**Federated Learning-Based Attendance System Using InsightFace Embeddings**

Appala Srinuvasu Muttipati1,Nagireddy Kumar Sai2, Ajay Rapeti3 ,Sunkara Lochan Kumar4,

Koka Venkata Sai Charan5

Department of CSE (AI&ML, DS), Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam

**Abstract.** This paper presents a scalable and privacy-preserving attendance system that integrates federated learning with InsightFace embeddings. Unlike centralized systems that store sensitive student data on a central server, our approach processes data locally on student devices. Only facial embeddings, numerical representations of facial features, are transmitted to a federated server for aggregation. This decentralized method significantly enhances privacy by eliminating the need to store sensitive biometric data in one location, reducing the risk of data breaches. This approach addresses key challenges, such as privacy concerns, scalability, and efficiency. By processing data locally and only aggregating model updates, the system minimizes latency and strengthens data security. Overall, the system leverages federated learning and advanced facial recognition technologies like InsightFace, offering a high-accuracy, low-latency, and secure solution for attendance management in large-scale educational institutions.

**Keywords:** Federated Learning, Face Recognition, InsightFace, Privacy-Preserving, Attendance System, ArcFace, Deep Learning**.**

**1.Introduction**

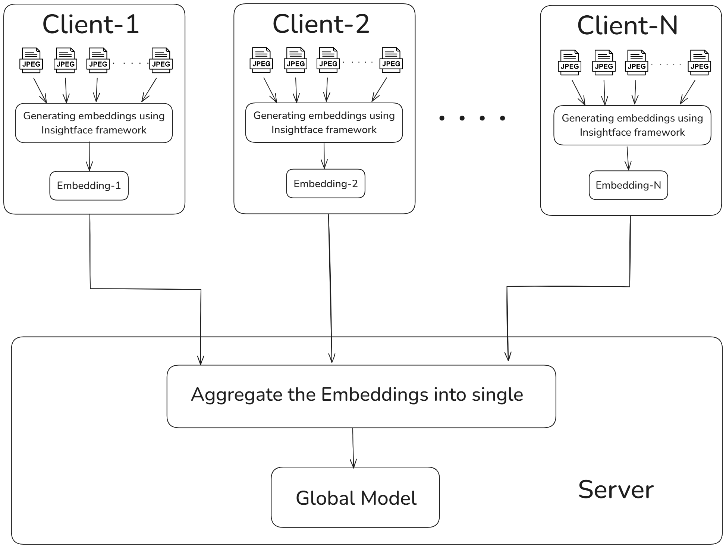
Attendance management systems play a critical role in educational institutions by tracking student participation, ensuring regulatory compliance, and promoting accountability. However, traditional methods like manual roll calls and centralized biometric systems come with significant limitations. Manual methods are time-consuming and error-prone, leading to inaccuracies such as proxy attendance, where students have others mark their presence. Centralized biometric systems, such as fingerprint or iris scanning, automate attendance but introduce challenges, including high infrastructure costs, hygiene concerns, and significant data privacy risks, as they store sensitive biometric information that can be vulnerable to cyberattacks. Facial recognition, driven by artificial intelligence (AI), presents a more efficient and hygienic solution by using cameras to capture student images and match them with pre-stored facial data for identification. This method is contactless, reducing hygiene risks, but centralized systems that store vast amounts of sensitive image data are still prone to security breaches and unauthorized access. Additionally, large-scale institutions may face performance challenges, including scalability and latency. Federated learning offers a promising solution to these issues by decentralizing data processing. Rather than transmitting sensitive raw data to a central server, devices process the data locally, sharing only model updates with the central server. This approach enhances privacy and security by ensuring that raw data never leaves the device, significantly reducing the risk of data breaches. It also improves scalability by distributing computational tasks across multiple devices, ensuring efficient performance even in large institutions. By integrating federated learning with advanced facial recognition technologies like InsightFace, educational institutions can create an attendance management system that is not only secure and privacy-preserving but also highly accurate, efficient, and non-intrusive, addressing both privacy concerns and scalability issues while enhancing overall system performance for modern academic environment.

**2.Related Work**

Traditional attendance management systems rely on manual roll calls and biometric verification methods such as fingerprint and RFID-based systems. While biometric systems enhance automation, they present challenges related to hygiene, infrastructure costs, and security risks associated with centralized data storage [1,2]. Face recognition has emerged as a contactless alternative, yet most implementations depend on centralized servers, making them susceptible to privacy violations [3]. Federated learning (FL), introduced by McMahan et al. [4], offers a privacy-preserving approach by enabling machine learning models to be trained across multiple devices without sharing raw data. The widely used FedAvg algorithm [5] aggregates model updates from distributed devices, with applications spanning healthcare [6], mobile applications [7], and financial security [8]. Several studies have explored FL for biometric authentication and privacy-preserving face recognition, with Zhuang et al. [9] highlighting its potential for decentralized identity verification. However, many attendance systems still use centralized architectures, posing privacy risks. Deep learning-based face recognition systems leverage embeddings to map facial features into high-dimensional space, significantly improving accuracy. Arc Face, introduced by Deng et al. [10], employs additive angular margin loss to enhance the discriminative power of facial embeddings, outperforming earlier loss functions such as SphereFace [11] and CosFace [12]. InsightFace, incorporating ArcFace loss, achieves high inter-class variance and low intra-class variance, making it highly effective for identity verification [13]. However, most existing implementations still rely on centralized storage, exacerbating privacy concerns. Privacy-preserving AI techniques, including differential privacy [14] and homomorphic encryption [15], further enhance security in machine learning workflows. Abadi et al. [16] introduced differential privacy in deep learning, ensuring models do not expose individual training samples, while Paper not et al. [17] proposed the Private Aggregation of Teacher Ensembles (PATE) method for improved privacy. These approaches, when integrated with FL, provide robust security while maintaining model performance. Despite significant advancements in face recognition, federated learning, and privacy-preserving AI, limited research has combined these techniques for attendance systems. This paper bridges this gap by proposing a federated learning-based attendance system using InsightFace embeddings, ensuring privacy, scalability, and high accuracy, addressing key concerns in modern educational settings.

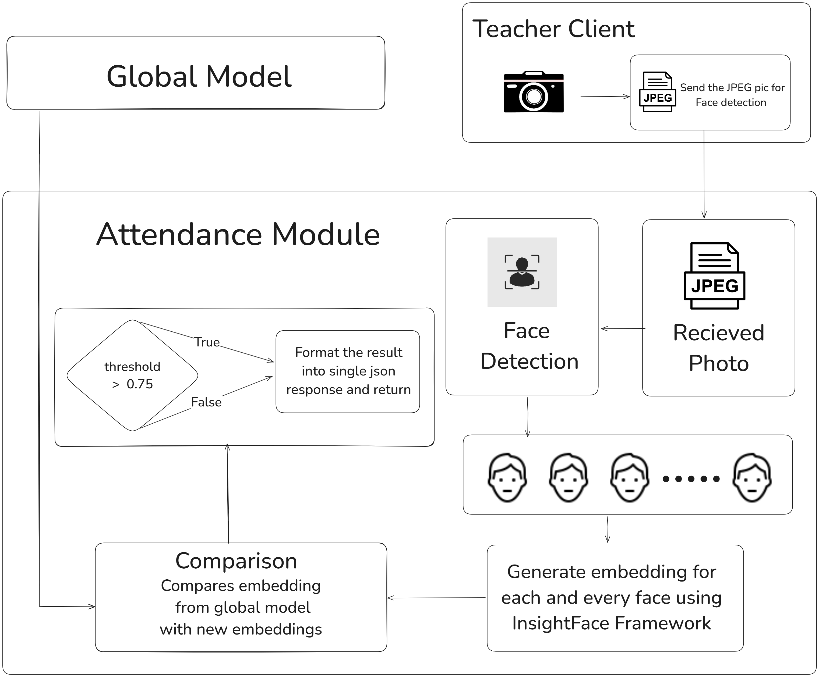
**3.System Architecture**

The federated model architecture enables secure and efficient facial recognition-based attendance systems by decentralizing model training. Instead of transmitting raw facial images, client devices locally generate facial embeddings using the InsightFace framework. These embeddings, which represent facial features numerically, are securely transmitted to a central server while preserving user privacy. The global model on the central server aggregates embeddings from multiple clients using federated averaging, refining its accuracy without directly accessing raw data. Communication overhead is minimized through techniques like quantization, which reduces update precision, and sparse updates, which transmit only significant model changes.

****

**Fig. 3.1.** This figure represents how multiple client devices generate embeddings locally using the InsightFace framework and send only the model updates to the central server.

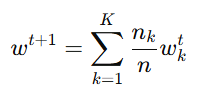
Secure multi-party computation ensures collaborative updates without exposing local data. The refined global model is then distributed back to clients for continuous learning. This decentralized approach improves accuracy, security, and adaptability while reducing risks associated with centralized data storage, such as breaches and unauthorized access. The integration of federated learning with InsightFace ensures high facial recognition accuracy while protecting data privacy. This architecture is particularly beneficial for educational institutions, ensuring compliance with regulations like GDPR and FERPA. By eliminating the need for centralized data collection, the system enables scalable and privacy-preserving attendance management. With its ability to continuously improve through distributed learning, the federated model offers a robust, secure, and efficient alternative to traditional biometric attendance systems.



**Fig. 3.2.** This figure illustrates the process of capturing student images, detecting faces, generating embeddings using the InsightFace framework, and comparing them against the global model with a similarity threshold to determine attendance.

The Attendance Module Architecture is designed to automate and streamline the process of tracking student attendance using facial recognition technology. It starts with capturing images of students, typically through a camera or a mobile device. These images are then processed to detect and extract the faces of the students present in the captured photo.Once the faces are detected, the next step involves generating embeddings using the InsightFace framework, a deep learning library that provides state-of-the-art performance for face recognition. The embeddings represent unique numerical features of each student’s face, allowing for accurate identification. These embeddings are then compared against a global model, which contains pre-trained data of all registered students' facial features.The comparison process calculates a similarity score between the student’s face embedding and those stored in the global model. If the score exceeds a predefined similarity threshold, the student’s attendance is marked as present. If the score is lower, the system determines the student’s face is not recognized, and their attendance is not recorded.Finally, the results, which include the attendance status of each student, are formatted into a JSON response. This response is sent back to the teacher’s client application for review and record-keeping. This automated system significantly reduces the time and effort required for manual attendance-taking, ensuring accuracy and efficiency in classroom management.

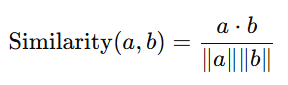
**4.Methodology**

Student devices capture facial images and generate feature embeddings locally using InsightFace. These embeddings are used to train a local model, which is then updated and shared with the federated server. The federated server aggregates the updates from multiple student devices using the Federated Averaging (FedAvg) algorithm, which ensures that the global model benefits from the collective knowledge of all participants while preserving data privacy. The Federated Averaging (FedAvg) algorithm, a widely used technique in federated learning, aggregates the local models by computing the weighted average of model parameters. The algorithm is mathematically expressed as:

where wkt represents the model weights from the k-th client at iteration t, nk is the number of training samples on the client, n is the total number of training samples across all clients, and wt+1 represents the updated global model. This iterative process continues until the global model achieves convergence, ensuring that all student devices contribute to model refinement without exposing their raw data.For facial recognition, InsightFace is employed to extract robust facial embeddings. InsightFace utilizes a deep convolutional neural network optimized with the ArcFace loss function, which enhances the discriminability of embeddings by introducing an angular margin between different identity classes. The ArcFace loss function is defined as:

A mathematical equation with black text

Description automatically generated

where θyi is the angle between the embedding and the target class center, m is the angular margin, s is a scaling factor, and N is the total number of samples. By maximizing inter-class distance and minimizing intra-class variance, ArcFace enhances the ability of the system to distinguish between different students even in varying lighting conditions, angles, and expressions.For attendance verification, the teacher’s device captures a class photo, from which faces are detected using a pre-trained Multi-task Cascaded Convolutional Network (MTCNN). InsightFace then extracts embeddings for each detected face. To determine student identities, cosine similarity is used to compare the extracted embeddings with stored student embeddings. Cosine similarity is calculated as:

where a and b represent two embedding vectors, and ∥a∥ and ∥b∥ are their respective magnitudes. If the similarity score between two embeddings exceeds a predefined threshold τ, the student is marked as present. The threshold is carefully chosen to minimize false positives and false negatives, ensuring high accuracy in attendance tracking.

**5.RESULTS AND DISCUSSIONS**

**INPUT 1:**

**Fig. 5.1.** This figure illustrates the process of capturing student images, through HaarCascading Technique and generating embeddings using the InsightFace framework .This System is implemented on 30 students in that particular class.each student taking 100 images.

**INPUT 2:**

**Fig. 5.2.** the test photo is captured by the teacher during his class ,where the respective students present in the trained data are seated in the classroom.

**OUTPUT:**

**Fig. 5.3.** the test photo is captured by the teacher during his class ,where the respective students indicated in green are considered as present and students in red indicate unknown in the classroom.

Number.of.Students Present-17

Number.of.Students Absent-13

Number of Student not registered(do not belong to that class)-02

(Roll Numbers of the Present Students are displayed with respective students and as end result)

**6.Conclusion**

The proposed attendance management system integrates federated learning with InsightFace-based facial recognition to offer a secure, scalable, and privacy-preserving solution. Unlike centralized systems that store sensitive data, this approach ensures facial data remains on student devices, reducing breach risks. Only essential model updates are shared, minimizing communication overhead while maintaining accuracy. Privacy-preserving techniques like differential privacy, homomorphic encryption, and secure multi-party computation further safeguard data, ensuring compliance with regulations like GDPR. The system leverages InsightFace’s ArcFace loss function for precise facial embeddings, ensuring high recognition accuracy. Its decentralized nature allows continuous improvement as new data refines the global model without compromising privacy, making it ideal for large institutions seeking a secure alternative to traditional attendance methods. Future advancements can further enhance system efficiency, including model compression techniques like knowledge distillation and quantization to optimize on-device computations, reducing latency and power consumption. Enhanced privacy methods, such as fully homomorphic encryption, will strengthen security while preserving accuracy. Integrating blockchain technology could provide tamper-proof attendance records, and real-time edge AI processing can reduce reliance on cloud-based computations, improving response times and scalability. Adaptive learning models may improve recognition under varying lighting and facial conditions, while multi-modal authentication—combining facial, voice, and behavioral biometrics—can enhance security. And provide efficient solution for modern attendance management in educational institutions.