and deep learning are essential to revolutionizing security and attendance management systems by offering clever and flexible solutions.

This survey aims to investigate how AI-driven technologies, particularly facial recognition and deep learning, may be integrated to improve security and attendance management systems. The survey looks at how these technologies are currently developed in order to demonstrate how well AI works to automate identity verification, real-time monitoring, and attendance tracking. How deep learning techniques, in particular Convolutional Neural Networks

(CNNs), enhance the precision and effectiveness of facial recognition systems is one of the main concerns addressed. What are the advantages and difficulties of deploying AI-based security solutions in various settings? In what ways do AI-powered attendance systems perform better than conventional techniques in terms of accuracy, scalability, and dependability? The poll also looks at prospective advancements in deep learning algorithms and privacy and data protection ethics, as well as future trends in AI-powered security and attendance management.

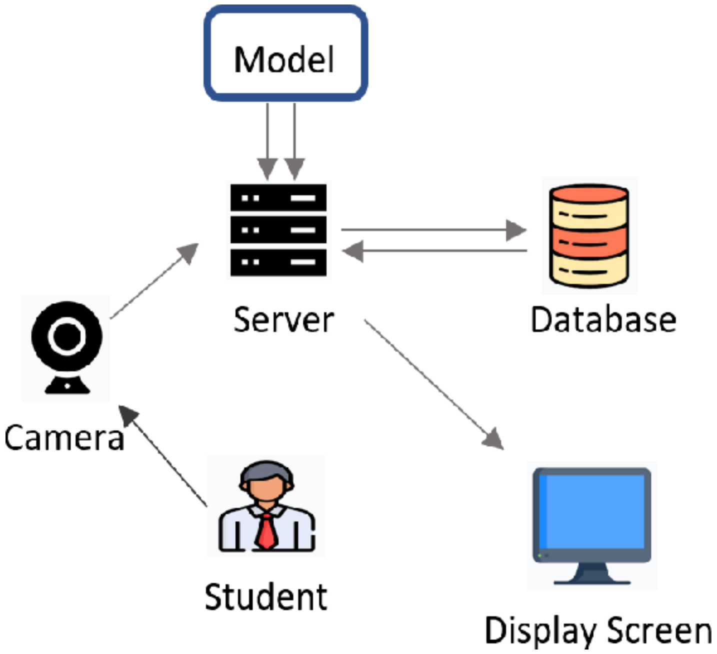


Fig 1. Overview of the application (source: Kakarla et al., 2020)

BACKGROUND AND RELATED WORK

Conventional security and attendance systems have historically depended on human procedures or antiquated technology, which frequently have accuracy, scalability, and security issues. Techniques such as PINs, keycards, and manual ID checks have been widely used in security systems. Although these systems work well for smaller-scale applications, they are vulnerable to mistakes, carelessness, and security lapses such illegal access via stolen or misplaced credentials (Eger et al., 2024). In a similar vein, conventional attendance methods such as card swipes or roll calls are laborious, prone to mistakes, and frequently manipulated, which results in incorrect data collecting, especially in large institutions (Talukder et al., 2024). An important turning point in security and attendance management systems has been brought about by the development of facial recognition technology. Low-resolution photos and basic algorithms that could only identify faces in controlled settings were the initial limitations of facial recognition (Dakhil et al., 2024). However, the capabilities of facial recognition systems have significantly increased with the introduction of deep learning techniques, especially Convolutional Neural Networks (CNNs). CNNs have improved precision and robustness by learning intricate patterns in facial features, allowing for effective identification even in the face of changing lighting, angles, and expressions (Sheikh et al., 2023). This development has made facial recognition a popular option for contemporary security solutions by enabling its effective deployment in real-time systems.

By providing more than simply facial recognition, AI-powered technologies have further transformed the landscape. To automate the verification process, adjust to new data, and make choices without human involvement, these systems make use of machine learning models. For instance, artificial intelligence (AI) systems are now able to identify unauthorized access or questionable activity, alerting security staff in real time and reducing the need for manual monitoring (Shabbir et al., 2024). Artificial intelligence (AI) systems have automated attendance management by using facial recognition to replace manual roll calls, enabling smooth and precise tracking. Larger datasets can also be handled by AI-powered systems, which can also learn and adapt over time to perform better as they process more data (Essien et al., 2023).

Current AI-powered systems still have important flaws and restrictions in spite of the tremendous progress. Since facial recognition requires the gathering and storage of sensitive personal data, maintaining privacy and data security is one of the main concerns. Widespread adoption is still significantly hampered by ethical worries about data breaches, spying, and abuse of biometric information. Furthermore, even though deep learning algorithms have greatly increased facial recognition accuracy, biases can still affect them, especially when they are trained on non-diverse datasets, which can cause performance differences among various demographic groups (Jang et al., 2023). The scalability of AI systems in varied and dynamic situations is another drawback, as problems with compute power, network capacity, and legacy system integration might reduce their efficacy.

Related Work

i The study titled "Automation of surveillance systems using deep learning and facial recognition" utilized a custom dataset of 7,500 images of 26 individuals to train a VGGFace-based system with transfer learning for real-time face detection and recognition, achieving 96% average accuracy, and demonstrating its potential to automate attendance and identity verification in surveillance systems (Singh et al., 2023).

ii The study titled "Enhancing Security in Public Spaces Through Generative Adversarial Networks (GANs)" explores the use of GANs to improve security in public spaces by generating realistic data for threat detection and enhancing system robustness, demonstrating their effectiveness in public space protection through simulations and real-time applications (Ponnusamy et al., 2024).

iii The study titled "An Automated Face Detection and Recognition for Class Attendance" uses a dataset of student faces to implement a system based on Histogram of Oriented Gradients (HOG) with Support Vector Machines (SVM) for face detection and deep Convolutional Neural Networks (CNN) for face recognition, achieving improved accuracy over traditional methods such as QR codes, and demonstrates the system's potential for enhancing class attendance efficiency and reliability (Boe et al., 2024).

iv The study titled "Generative AI: A Systematic Review Using Topic Modelling Techniques" analyzes 1,319 records from Scopus between 1985 and 2023, using the BERTopic algorithm to identify seven key clusters in generative AI research, including image processing, content generation, emerging use cases, and data privacy, highlighting the field’s expansion and the need for further research in areas such as explainability, robustness, and security (Gupta et al., 2024).

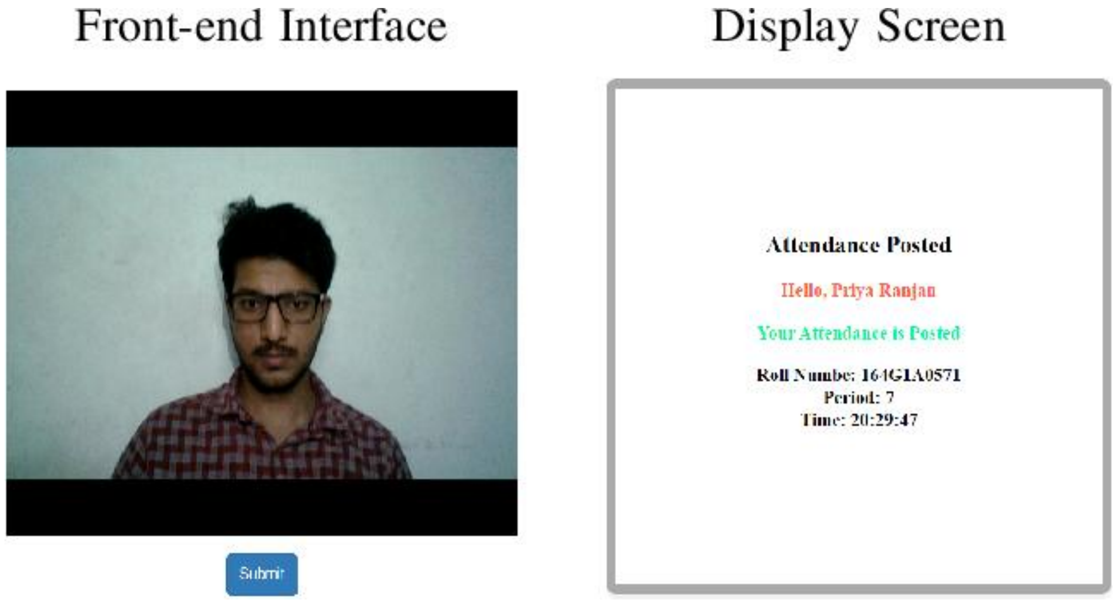
v The study titled "The Technology Interface and Student Engagement Are Significant Stimuli in Sustainable Student Satisfaction" examines a dataset of 400 respondents from higher education institutions (HEIs), using PLS-SEM to show that technology interfaces (including cyber infrastructure, e-content quality, and technology-assisted facilities) positively influence student engagement, which in turn enhances student satisfaction, emphasizing the need for HEIs to focus on improving both technology and engagement practices to boost satisfaction (Pandita & Kiran, 2023).

vi The study titled "Face Recognition for Classroom Attendance Based on Convolutional Neural Network" uses a dataset of 100 images per student captured via webcam, employing Convolutional Neural Networks (CNN) for face recognition to automatically mark attendance, achieving an accuracy increase with more images in the dataset and demonstrating the system's efficiency over traditional manual methods (Sayyad et al., 2024).

vii The study titled "Facial Recognition Reinvented: Deep Learning Based Security Alert System" employs a dataset of facial images, using Haar Cascade, Local Binary Pattern (LBP), and Convolutional Neural Networks (CNN) to identify authorized and unauthorized access, achieving improved accuracy and efficiency over traditional methods, and demonstrates potential for enhancing security in restricted areas by triggering alarms and email alerts for unauthorized individuals (Reddy et al., 2024).

viii The study titled "Smart Attendance System Based on Improved Facial Recognition" uses a dataset of 150 labeled student images from three classrooms, implementing an enhanced FaceNet model based on MobileNetV2 and SSD for efficient face recognition, achieving 95% accuracy and a frame rate of 25 FPS, and demonstrating its potential for deployment on low-resource devices like Jetson Nano for automated attendance tracking (Dang, 2023).

ix The study titled "Advancements in AI-Powered Facial Recognition for Secure User Authentication in E-Learning Environments" discusses the evolution and application of AI-based facial recognition technologies for enhancing user authentication and security in online assessments, highlighting their potential to reduce cheating, increase trust, and improve integrity in e-learning systems (Adetunji, 2024).


Front-end Interface

Display Screen

Attendance Posted

Hello, Priya Ranjan

Your Attendance is Posted

Roll Numbe: 164G1A0571
Period: 7
Time: 20:29:47

Fig 2: A Sample input image and the corresponding output

METHODOLOGIES AND TECHNIQUES

3.1 Deep Learning Algorithms:

Because of their excellent accuracy in processing and extracting characteristics from photos, Convolutional Neural Networks (CNNs) have emerged as the foundation of contemporary facial recognition systems. Several layers make up CNNs, a kind of deep learning algorithms that are intended to automatically identify hierarchical patterns in visual data. Because CNNs can learn to recognize important face characteristics like the eyes, nose, and mouth without the need for manual feature extraction, they are very useful in the context of facial recognition. CNNs are extremely resilient since they can distinguish faces in a variety of positions, lighting circumstances, and expressions thanks to training on big datasets (Barcic et al., 2023). Automatic feature extraction from photos is made possible by CNNs in facial recognition, which lowers the need for human interaction and increases scalability. The model can generalize and recognize new, unseen faces with remarkable accuracy since the network is trained using tagged photos in which the facial traits are linked to certain identities. For security and attendance systems where prompt identification is critical, CNNs' ability to process data in parallel allows for real-time recognition (Sheikh et al., 2023). Because CNNs provide automatic, accurate, and efficient identification processes, their use in facial recognition systems has completely transformed security infrastructures.

Modern object detection algorithms like YOLO (You Only Look Once) are well-liked for real-time applications like facial recognition because of their effectiveness and speed. YOLO splits the input image into a grid and predicts bounding boxes and class probabilities for each grid cell at the same time, in contrast to conventional object identification techniques that use region proposal networks or sliding windows. With a single forward trip across the network, our method enables real-time detection and end-to-end training (Azzalini et al., 2023). YOLO is used in facial recognition to instantly identify faces in pictures or video frames. To identify the person, a face is identified and then runs through a facial recognition model, like a CNN. YOLO's main benefit is that it can complete both object detection and classification tasks in a single pass, which makes it especially effective for applications like automated attendance systems and surveillance where speed is crucial (Shabbir et al., 2024). Because of its fast-processing speed, YOLO can process live video streams and recognize faces with minimal computing overhead. This effectiveness is essential in settings where a lot of people need to be recognized instantly, such offices, airports, or classrooms, where attendance and security systems must work flawlessly.

3.2 Data Handling:

Large, varied datasets are necessary for facial recognition systems to successfully train deep learning models. A broad range of photos of people in various positions, lighting scenarios, facial expressions, and facial orientations must be included in these datasets. Since they include millions of annotated photos from various identities, high-quality datasets like LFW (annotated Faces in the Wild), VGGFace2, and MS-Celeb-1M are frequently used to train face recognition algorithms (Koodalsamy et al., 2023). These datasets need to represent a range of demographics, such as differences in age, gender, ethnicity, and environmental circumstances, in order to minimize biases that can occur in real-world situations and guarantee strong performance (Chen et al., 2023). In order to prepare facial images for efficient training, preprocessing is essential. According to Dakhil et al. (2024), this procedure frequently entails face detection, which involves identifying and cropping the face from the background, image normalization, which standardizes pixel values, alignment, which modifies facial landmarks for consistent orientation, and resizing, which guarantees uniform image dimensions for neural network input. By supplying clean, aligned, and standardized input data, these preprocessing methods increase model accuracy by lowering noise and inconsistencies that can impede learning.

One important method for increasing the variety of training data and avoiding overfitting is data augmentation. The training dataset's size and diversity are artificially increased using data augmentation, which applies random alterations such rotation, scaling, flipping, and color adjustments. This improves the model's generalization and robustness in various scenarios (Saraiva et al., 2024). For instance, faces in photos can be slightly rotated or translated to simulate different angles. This is crucial for real-world facial recognition applications since faces are rarely photographed directly. The resilience of the model can also be increased by simulating various environmental circumstances by adjustments to the lighting, contrast, or color balance of the photographs. Although data augmentation enhances speed, it also brings up security issues, especially with regard to privacy and the possible exploitation of biometric information. It is crucial to make sure that training data is anonymized and managed securely because facial recognition systems depend on gathering and storing sensitive biometric information. To stop unwanted access or misuse of face data, data encryption, safe storage, and adherence to data protection laws like the GDPR are crucial. Furthermore, appropriate anonymization methods must be used to guarantee that people cannot be readily identified or followed without their permission. These security factors are essential for protecting user privacy and averting moral dilemmas related to surveillance and the gathering of biometric data.

3.3 Integration with Attendance Systems:

There are many benefits to integrating facial recognition with automatic attendance systems, including increased precision, effectiveness, and user-friendliness. Facial recognition serves as the main means of identifying and validating people in these systems, automating the attendance procedure without the need for human involvement. Usually, the integration entails taking a picture of a person's face using a camera, analyzing it using a facial recognition algorithm (such CNNs or YOLO), and comparing it to a database of previously registered facial photos connected to employee or student IDs. When a match is discovered, the system immediately logs the person's identity, time, and date of attendance. Traditional techniques like roll calls and swipe cards, which can be laborious and prone to human error, are no longer necessary as a result (Khairnar et al., 2023). Additionally, facial recognition guarantees a contactless and sanitary procedure, which is especially helpful in settings like workplaces, public institutions, and schools where a lot of individuals need to be monitored on a daily basis (Sheikh et al., 2023). By decreasing inconsistencies in attendance data, the automated structure of the system also increases accuracy and lessens administrative duties. However, integrating facial recognition with attendance systems presents a number of significant technical obstacles. Accurate recognition can be hampered by environmental variability, which includes variations in illumination, face angles, and facial obstructions like masks or spectacles. In order to overcome this, systems frequently use deep learning models that are resilient to changes in face location and lighting, as well as preprocessing methods such face alignment and normalization to guarantee consistency in the input data (Kou et al., 2024). Assuring real-time processing is another difficulty because, in order to remain effective, facial recognition systems must swiftly scan video streams and compare faces to a sizable database, especially in expansive settings like corporate buildings or campuses. To guarantee that the system can process numerous photos at once without any delays, this calls for strong hardware, like GPUs, and optimization strategies (Liu et al., 2024). Another issue is scalability, since the system needs to be able to process photographs in real-time while maintaining accuracy even when handling an increasing number of users. By allowing for decentralized processing and dispersing the computational load, cloud-based solutions and edge computing can assist mitigate these problems (Şengönül et al., 2023).

Given the sensitivity and privacy concerns surrounding facial data, security presents even another formidable obstacle. Data encryption and secure storage procedures are crucial to reducing these problems and guaranteeing that attendance records and facial photos are shielded from breaches and unwanted access. These solutions aid in guaranteeing the system's dependability, security, and privacy—all of which are essential for effective implementation in practical applications.

SYSTEM ARCHITECTURE

An AI-driven facial recognition-based security and attendance system's system architecture is made up of a number of essential parts that cooperate to provide precise identification, data storage, and real-time alerts. The system's main components include a secure database, facial recognition algorithms, an input interface (camera or video stream), and an alarm system that notifies managers of any unauthorized access or irregular attendance.

Initially, the system uses cameras positioned in key areas to record live video or pictures of people. A facial recognition model, usually built on deep learning methods like Convolutional Neural Networks (CNNs), processes the input. The eyes, nose, and mouth are among the face traits that these models are trained to recognize and extract for use in identification. In order to ensure that faces are properly oriented for identification, facial feature mapping entails locating landmarks within the image and aligning them to a consistent reference frame. To confirm the person's identification, the model then matches the identified face with pre-registered information kept in a secure database (Nallappan & Mahendiran et al., 2023). When a user approaches or enters the monitored region of the system, the facial recognition model can identify them in real time by continuously processing incoming video frames and matching features. Facial templates or feature vectors, which depict the distinctive features of each registered person's face, are kept in a secure database for identification verification. Because it enables the recognition model to compare current input with known identities, this database is crucial to the system's functionality. To prevent unwanted access to this sensitive data, security measures like encryption are put in place. In order to keep the system scalable and responsive to evolving requirements, the database can be dynamically updated to add or remove users. Furthermore, the system guarantees that all biometric data is anonymised and safeguarded in compliance with privacy laws like the GDPR in order to allay privacy worries (Falalu et al., 2023).

The system records attendance or provides access after the facial recognition procedure is finished and the user's identification has been verified. The system triggers an alarm mechanism if it detects any suspicious activity or an unauthorized person. The notification system is made to deliver alerts in real time over a variety of channels, such as email, SMS, and app notifications. This guarantees that any security breaches or problems pertaining to attendance are promptly communicated to the system administrators or security staff. Key information including the ID, location, and time of entrance of the discovered individual are included in alerts, enabling prompt action. Furthermore, if an intruder is identified, the system can initiate measures like locking doors or alerting the appropriate authorities for increased security (Şengönül et al., 2023). An effective, safe, and automated solution for security and attendance management is offered by these interconnected parts that function flawlessly together.

APPLICATIONS and CASE STUDIES

With notable gains in accuracy, productivity, and security, AI-powered facial recognition systems have found a wide range of uses in academic, institutional, and smart building settings.

By automating the roll-call procedure, facial recognition software is revolutionizing attendance management in educational settings. Conventional attendance techniques, including card swipes or manual sign-ins, can be laborious and prone to human mistake. AI-powered facial recognition ensures precise and instantaneous data gathering by automatically recording attendance as students enter the classroom. Teachers or administrators may concentrate on more crucial duties using this technology, which also removes the need for manual entry and lowers the possibility of fraud (such proxy attendance). Additionally, by lessening the likelihood of impersonation, it gives pupils a safer atmosphere. This technology is being used more and more by colleges and universities to increase productivity, increase accuracy, and expedite administrative duties (Barhate et al., 2024). In addition to being easily scalable to accommodate sizable student populations, the system offers insightful data on attendance trends, such as tardiness or frequent absences, which can be utilized to guide interventions or academic help. Facial recognition is essential for improving security in institutional settings by prohibiting unwanted entry to restricted areas. This is especially crucial in settings where assets or sensitive data must be safeguarded, like government buildings, company offices, and research labs. A smooth, contactless substitute for conventional access control techniques like keycards, PINs, or security personnel is offered by facial recognition software. These systems assist lower the danger of internal theft, unlawful entry, and other security breaches by making sure that only authorized individuals may access specific locations. The system's real-time alerting capability adds an extra degree of security by assisting security staff in reacting promptly to possible threats. For example, the system can instantly alert security and initiate alarms or lockdowns when someone tries to enter a secure area without permission (Barcic et al., 2023). It is increasingly common practice to include facial recognition technology into access control systems in order to improve institutional security. Facial recognition's wider ramifications can be seen in smart building management, where AI technologies are applied to improve security, energy efficiency, and building operations. Facial recognition technology can be used in smart buildings to monitor occupancy in different rooms or floors in addition to controlling entry, ensuring that space is used effectively. Furthermore, a more comprehensive and automated management strategy is made possible by combining facial recognition with other building management systems (including lighting, HVAC, and security). For instance, the system can improve energy efficiency by modifying temperature and lighting settings according to the number of people in a space. Additionally, by offering personalized settings, like preferred lighting or workspace modifications, based on the user's identity, facial recognition can be utilized to personalize the user experience (Zareinia & Kourosh, 2023). These systems' scalability enables their use in a variety of settings, including urban smart towns, big corporate buildings, and small offices. Incorporating AI with the Internet of Things (IoT) will probably be crucial to future urban development as more buildings implement these technologies, helping to build smarter, more effective cities.

CHALLENGES and LIMITATIONS

Although facial recognition technology has advanced significantly in recent years, it still has a number of ethical and technical drawbacks. The issue of privacy is among the most important ethical ones. Biometric information, including extremely sensitive personal data, is frequently gathered and stored by facial recognition systems. This calls into question the possible misuse of such data, such as the establishment of databases that track people's movements in both public and private settings or the use of such data for surveillance purposes without consent. These issues are especially important when it comes to surveillance in public areas, where people might not be able to give their agreement before data is collected. The possibility of data breaches, in which hackers obtain illegal access to face data and suffer grave repercussions like identity theft, exacerbates privacy concerns even further. Concerns about bias in facial recognition systems are present in addition to privacy issues. Numerous facial recognition algorithms have been found to be less accurate in detecting members of specific demographic groups, including women, older adults, and people of color (Schuett J., 2024). These prejudices have the potential to worsen already-existing societal injustices by producing unfair results like misidentification or unfair treatment. In order to guarantee that face recognition technologies are utilized ethically and in accordance with data protection laws such as GDPR, it is imperative that these ethical issues be addressed. Technically speaking, accuracy and scalability are two other issues that facial recognition systems must deal with. Common problems include false positives and false negatives, in which the system either fails to recognize a person who is in the database (false negative) or mistakenly recognizes a person (false positive). Particularly in high-stakes applications like security and law enforcement, these mistakes have the potential to compromise the system's dependability (Barcic et al., 2023). It is crucial to use strong algorithms that can handle changes in lighting, angles, and facial expressions in addition to high-quality, diverse datasets for training in order to reduce these inaccuracies. It is still difficult to achieve near-perfect accuracy under all circumstances, though. An additional technological constraint is scalability. The computational demands on facial recognition systems rise sharply with the number of users. Processing video feeds from numerous cameras in real time demands a significant amount of processing power, which might be a constraint, especially in public areas or huge institutions with thousands of people. Systems frequently use cloud computing or edge computing to overcome these difficulties since they can lower latency and distribute the processing load (Şengönül et al., 2023). These methods do, however, also add new layers of complexity to data synchronization, network architecture, and security.

Lastly, a major obstacle is integrating facial recognition technology with existing systems. Many of the security and attendance systems in use today are based on antiquated technology, including PIN-based access control or swipe cards, which might not work with contemporary facial recognition software. It can be expensive and time-consuming to upgrade or replace legacy systems to support facial recognition, involving large expenditures for software, hardware, and training (Sheikh et al., 2023). Furthermore, integrating facial recognition with current infrastructures frequently entails overcoming user resistance to adopting new systems, data migration difficulties, and compatibility issues between new and old technology. Despite these obstacles, the development of more adaptable, modular solutions that can coexist with current technologies is making it more and more possible to integrate facial recognition technology with legacy systems.

CONCLUSION and FUTURE OUTLOOK

In summary, security and attendance management have been greatly revolutionized by AI-driven facial recognition systems, which provide more accuracy, efficiency, and scalability than conventional techniques. These systems have proven their capacity to carry out real-time identification verification in a variety of settings by utilizing sophisticated detection models like YOLO (You Only Look Once) and deep learning algorithms like Convolutional Neural Networks (CNNs). Processes have been expedited, security has been increased, and user experience has been improved by integrating these technologies into academic, institutional, and smart building management systems. But despite these developments, there are still issues, especially with prejudice, privacy, and system scalability. For these systems to realize their full potential, ethical issues pertaining to the usage of biometric data, the possibility of bias in facial recognition, and technical constraints like false positives and false negatives must be resolved.

Technology will probably concentrate on strengthening privacy protections, decreasing biases, and increasing accuracy. In order to guarantee impartial and equitable performance across a range of demographic groups, researchers are looking into ways to strengthen facial recognition algorithms against changes in ambient factors like lighting and face angle. By reducing the possibility of data breaches, the incorporation of federated learning—where data is processed locally on devices without the requirement for centralized storage—offers a possible remedy for privacy issues. More integration with other technologies, such edge computing and the Internet of Things (IoT), is also anticipated as AI systems advance in sophistication, allowing for smarter, more responsive systems. In addition to managing security and attendance, these technologies will be able to optimize building operations, customize user experiences, and boost overall productivity. As these technologies advance, it will be crucial to maintain a balance between innovation and morality to make sure facial recognition software is used sensibly and for the good of society at large. As we move forward, the ongoing advancement of facial recognition With advancements in hardware and software, AI-powered systems will become even more scalable in the upcoming years, allowing them to manage increasingly complex surroundings and greater populations. The future of AI-driven security and attendance systems will be shaped by the expanding use of facial recognition in smart cities and the creation of legal frameworks to protect privacy and security.

DECLARATIONS

Conflict of Interest:
The authors declare that there are no conflicts of interest regarding the publication of this paper.

Informed Consent:
Not applicable.

Ethical Approval:
Not applicable.

REFERENCES

[1] Şengönül, E., Samet, R., Abu Al-Haija, Q., Alqahtani, A., Alturki, B., & Alsulami, A. A. (2023). An analysis of artificial intelligence techniques in surveillance video anomaly detection: A comprehensive survey. Applied Sciences, 13(8), 4956. https://doi.org/10.3390/app13084956

[2] Sheikh, H., Prins, C., & Schrijvers, E. (2023). Mission AI: The new system technology. Springer Nature. https://doi.org/10.1007/978-3-031-21448-6

[3] Jang, K., Pilario, K. E., Lee, N., Moon, I., & Na, J. (2023). Explainable artificial intelligence for fault diagnosis of industrial processes. IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2023.3240601

[4] Shabbir, A., Arshad, N., Rahman, S., Sayem, M. A., & Chowdhury, F. (2024). Analyzing surveillance videos in real-time using AI-powered deep learning techniques. International Journal of Systems Assurance Engineering and Management, 12, 1-12.

[5] Essien, U., & Ansa, G. (2023). A deep learning-based face recognition attendance system. Global Journal of Engineering and Technology Advances, 17, 009-022. https://doi.org/10.30574/gjeta.2023.17.1.0165

[6] Eger, V., Sartor, S., Coppari-Hollmann, A., Milsztein, A., Borsutzky, A., Wieser, B., Harjes, F., Preuss-Neudorf, F., Tscherniak, I., Skupien, J., Seidou, J., Fall, K., Driese, L., Zimmer, L., Stein, L., Knoll, M., Uludoğan, M., Serbinova, M., Sindemann, N., Maurer, T. (2024). The future of software engineering and IT operations. Journal of Software Engineering, 4(2), 112-118.

[7] Talukder, A., & Ghosh, S. (2024). Facial image expression recognition and prediction system. Scientific Reports, 14. https://doi.org/10.1038/s41598-024-79146-z

[8] Dakhil, N., & Abdulazeez, A. (2024). Face recognition based on deep learning: A comprehensive review. Indonesian Journal of Computer Science, 13, 1-14. https://doi.org/10.33022/ijcs.v13i3.4037

[9] Azzalini, L., Blazquez, E., Hadjiivanov, A., Meoni, G., Izzo, D. (2023). Generating a synthetic event-based vision dataset for navigation and landing. https://doi.org/10.5270/esa-gnc-icatt-2023-202

[10] Barcic, E., Grd, P., & Tomicic, I. (2023). Convolutional neural networks for face recognition: A systematic literature review. https://doi.org/10.21203/rs.3.rs-3145839/v1

[11] Saraiva, R., Carvalho, P., Henriques, J., & Simões, M. (2024). Comparative analysis of data augmentation approaches for blood pressure prediction. 1-4. https://doi.org/10.1109/EMBC53108.2024.10781892

[12] Chen, P., Wu, L., & Wang, L. (2023). AI fairness in data management and analytics: A review on challenges, methodologies, and applications. Applied Sciences, 13(18), 10258. https://doi.org/10.3390/app131810258

[13] Koodalsamy, B., Veerayan, M., & Narayanasamy, V. (2023). Face recognition using deep learning. E3S Web of Conferences, 387, 1-5. https://doi.org/10.1051/e3sconf/202338705001

[14] Liu, D., Zhu, Y., Liu, R., Xing, Z., Geng, W., & Wang, Y. (2024). MSD-YOLO: An efficient algorithm for small target detection. https://doi.org/10.1007/978-981-96-2064-7_5

[15] Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions. Big Data Cogn. Comput., 7(1), 37. https://doi.org/10.3390/bdcc7010037

[16] Kou, Y., Jiang, Q., Zhang, J., Xin, J., Wei, P., Miao, S., & Chu, X. (2024). Learning dual aggregate features for face forgery detection. Neural Computing and Applications, 1-13. https://doi.org/10.1007/s00521-024-10700-6

[17] Nallappan, M. (2023). An intelligent facial recognition system using stacked auto encoder with convolutional neural network (CNN) approach. https://doi.org/10.12723/mjs.sp2.17

[18] Falalu, M. A., Umar, I., Ibrahim, A., Bari, A. S., Baballe, M. A., et al. (2023). A smart attendance system based on face recognition: Challenges and effects. J Math Techniques Comput Math, 2(5), 203-208.

[19] Zareinia, K. (2023). Navigating emerging cyber threats with AI-powered security solutions. Journal of Cybersecurity, 13, 202-210.

[20] Barhate, P., Ramdasi, I., Shaikh, I., Ingawale, V., Ingle, P., Ingle, P., & Jadhao, M. (2024). Innovative attendance tracking: Facial recognition. 1-6. https://doi.org/10.1109/ESCI59607.2024.10497364

[21] Schuett, J. (2024). Frontier AI developers need an internal audit function. Risk Analysis. https://doi.org/10.1111/risa.17665

[22] Singh, A., Bhatt, S., Nayak, V., & Shah, M. (2023). Automation of surveillance systems using deep learning and facial recognition. International Journal of Systems Assurance Engineering and Management, 14(Suppl. 1), S236–S245. https://doi.org/10.1007/s13198-022-01844-6

[23] Ponnusamy, S., Antari, J., Bhaladhare, P. R., Potgantwar, A. D., & Kalyanaraman, S. (2024). Enhancing security in public spaces through generative adversarial networks (GANs). In Advances in Information Security, Privacy, and Ethics (AISPE). IGI Global. https://doi.org/10.4018/979-8-3693-3597-0

[24] Boe, C.-H., Ng, K.-W., Haw, S.-C., Naveen, P., & Anaam, E. A. (2024). An automated face detection and recognition for class attendance. International Journal on Informatics Visualization, 8(3), 1146-1153. https://doi.org/10.1109/joiv.2024.000084

[25] Gupta, P., Ding, B., Guan, C., & Ding, D. (2024). Generative AI: A systematic review using topic modelling techniques. Data and Information Management, 8(1), 100066. https://doi.org/10.1016/j.dim.2024.100066

[26] Pandita, A., & Kiran, R. (2023). The technology interface and student engagement are significant stimuli in sustainable student satisfaction. Sustainability, 15(10), 7923. https://doi.org/10.3390/su15107923

[27] Sayyad, S., Mulla, A., Gote, N., Bhosale, P., Yadav, P., & Adsul, I. (2024). Face recognition for classroom attendance based on convolutional neural network. International Journal of Intelligent Systems and Applications in Engineering, 12(1), 474–479.

[28] Reddy, T. S., Sujatha, B., Kumar, V. G. V. P., Srihari, P., Harshitha, M. D., & Manohar, B. M. (2024). Facial recognition reinvented: Deep learning based security alert system. Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024), Advances in Computer Science Research, 112, 1220-1227. https://doi.org/10.2991/978-94-6463-471-6_117

[29] Dang, T.-V. (2023). Smart attendance system based on improved facial recognition. Journal of Robotics and Control, 4(1), 46-53. https://doi.org/10.18196/jrc.v4i1.16808

[30] Adetunji, T. O. (2024). Advancements in AI-powered facial recognition for secure user authentication in e-learning environments. Journal of Technology & Innovation, 4(2), 44-46. https://doi.org/10.26480/jtin.02.2024.44.46

[31] Kakarla, S., Gangula, P., Rahul, M., Singh, C., & Sarma, T. (2020). Smart Attendance Management System Based on Face Recognition Using CNN. 2020 IEEE-HYDCON, 1-5.