© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716854

Transplant Track: Privacy-Preserving Smart Attendance System with Face and Liveness Detection

K. KALYANBABU[1], T. RAGHUNATH[2], P. RAKSHAN[3], K. DAMODHAR RAO[4]
[1, 2, 3]*Dept of CSE, UG Student, Sreenidhi Institute of Science and Technology, Hyderabad.*
[4]*Professor, Sreenidhi Institute of Science and Technology, Dept of CSE, Hyderabad.*

Abstract - The conventional way of keeping track of attendance in learning institutions is through manual roll calls or physical biometric systems, which are not effective and could also pose security challenges in relationships with privacy. The study offers a smart attendance system that protects privacy through face recognition and face detection that are applied to edge devices. The system uses computer vision and deep learning technologies including the OpenCV, DeepFace, Dlib, MTCNN and FaceNet to identify and determine student faces in real time. Eye blink analysis is implemented to detect passive liveness in order to decrease spoofing attacks via photos or videos. Embeddings on the face are stored in an encrypted SQLite database with user identifiers being hashed with a hash (SHA-256) to improve the security of privacy. The attendance records are recorded on the local disk with time stamps and have been saved as an append only file (csv). The system does not require cloud storage and the risk of privacy is less because all data processing is done in the device, which is constructive. It is proven through experimental assessment that the system is highly recognition accurate with low latency, and thus can be used in classroom settings.

Keywords: Face Recognition, Privacy preserving systems, smart attendance, edge computing, liveness detection, computer vision.

I. INTRODUCTION

Conventional attendance systems have been in use in learning institutions over a long time but all of them have some form of limitation that influences the efficiency, security as well as reliability. The simplest and the most widespread one is manual attendance. Under this style, teachers call the names of students or give them a list of students. Although this can be easily used with no need of technological infrastructure, it is extremely time consuming particularly in the large classes. Also manual systems are susceptible to proxy attendance where one student can check the attendance on behalf of another hence decreasing the credibility of the data that is recorded. Attendance systems based on RFID were implemented to make the process automated and save time that was needed to mark attendance. In such an approach, students will be equipped with RFID cards that shall be scanned by a reader to automatically record the attendance. Despite the fact that this is a faster method of attendance as compared to manual attendance, it also comes with some disadvantages. RFID cards can be shared easily among the students where one student can mark another student. This poses security risks and reduces the accuracy of the attendance records. Biometric systems based on fingerprints offer better accuracy as opposed to those based on RFID since the prints are unique to a person. These systems can be able to authenticate the identity of a student more efficiently. Fingerprint systems however need physical contact with the scanner thus raising hygiene issues particularly in areas where the device has numerous users. Moreover, the wear and tear of the hardware can be a common thing with the frequent use and can slow down the attendance process when a large number of students have to authenticate in a daisy chain. The cloud based facial recognition systems are a more advanced solution whereby the facial images are recorded and processed in remote servers. Such systems machine attendance without the need to touch physically, and therefore are convenient and efficient. Nevertheless, the transfer of facial data to cloud computing environments and its storage triggers serious privacy and security issues. Exposing sensitive biometric information to unauthorized access, data breach or misuse can occur unless measures are put in place. In order to address these shortcomings, the proposed system proposes an edge-based privacy preserving facial recognition attendance system. All processing is done in edge devices rather than transmitting biometrics data to cloud servers. This method has a very low chance of invasion of privacy and at the same time, high recognition accuracy is guaranteed. Moreover, the liveness detection techniques are integrated, so the system is able to identify a genuine individual and spoofing attempts made by utilizing photographs or videos, and thus the attendance system is more secure and dependable.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716854

Fig:1 Face Recognition Attendance System

II. RELATED WORK

Various scholars have researched the use of automated attendance system based on facial recognition and computer vision technologies to enhance efficiency and accuracy of attendance system in learning institutions. Initial studies were devoted to the application of face recognition algorithms with the purpose of automating attendance marking. Agarwal (2024) proposed a facial recognition attendance system that used Haar Cascade face detector algorithm and Local Binary Pattern Histogram (LBPH) classifier. The system accesses the facial images of the students during student registration and compared them with the current camera feeds to take note of attendance automatically. The experimental results indicated that the system reached recognition accuracy of about 91 percent and this indicated that face recognition can be used to track attendance automatically. Nevertheless, the system did not have sophisticated security features like liveness detection, thus, it was prone to spoofing attacks by the use of photos. Face recognition and liveness detection A different study came up with a convolutional neural net (CNN)-based system of face recognition and liveness detection to make attendance automatic. The proposed system (used face recognition algorithms and liveness detection) was able to distinguish real faces and spoofing attempts. To detect faces, the Haar Cascade classifier was used and to recognize the faces; LBPH algorithm and a CNN-based model was used to authenticate the facial liveliness. The results of the experiments demonstrated that the use of liveness detection enhanced the security of the attendance system and facilitated in eliminating fraud attempts of marking the attendance. There is also recent research on improving attendance systems with deep learning models and improved computer vision frameworks. As an example, a study released in 2024 suggested a facial recognition attendance system based on video processing in real-time and deep neural networks. The system was built using machine learning algorithms and Python libraries: OpenCV and TensorFlow, and it was able to identify and recognize student faces automatically. The solution greatly minimized the number of labor required to perform duties and enhanced the attendance management system since it was able to recognize automatically under different lighting conditions and different angles of viewing. The other study examined the performance of smart attendance monitoring systems based on the current deep learning methods, including YOLO-based face detection models and InsightFace recognition models. The system was found to be more accurate in detection and have higher processing rates than the conventional approaches, and this shows the prospects of using modern neural network designs in real-time attendance. The systematic review of face recognition attendance systems has also shown that the present solutions given extensively tend to achieve higher recognition accuracy without addressing the issue of privacy protection and anti-spoofing as a whole. The review has indicated that the existing deployments seldom combine high-precision recognition, multi-layer liveness detection as well as secure data control inside a single framework. Resting on the examination of the earlier research, one can conclude that automated facial recognition-based attendance systems have some great benefits compared to the conventional ones. Nevertheless, a number of issues, such as privacy protection, prevention of spoofing, and safe data storage, are still there. In order to present such problems, the suggested system proposes a privacy-aware edge based smart attendance system that achieves a facial recognition on the edge devices and adds liveness detection and secure data processing protocols. This strategy is meant to boost the security and reliability levels of the automated attendance management systems.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716854

III. BACKGROUND AND PURPOSE

In recent years, the facial recognition technology has received much awareness because it can be used to identify individuals based on the unique facial features. Deep learning algorithms are used in modern systems to extract distinguishable features on the images of faces and transform them into a numerical representation called embeddings. A number of works have shown that the convolutional neural networks are useful in recognizing faces. Embedding models like FaceNet are able to create high-dimensional representations that are capable of capturing the marks of the facial features. These embeddings make it possible to efficiently compare the facial data stored with the images recently acquired. Although face recognition has benefits, the privacy issue is a very crucial problem. Biometric data is processed with the help of many systems that use centralized servers or cloud infrastructure. This is because such methods pose the risk of data leakage, unauthorized access, and even misuse of personal information. This study is aimed at creating the safe and privacy-aware attendance system that will meet the following objectives: Facial recognition should be used to automate the process of marking attendance. Secrecy of the sensitive biometric information by local processing and encryption. Detection of liveness will help to prevent spoofing attacks. Give quick and correct identification which is appropriate in the classroom set up. Integrating data management with secure computing methods.

IV. PROPOSED METHODOLOGY

The proposed system has a methodology that consists of several steps, which together make it possible to track the attendance safely and automatically.The initial step is data acquisition, in which images are obtained with the help of a camera device integrated with the edge computing platform. The real-time processed captured frames are then examined by the face detection phase where the position of faces in every frame is searched using the MTCNN algorithm. This model can do face recognition with different lighting conditions and orientations. After the detection of faces, the feature extraction step applies the FaceNet model in order to produce embeddings of distinguishing facial features. These embeddings are numerical vectors which can be compared using identity comparison which can be achieved effectively based on the similarity measures in the database like the EUclidean distance.Face matching stage involves the comparison of the generated embeddings with the ones stored in the database.

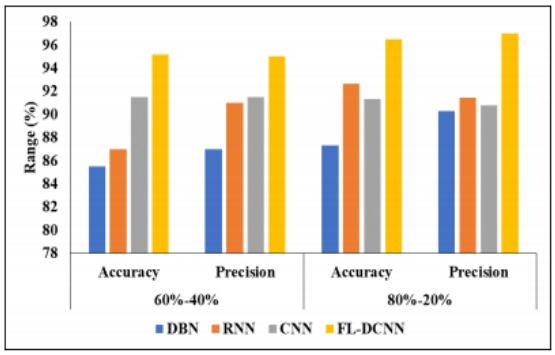

Fig:2 Analysis of models

In case the similarity score is less than a specified value, the identity is authenticated.Liveness detection is applied to strengthen the system security through blink. The Dlib library locates face features and monitors eye movement to ensure the presence of the subject physically and writes the confirmed identity of the student, date and time in a CSV file. It is a permanent record of attendance which is easily obtained and used by the administration.

V. SYSTEM ARCHITECTURE

The smart attendance system suggested adheres to a modular system which has a number of interrelated modules that perform image capture, face recognition, face detection, and attendance taking. The system starts with a camera module which records real time video frames of the classroom setting. These are forwarded to the face detection module, which locates human faces in the picture with the help of MTCNN model. After a face has been identified, a region with the face is obtained and passed on to the feature extraction module. The extraction of features is done through the FaceNet deep learning model to produce a distinctive embedding, which also signifies the facial features of the identified person. The similarity measures are then used to compare these embeddings to already stored embeddings in the local database. The liveness detection module is used to compare facial landmarks with the Dlib library in order to stop spoofing efforts by utilizing photographs or videos. The system will identify eye-blink patterns to ensure that the recognized face on the person is not that of a dead image. After verifying the identity of the individual and successful liveness detection, the attendance

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716854

management module registers the attendance of the student as well as time stamp. It is recorded in an append only CSV file to ensure the traceability and ensuring unauthorized changes. All of the facial embeddings are stored in the secure SQLite database, with the user identifiers being hashed with the assistance of the SHA-256 algorithm. The design eliminates the risks of security breach of vital biometric data and ensures efficient system operation.

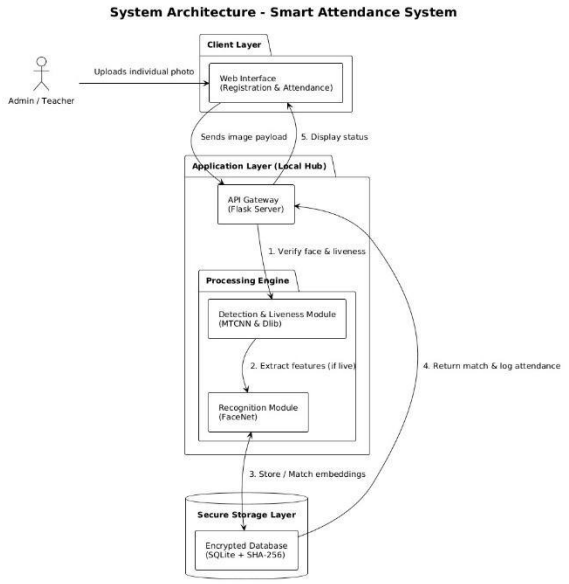

Fig:3 System Achitecture

VI. ADVANTAGES

The Privacy-Preserving Smart Attendance System with Face Detection suggested has a number of benefits over the conventional methods of attendance and the currently existing automated systems. Among the major benefits of the system is that the attendance is automated. With the facial recognition system, the system automatically detects students and takes an attendance without the involvement of the instructors. This saves time that can be used in attending to the marking during the classroom sessions and enables the instructors to devote more time to the teaching activities. The other significant benefit is that the system is contactless. The proposed system identifies people by using facial recognition with a camera unlike other systems that are based on biometrics that use fingerprints by physical contact with a scanner. This method removes hygiene issues and it is also effective in a setting that has more than one user of the equipment. There is also increased privacy protection of the system. Most of the current facial recognition systems are based on cloud-based servers to process and store biometric data, which may make sensitive information vulnerable to security attacks. Conversely, the proposed system handles all the facial data on edge devices. This means that biometric data will be stored in the local infrastructure of the institution and the chances of data leaks or data intrusions are minimal. The other benefit would be the incorporation of liveness detection measures. Blink detection is also made within the system by means of facial landmark analysis to ensure the face that is identified as that of a person is real. The system is also assuring in terms of secure storage of biometric information. The system manages facial embeddings in an encrypted database as opposed to raw facial images. Moreover, the user identifiers are secured with the help of SHA-256 hashing that enhances personal data safety and prevents the possibility of reconstructing the personal details without the user's permission. Moreover, the system exhibits real-time performance, as well as high recognition accuracy because it uses pre-trained deep-learning models like MTCNN and FaceNet. Lastly, the proposed system is affordable and can be implemented easily. The fact that it can operate on widely used edge devices, e.g., laptops or embedded platforms, means that an institution will not be required to install costly infrastructures to deploy the system.

VII. LIMITATIONS

Although the proposed system has its strong points, it also faces some drawbacks, which should be mentioned. The reliance on the light conditions is one of the limitations. Facial recognition systems are mostly effective in sufficient lighting conditions. Lighting can be poor or excessive shadows and this can diminish the accuracy of detection and the performance of the system. The other limitation is associated with the facial occlusion and difference in appearance. In the event that a student is covered partially on the face by accessories like mask, scarf or giant glasses, the system might have a problem with the identification of the person. In the same way, major alterations in the appearance, perhaps hairstyles or facial hair, may at times affect the accuracy of recognitions. The system is also based on the positioning of the cameras and quality of the image. When there is a low camera resolution or the camera is placed in the wrong position, it might fail to produce a clear image of the face and this can have

an impact on the detection as well as recognition performance. The other weakness is related to scalability in large classes. There is also a possibility that the system might take more time to process an image and identify more than one face as a large number of students can be seen at the same time in a frame thereby adding a little bit of latency to the system. Lastly, despite the fact that the system enhances privacy because it processes the data locally, it still needs to be keen on how the stored biometric embeddings are managed to ensure that they do not violate institutional data protection policies. The Privacy-Preserving Smart Attendance System based on Face Detection was tested in order to assess the system performance regarding the recognition accuracy, the ability to detect spoof and the response time of the system. The tests were done in a classroom-like set up with a regular webcam attached to an edge device running the Python-based implementation. The system used pretrained models which include MTCNN to detect faces and FaceNet to extract features. At the evaluation stage, the facial images of the registered students were taken and embedded into the local encrypted SQLite database. The system identified the faces of students in front of the camera and created embeddings, which were compared with the entries stored in the database to identify them. The attendance was automatically calculated in case of a match and the process of liveness was performed and the presence of a real individual was verified. The experimental findings indicated that the system was very accurate in recognition, which was able to identify most of the registered users in typical lighting conditions. Blink-based liveness detection that was successfully integrated minimized spoofing (attempts) with printed photographs and digital pictures that could be viewed on mobile devices. Besides accuracy, system latency was measured to establish the time that it takes to identify and recognize faces. The findings revealed that the system can recognize faces and mark attendance in a limited time period; hence, it can be applied in classrooms in real-time. The system does not need to be connected to a network because all computations are done locally in the edge device. Altogether, the results of evaluation confirm that the offered system can be used as the effective and trusted way of the automated attendance regulation and the high level of privacy is guaranteed.

VIII. FUTURE WORK

Despite positive outcomes of the proposed system, a number of enhancements could be researched in the future to improve the functionality of the system and its scalability. Among the possible extensions are the inclusion of the attendance system with the institutional management systems like learning management systems or academic information systems. This would allow automatic creation of attendance reports and give instructors real time monitoring capabilities. The other possible enhancement is the use of more sophisticated models of deep learning which can further enhance accuracy in recognition in difficult environments like low light, face covering or different camera angles. System robustness can also be achieved by training customized models with larger datasets. The future studies can also focus on the implementation of the system with embedded edge computers like Raspberry Pi or Jetson Nano to develop a small and affordable hardware platform that can be used in large-scale implementation by institutions. The system may as well be expanded to accommodate an array of cameras to control bigger classrooms or lecture halls in which more than one student should be tracked at a time. Lastly, additional efforts may be applied to the application of the multi-factor authentication methods, which will integrate facial recognition with other biometric or behavioral characteristics and enable an extra security approach. The following improvements can be also used to make the suggested system of maintaining privacy through smart attendance more efficient, scalable, and reliable.

IX. RESULTS AND DISCUSSION

The proposed Privacy-Preserving Smart Attendance System by using Face Detection was tested to determine the system performance in recognition accuracy, spoof detection, and the response time of the system. The experiments were done in a classroom-like setup where a standard webcam was used to connect to an edge device that was running the Python based implementation. Pretrained models like MTCNN to detect the face and FaceNet to extract features were used in the system.

At the evaluation stage, the face images of the registered students were captured and saved as embeddings at the local encrypted SQLite database. When students were shown before the camera, the system identified their faces, created embeddings,

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716854

and compared them with the stored entries in the database to identify them. The attendance was automatically identified as a match was found and as a real person was verified using the liveness detection.

The experiment revealed that the system was very accurate in recognition, and it was able to recognize most of registered users in normal lighting conditions. Blink-based liveness detection has been integrated effectively to prevent fake-ID efforts done through printed images and digital images on phone screens.

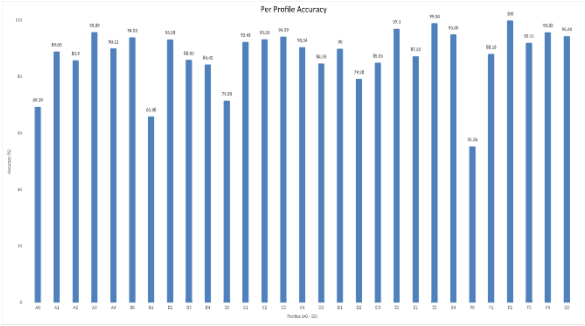

Fig 3:Results Graph

Besides the accuracy, system latency has been considered to establish the time taken to identify and recognize faces. The findings showed that the system takes a relatively short period of time in processing the facial recognition and attendance marking which do not render it inappropriate in real time classroom setting. The system is self-sufficient since all the calculations are carried out locally in the edge device, thus, no network connectivity is necessary.

On the whole, the results of the evaluation allow stating that the suggested system is an efficient and reliable solution of automated attendance management with high-level privacy protection.

Comparison of Performance (Sample Results)

Table 1: System Performance Metrics

MERICS	VALUE(%)
Recognition Accuracy	86.97%
Precision	95.1%
Recall	95.9%
F-1 SCORE	95.5%
SPOOF DETECTION ACCURACY	97.2%

X. CONCLUSION

This research presented a privacy-preserving smart attendance system based on facial recognition and edge computing technologies. The system was designed to automate attendance recording in classroom environments while ensuring the protection of sensitive biometric information. By integrating computer vision and deep learning techniques, the system is capable of detecting and recognizing student faces in real time.

Unlike many conventional attendance systems that rely on cloud-based processing, the proposed solution performs all operations locally on edge devices. This design significantly reduces privacy risks associated with transmitting and storing biometric data on external servers. Furthermore, the implementation of blink-based liveness detection enhances system security by preventing spoofing attempts using photographs or videos.

The use of pretrained models such as MTCNN and FaceNet enables the system to achieve high recognition accuracy and efficient performance. Additionally, the secure storage of facial embeddings using encryption and hashed identifiers strengthens data protection mechanisms.

Based on the experimental evaluation, the system demonstrates reliable recognition performance, low processing latency, and effective spoof detection. These features make the proposed approach suitable for deployment in educational institutions seeking a secure and automated attendance management solution.

REFERENCES

[1] Florian Schroff, Dmitry Kalenichenko, and James Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” in *Proceedings of the* IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, 2015, pp. 815–823.

[2] Kaipeng Zhang, Zhanpeng Zhang, Zhifeng Li, and Yu Qiao, “Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks,” IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499–1503, 2016.

[3] Davis E. King, “Dlib-ML: A Machine Learning Toolkit,” Journal of Machine Learning Research, vol. 10, pp. 1755–1758, 2009.

[4] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” in *Proceedings of the* IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 1701–1708.

[5] Jiankang Deng, Jia Guo, and Stefanos Zafeiriou, “ArcFace: Additive Angular Margin Loss for Deep Face Recognition,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 10, pp. 5962–5979, 2022.

[6] Stan Z. Li and Anil K. Jain, Handbook of Face Recognition, 2nd ed. London, U.K.: Springer, 2011.

[7] Paul Viola and Michael Jones, “Rapid Object Detection Using a Boosted Cascade of Simple Features,” in *Proceedings of the* IEEE Conference on Computer Vision and Pattern Recognition, 2001, pp. 511–518.

[8] Adam Geitgey, “Face Recognition Library Documentation,” 2020. [Online].