Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2023 SCPE. Volume 24, Issues 3, pp. 191–201, DOI 10.12694/scpe.v24i3.2136

SYNCHRONOUS FEDERATED LEARNING BASED MULTI UNMANNED AERIAL VEHICLES FOR SECURE APPLICATIONS

ITIKA SHARMA[*] SACHIN KUMAR GUPTA[†] ASHUTOSH MISHRA[‡] AND SHAVAN ASKAR[§]

Abstract. Unmanned Aerial Vehicles (UAVs), also known as drones, have rapidly gained popularity due to their widely employed applications in various industries and fields, including search and rescue, agriculture, industry, military operations, safety, and more. Additionally, drones assist with tasks such as search and rescue efforts, pandemic virus containment, crisis management, and other critical operations. Due to their unique capabilities in image, video, and information collection, a multi-UAV system plays a crucial role in these activities. However, such images and video data involve individual privacy. Therefore, such multi-UAV applications have an indigenous tradeoff of privacy preservation. We have proposed a Federated Learning (FL) based approach for ensuring privacy in multi-UAV applications. The proposed methodology utilizes a synchronous FL approach and the Convolutional Neural Network (CNN) to ensure security. The model parameters are protected by using a secure aggregation. Results demonstrate that the proposed approach outperforms existing techniques in terms of accuracy and precision.

Key words: Federated Learning, Machine Learning, Privacy, Security, Unmanned Aerial Vehicles

1. Introduction. Unmanned Aerial Vehicles (UAVs) or drones, have experienced tremendous growth in both the industrial and academic fields. Drones play a crucial role due to their unique characteristics and ability to perform critical tasks such as capturing images and videos. The market value of UAV usage in civil infrastructures exceeds 45 billion dollars. A drone, also known as a UAV, is an aircraft that operates without an onboard operator or crew. Drones were first used in Italy in 1849 during the struggle for independence between Venice and Austria. Austrian soldiers attacked Venice using bomb-laden hot-air, hydrogen, or helium-filled balloons. In 1982, the Israeli Air Force utilized UAVs to destroy the Syrian fleet while minimizing Israeli losses [1]. Israeli UAVs were employed as a deception tactic, disrupting communications and providing real-time video surveillance. The rapid adoption of drones over the past decade has raised concerns about privacy, security, and safety. Drones are used by travelers and paparazzi to capture images of individuals in their homes and other previously private locations. Additionally, drones are utilized in high-risk areas such as cities and airports. UAVs are an integral part of an Unmanned Aircraft System (UAS), which includes a controller and communication system for the UAV. Companies like Google and Amazon are developing drones to facilitate the delivery of goods by air. Another intriguing concept being explored by Facebook involves the construction of massive drones to provide direct internet access to remote areas. Lightweight synthetic structures are commonly used in the construction of unmanned aircraft to enhance maneuverability and manage weight [2]. Military drones, thanks to the strength of composite materials, are capable of flying at extremely high altitudes. The combination of drones and IoT technology has resulted in a surge of new commercial applications. UAVs integrated with IoT sensor networks on the ground can assist agricultural organizations in monitoring lands and harvests, enable energy companies to inspect power lines and operate equipment, and help insurance companies assess claims and policies.

[*] School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Kakryal-182320, Katra, (Jammu and Kashmir), UT, India (itikasharma142@gmail.com)

[†] Department of Electronics and Communication Engineering, Central University of Jammu, Samba, UT of J&K, 181143 India and School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra-182320, (UT of J&K), India (sachin.gupta@smvdu.ac.in, Corresponding Author)

[‡] School of Integrated Technology, Yonsei, University, South Korea, and the Department of Electronics & Communication Engineering, Graphic Era Deemed to be University, Dehradun 248002, Uttarakhand, India (ashutoshmishra@yonsei.ac.kr, Corresponding Author)

[§] Technical Engineering College, Information System Engineering Department, Erbil, Iraq (shavan.askar@epu.edu.iq)

ML techniques like differential privacy and homomorphic encryption have surged in IoT devices. Even commonplace items used by people in daily life, such as wearables, smart meters, and smart water meters, can be utilized with the Internet of Things (IoT) network to collect data from the environment using sensors and actuators. This data can then be used to solve a variety of problems in daily life. IoT has transformed traditional industries into smart ones, including smart waste management, smart grids, smart homes, and smart healthcare [3]. However, the heterogeneity of devices, energy shortages, restricted bandwidth, and other limitations pose challenges in implementing advanced security methods in IoT networks, making them more susceptible to destructive insider attacks [3]. Also, security problems lead to privacy-sensitive issues. There are security issues in IoT networks because central data is collected to train the model. So, protecting data is quite critical as there is a central server in a common model that works on training and test sets.

There are many challenges in UAV civil applications, including swarming challenges and network security challenges. Another issue is the scalability issue [4]. Therefore, the unacceptable latency and the raw data transfer to the server by UAV requiring high network bandwidth are the most significant issues faced by traditional ML. To handle these problems, we suggest using federated learning (FL) model that efficiently addresses all privacy and latency issues. Google introduced the first application of FL in 2016. They established FL to improve the predictive text on Google's Android keyboard. Apple also utilizes FL to enhance voice recognition on Siri. FL can protect clients' raw data and reduce communication costs. There is widespread use of FL in the healthcare system, where it securely handles data without sending raw data directly to the server [5, 6, 7, 8]. FL utilizes less complex hardware as it doesn't rely on a central server. Each UAV locally trains its models, and then the updated parameters are sent to the server and aggregated globally there [9, 10, 11, 12, 13, 14].

1.1. Key Contributions. The FL methodology has been used to address multi-UAV systems due to security concerns associated with DL-based methodologies that transmit raw data. FL was developed as a solution to this problem, aiming to store original data at its source and solely send locally trained models from users to the server for aggregation. Both asynchronous and synchronous UAVs are employed in conjunction with federated learning. Asynchronous federated learning allows for faster training of local models, but it entails a loss of data packets, resulting in subpar communication and diminished accuracy. Therefore, we utilize federated learning to effectively communicate and achieve accuracy. The key contributions of this study are as follows:

1. Application of FL in conjunction with multi-UAV systems to ensure privacy.
2. Utilization of convolutional neural networks (CNN)-based algorithm for model training.
3. Comparative analysis of the traditional centralized model versus the federated model.
4. Performance assessment of the federated models in terms of accuracy, precision, and recall.

The remainder of the paper is structured as follows: part II reviewed related literature. The proposed model is illustrated in Section III. The debate and findings are examined in Section IV. Section V serves as the work's conclusion with its future scope.

2. Related Works. This section will differentiate the study of previous work done from our article by revealing the procurement of UAVs with FL. Al-Emadi et al. in [1] discussed a drone detection solution based on RF frequency. The author proposed a model for detecting and classifying drones using an RF signal and compared CNN and DNN. In this model, the author used a DL technique called CNN, which is an effective mechanism for drone detection. The proposed model was tested and trained using a dataset. To analyze and determine the performance of this model, the author made a comparison of data obtained with ANN, CFAR, and HOC. Due to its unique qualities that integrate feature extraction and classification into a single model, CNN has a wide range of applications, particularly in recognition and classification challenges. In this paper, the author claims to have achieved accuracy and provided better performance in drone detection as well as drone identification.

Brik et al. in [2] introduced the FL concept and its fundamentals. The author gives a broad overview of FL applications for UAV networks. The traditional DL methods use a centralized server to which the UAV data is directly sent. This creates issues in network communication overhead, leading to energy inefficiency and network bandwidth problems for UAV devices. Moreover, there may be private data like localization and identification of UAVs, which can directly impact UAV privacy. To address these concerns, the author introduced the FL concept, where data is not directly sent to the server. The basic concept behind UAVs is to preserve raw data where it is created and locally train the models. In this paper, the author discusses the open issues and challenges in the FL approach.

In [3], Ahmad et al. demonstrated malicious attacks in the IoT using supervised machine learning techniques. The IoT was created to connect numerous smart gadgets and sensors for gathering and analyzing vital information online. However, the IoT network faces several limitations, including limited sensor computational capability, heterogeneity of gadgets, limited energy resources, and bandwidth, among others. These limitations prevent the use of high-end security techniques, making the networks more susceptible to insider assaults and other security threats. Additionally, due to the unexpected behavior and ubiquity of IoT networks, identifying malevolent insiders in the network is exceedingly challenging. Machine learning techniques can address these issues by forecasting anomalies in the system and understanding its behavior. The authors applied various supervised machine-learning approaches to the available IoT dataset to determine the most effective method for identifying hostile insider assaults in the IoT network. Multiple supervised algorithms were trained on the NSL-KDD dataset, and the results show that the Gradient Boosting technique outperforms the other covered techniques.

The FL-based approach is the suggestion made by Lim et al. [4] to enable security in IoV applications such as traffic forecasting. In this article, the authors have developed an FL-based detecting and collaborative learning scheme in which UAVs gather data and participate in private information collaborative model training for IoV paradigm applications, aiming to establish an Intelligent Transportation System (ITS). Additionally, the authors presented a multidimensional contrast matching-based reasoning framework layout that aims to utilize the self-revealing characteristics of an ideal contract to produce the most ideal UA. Yang et al. [5] suggested an asynchronous FL framework for multi-drone networks, which may provide asynchronous learning or distributed computing by allowing the training model to operate without transmitting or sending raw sensitive information to UAV servers. It also includes a device selection technique to prevent devices of poor quality from compromising efficiency and precision in learning. Furthermore, the author has proposed an asynchronous advantage actor-critic (A3C)-based combined device selection, UAV deployment, and resource management strategy to increase federated convergence speed and accuracy. Simulation results reveal that the suggested scheme and algorithm produce greater accuracy and quicker federation execution time than existing solutions.

Yang et al. demonstrated energy-efficient UAVs based on federated learning [6]. This article examines the problem of resource allocation for federated learning across UAVs and efficient energy transmission. With the goal of reducing the overall energy consumption of the devices while considering the delay restriction, both the challenges of local processing and transmission energy are approached as optimization problems. The author presents a solution to the energy minimization problem by providing the delivery time for the reduction problem and suggests a bisection-based strategy to obtain the optimal answer, which is a practical option due to the iterative technique recommended by the author. Khamidehi et al. proposed a federated-based architecture in order to shorten UAV flight times while maintaining reliable internet connectivity [7]. Since UAVs are unable to independently develop the global model, the author provides the following two options: (1) Using federated learning, the UAVs cooperate to build a large model to predict outages in the environment; (2) Based on a model created in the first phase using fast random trees (RRTs), the author provides a path-planning technique. The author devises an optimal course for UAVs that reduces travel time while ensuring cellular connectivity. In [8], Yazdinejad et al. proposed a federated learning approach based on deep neural networks (DNN) for drone authentication. By integrating drones with federated learning, maximum privacy is achieved. The author creates an authentication model based on the DNN Neural Network and the Federated Learning idea. This authentication mechanism federates the number of aircraft while maintaining anonymity. This approach protects privacy and utilizes DNN design to scale with a large number of drones. Secure aggregation techniques and cryptographic algorithms are used to safeguard secure parameters for the models. The author states that the simulation demonstrates a high True Positive rate and performs best when used with the training and validation datasets.

Tang et al. conducted research [9] to improve Federated Edge Learning (FEEL) for B5G/6G networking in the Internet of Things (IoT) enabled by UAVs. Federated learning is an effective framework for creating a decentralized shared paradigm between computers and edge devices without transmitting raw data. However, FEEL's performance in connected devices with UAV support is limited by two important factors: latency and energy consumption. While earlier research has focused on reducing latency and promoting energy efficiency, few studies have examined how the limited battery life of devices affects FEEL.

Wang et al. proposed an asynchronously federated learning system based on a permissioned blockchain in [10]. The article suggests a blockchain-based synchronization federated learning server that consists of a core blockchain and several sub-blockchains. Each sub-blockchain is responsible for updating a specific model parameter while the main blockchain updates all parameters globally. Based on this design, a permissioned blockchain technology federated learning synchronization aggregation protocol is suggested. This protocol combines second-order aggregation calculations with the learning algorithm to effectively replace concurrent federated supervised learning. As a result, synchronization problems are avoided and the reliability of distributed data is guaranteed. According to calculations and experimental results, the suggested architecture can maintain acceptable training results when working with a small number of nodes with varying data quality, has good automated failover, and can be expanded to edge computing applications.

In [11, 12, 13], the authors proposed a privacy computing system (AFLPC) for 5G-V2X scenarios using asynchronous federated learning to address potential privacy leakage issues at the network edge in the 5G V2X environment. This model combines secure computing and asynchronous federated learning. The article introduces an adaptive independent privacy strategy to protect parameter privacy and reduce the impact of noise on model validity. To address the consolidation issue of asynchronously federated learning based on moving averages in practical applications, an aggregate approach based on weighted summaries is recommended. The proposed asynchronous federated instruction and learning mechanism primarily focuses on the 5G V2X environment, but further investigation into other settings is also suggested [14, 15, 16, 17, 18]. Results from the study conducted using the MNIST and CIFAR-100 datasets demonstrate that the approach described in this article can provide high precision in terms of confidentiality and safety, solve the issue of diminishing model calculation time caused by variations in node learning speed, and improve the productivity of AFL.

The use of "UAV with FL" demonstrates that when UAVs are used with federated learning, it ensures the privacy of transmitted data without any loss and avoids communication overhead. This leads to efficient network bandwidth and energy utilization. In traditional DL-based UAVs, the original information is sent to a central server, which creates issues related to network bandwidth, energy efficiency, and privacy. Due to these concerns, the concept of federated learning is now being used, where only local models are transferred instead of the original information. This approach offers the benefits of privacy, energy efficiency, and network bandwidth.

3. FL: A System Model. This section covers the proposed model, the function of FL in UAVs, the function of CNN, and the encryption technique utilized in the FL process.

3.1. Proposed Model. The majority of machine learning (ML) techniques are cloud-based, which means that data must be transferred to and analyzed in a single location, such as a database server. However, these ML methods are not suitable for UAV-wireless networks due to several reasons. Firstly, since the generated data could contain sensitive information like the location and identification of UAVs, the private data might not be accessible. Secondly, the continuous transmission of unprocessed data by UAVs, such as images, videos, and other types of data, to the server requires a high network bandwidth and consumes more UAV energy, especially when bandwidth and UAV energy are constrained.

Moreover, cloud-centric approaches introduce significant latency, particularly for applications that require instantaneous decisions, like unmanned drone monitoring and UAV-based virtual reality applications. Therefore, decentralized teaching methods are crucial for effectively managing scattered sub-datasets produced by UAV instruments. In 2016, Google introduced Federated Learning (FL) as a novel form of AI that moves training to the edge or on-device. FL is based on decentralized data and training, enabling multiple parties to collaborate on a shared, robust ML model without disclosing data. It addresses critical issues related to data confidentiality, safety, data login credentials, and access to heterogeneous data.

In our proposed model, we incorporate privacy by deploying multiple UAVs and utilizing FL. The server sends the model to each UAV for training, and these neighboring UAV clients regularly exchange the model parameters. Before delivering these parameters, several models encrypt them, thus enhancing data security and protection. The features of the global model are sent to data centers to include them in their ML model

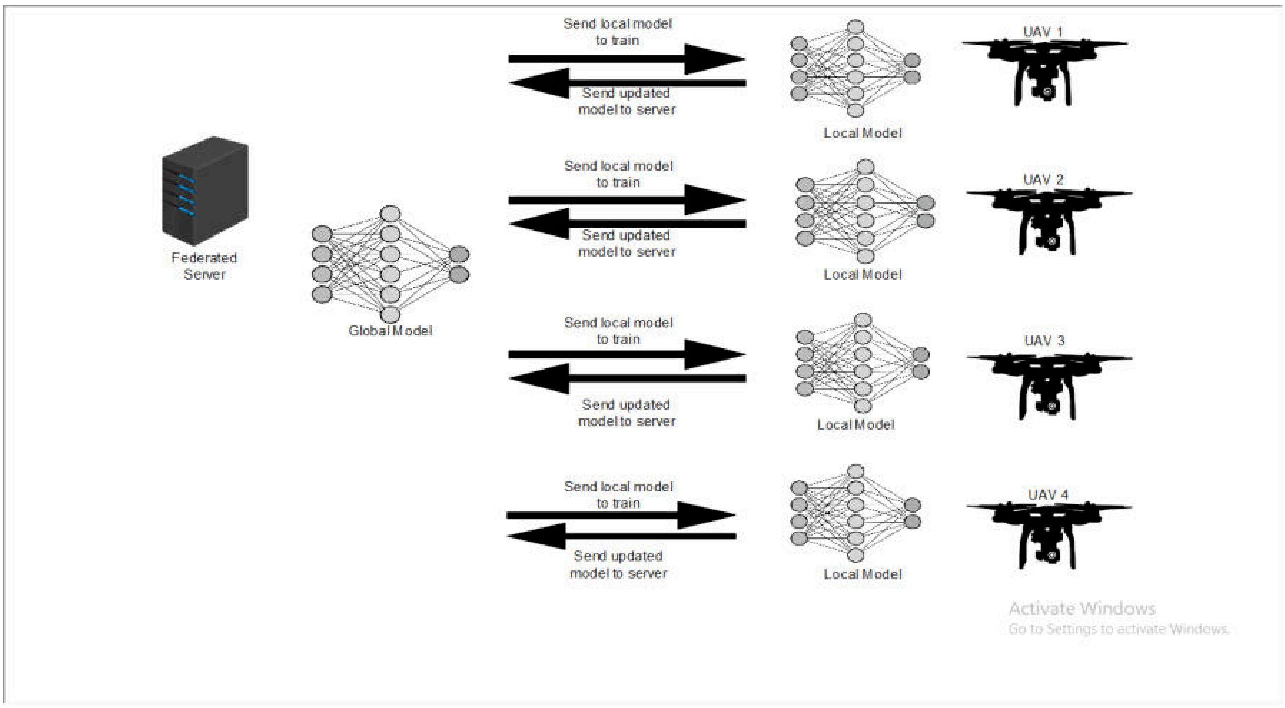
Send local model to train
Send updated model to server
Local Model
UAV 1
Federated Server
Global Model
Send local model to train
Send updated model to server
Local Model
UAV 2
Send local model to train
Send updated model to server
Local Model
UAV 3
Send local model to train
Send updated model to server
Local Model
UAV 4
Activate Windows
Go to Settings to activate Windows.

Fig. 3.1: FL Process

parameters. Each UAV then trains the model on its own data before sending the revised model back to the server. The models are globally aggregated at the server, and the process is repeated until the desired accuracy is achieved. As a result, privacy is ensured as raw data is not sent directly to the server; only models are transmitted. Secure aggregation, which encrypts both the data and the model, is employed in our work. Secure aggregation is essentially a protocol used for privacy-preserving federated learning. It enables the aggregation of models without revealing individual models, thereby preventing the disclosure of private information from both individual and local models. This aggregation ensures that the server cannot access the private data of the local models. Additionally, Fig. 3.1 illustrates the federated learning process. First, the FL server creates the global model G0 and sends the UAVs the requirements for data types and training parameters. To prevent the exhaustion of the UAV's resources, the FL server displays the number of iterations and the learning rate. For each UAV I start gathering information and updating local parameters, Lij. Using the global model Gj (j is the iteration index), UAVs also search for the optimal settings to minimize the loss function. The modified settings are then provided to the server. The FL server compiles the local updates and sends the refreshed parameters to the UAVs. The purpose of the FL server is to minimize the overall global loss function (Gj) as shown in equation (3.1):

$$Loss(G^j) = \frac{1}{M} \sum_{i=1}^{=M} Loss(L_i^j) \tag{3.1}$$

In the initial stage of implementation, each UAV receives models from the server. The initial stage of the suggested methodology's implementation includes sending models to every local UAV client. The second phase of implementation will then begin after the training procedure has been finished. Each UAV client begins the training process using their own data in the second phase. The trained model will then be sent back to the drones in a third stage when there is no or low accuracy from the server and federated server. The procedure will continue until the correctness of the data is maintained. After the servers have globally combined the federated learning model and accuracy is maintained, the federated server will broadcast the globally aggregated model.

3.2. Role of FL in UAVs. Security risks are increasing every day as the number of UAVs rises. Each day, a large number of drones are being attacked. Therefore, there is a critical demand for highly secure drones. Several researchers have developed AI-based drones and incorporated privacy into them using the concepts of ML and DL. However, there have still been some issues with achieving truly secure communication. To address this problem, the concept of FL was introduced.

FL is an ML method that involves training an algorithm on numerous decentralized edge devices or servers. Each device or server retains local data samples and does not share them. In contrast, conventional DL-assisted systems are centralized and rely on servers to receive and store UAV data. However, UAVs are resource-constrained devices, particularly in terms of CPU and electrical resources. By avoiding the transfer of data to a central organization, FL significantly reduces network overhead. Consequently, FL utilizes less bandwidth compared to centralized ML systems.

This implies that FL may enable the training of learning models for UAV wireless communication in the future, in contrast to cloud-centric approaches that are centralized. FL avoids transmitting sensitive information to a single node, ensuring the security of UAV data while also reducing network costs and latency. In our work, we focused on the CNN model for the training phase. Although any NN can be used for training, the CNN model offers advantages in terms of computational efficiency, memory efficiency, and complexity efficiency. FL is increasingly being adopted in various domains, including healthcare, autonomous vehicles, mobile applications, predictive maintenance in industries, and others.

3.3. Role of CNN Model. A Convolutional Neural Network (CNN) is constructed with a convolutional layer that performs a process known as convolution. During the convolution process, the input undergoes convolution with filters, leading to activation. CNN has a broad range of applications in object recognition and is primarily employed in image classification to evaluate visual information. CNN can be utilized for tasks such as image and video categorization, identification, medical image analysis, and recommendation systems. Convolutional, ReLU, Pooling, and Fully Connected (FC) layers are the concealed layers within a CNN.

3.4. Homomorphic Encryption. Rivest et al. began their exploration of the creation of the homomorphic encryption (HE) method in 1978. HE is a unique encryption method that addresses security and privacy concerns. One option is to encrypt both our models and data. This encryption technique allows data to remain encrypted while being processed and handled. Model security is ensured during model training. HE is an encryption technology that enables computations to be performed on encrypted information without the need for a secret key to decrypt it.

The HE approach can be used to construct privacy-preserving machine learning (PPML) in industries where privacy protection is important. HE is an encryption technology that empowers service providers to perform calculations. Network operators can directly execute arithmetic computations on ciphertexts by utilizing HE encryption technology. Partially homomorphic encryption (P.H.E.) was originally capable of addition and multiplication.

3.5. Practical Applications of Federated Learning in UAV. The following are potential real-time applications of FL-enabled UAVs:

- A2G photographs can sometimes be taken and kept private, which is why FL-based UAVs come into service. FL-based UAVs keep data safer because the initial information is not sent directly to the server. As a result, no one will be able to easily breach the data area.
- FL-based UAVs play a significant role in data security and privacy, especially in the military. Given the sensitivity of military information, FL-based UAVs are essential for maintaining security and privacy.
- Federated technologies can be utilized to generate user behavioral patterns from a pool of smartphone data, including voice recognition, face identification, and next-word prediction, without disclosing any personal information. For example, Google employs federated learning to develop pattern recognition algorithms for on-device voice commands like ”Hey Google” in Google Assistant.
- Manufacturing companies can utilize federated learning algorithms to create equipment predictive maintenance predictions. Predictive maintenance may face challenges when clients or users are reluctant to provide personal information, and when there are data exporting issues from various locations. Federated learning can overcome these problems by utilizing regional datasets.

Table 4.1: Simulation Parameters

Description	Value
UAV Servers	1
Epochs	60
UAV Clients	4
CPU Usage	2.5Ghz
Global Training Accuracy	97
Global Training Loss	3
RAM	16GB

- Federated learning techniques would be beneficial for insurance and healthcare systems as they allow for the protection of private data in its original form. Federated learning systems can gather data from multiple sources such as hospitals and electronic health record databases to diagnose uncommon diseases, thereby providing a more diverse set of data. In contemporary healthcare systems, hospitals, research institutions, and federal departments collaborate to enhance healthcare nationwide.

3.6. Core Challenges of the Federated Learning Process. A number of major obstacles must be overcome for Federated Learning to be implemented in UAVs:

- Effective communication between federated learning-enabled UAV networks.
- Managing diverse systems within a single network.
- Data in federated networks are statistically heterogeneous.
- Privacy issues and methods to protect them.

4. Results and Discussions. In this section, the gathered results discuss the training accuracy and training loss of local UAV client models, as well as the global model. The performance has been analyzed using Python libraries, including NumPy, TensorFlow, pandas, and Keras. Socket programming is used to communicate local client models to the server, and an HTTPS connection is established for the interconnection of multiple UAVs and servers. In this work, 6000 training samples are taken, and each sample is tested. The experimental parameters used throughout the work are described in Table 4.1.

4.1. Flowchart of the Proposed Work. Fig. 4.1 represents the flowchart of the proposed work. Firstly, the UAV client is loaded with the models or architecture, weights, and gradients. Then, the models undergo training using CNN. The input layer of the CNN takes the models or architectures as input and various hidden layers perform the learning process, resulting in updated or trained local models. The trained local models are encrypted using secure aggregation and homomorphic encryption and then sent to the server for global aggregation. Subsequently, the global models are broadcasted.

In Fig. 4.2 the training process of local UAV clients is depicted in Python, showing the training accuracy of the local models. During the training process, local model 4 shows accuracy after 10 epochs, while local models 1, 2, and 3 show accuracy after 40-45 epochs. The accuracy and loss graphs depend on the batch size and the type of data used. Some data is smooth and can be filtered easily, requiring less time for training. However, some data is more challenging to filter, so when a batch size of 200 is used, the graph reflects the corresponding accuracy and loss.

In Fig. 4.3 the training accuracy of the global model is displayed. This figure was generated using Python. The global model demonstrates accuracy after 10 epochs during the training process, while all other local clients (Aircraft) achieve stability after 30 iterations. Once the local clients are aggregated through the Federated Learning (FL) process, their accuracy and stability increase, while the remaining local clients exhibit different characteristics. Therefore, Figure 4 illustrates that local UAV clients achieve accuracy after 30 epochs, indicating that FL can achieve privacy in multiple ways.

Fig. 4.4 presents a comparison graph of accuracy between centralized and FL approaches. We utilized FL to train UAV data and used centralized learning with Python to train the same data, comparing the results. In the case of centralized and automated systems, Data 1, 2, and 4 indicate an accuracy of 80%, Data 5 has an

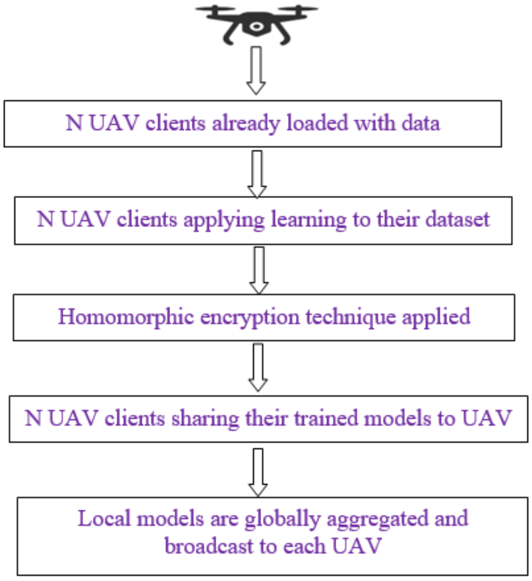
N UAV clients already loaded with data
N UAV clients applying learning to their dataset
Homomorphic encryption technique applied
N UAV clients sharing their trained models to UAV
Local models are globally aggregated and broadcast to each UAV

Fig. 4.1: Flowchart of Proposed Work

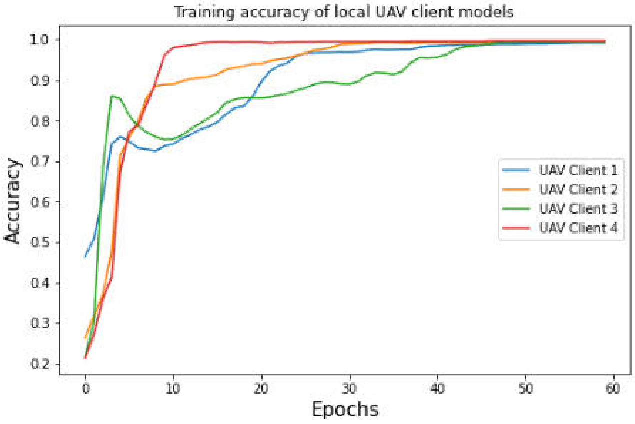

Fig. 4.2: Training Accuracy of Local Model

accuracy of 75%, and Data 3 has an accuracy of 90%. For FL, Data 1 and 4 demonstrate an accuracy of 82%, while Data 2, 5, and 3 provide accuracies of 80%, 75%, and 88%, respectively. The accuracy in FL is lower than in centralized learning, as evidenced by Data 3, suggesting that accuracy can depend on the type of data collected. Perhaps the dataset used in that case is not as clear and filtered.

Similarly, in Fig. 4.5, we conducted a comparison between centralized and FL approaches and depicted the graph. Data 1, 4, and 5 exhibit a precision of 80%, while Data 2 shows a precision of 85%, and Data 3 shows 90% in the case of centralized learning. For FL, Data 1 and 5 show a precision of 85%, Data 2 and 4 show a precision of 90%, and Data 3 shows a precision of 75%. In this graph, Data 1 and Data 5 show almost no variation in terms of precision. Data 3 displays a significantly lower precision rate in the case of FL compared to centralized learning. Thus, in terms of precision, FL yields result similar to centralized learning, with only minor variations observed in the comparative analysis.

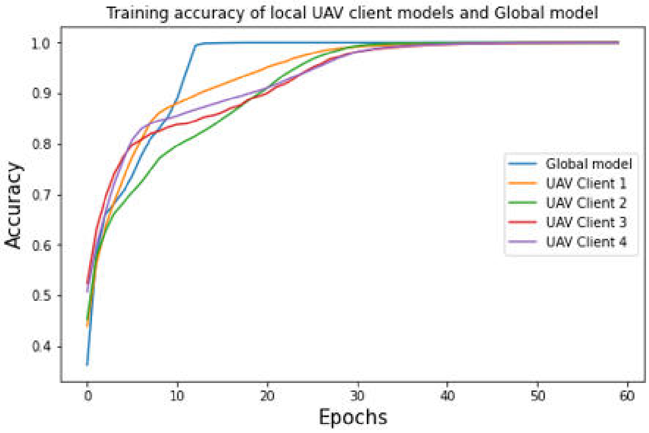

Fig. 4.3: Training Accuracy of the Global Model

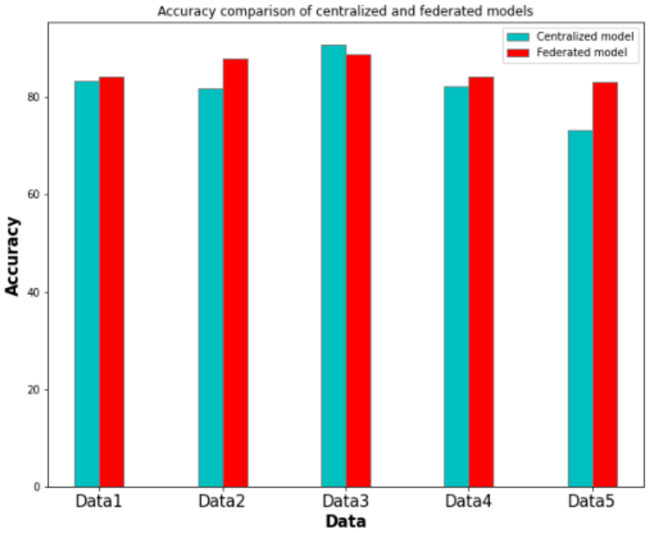

Fig. 4.4: Comparison Graph of the Accuracy of Centralized and Federated Learning

In Fig. 4.6, we employed UAV data and trained it using the FL process and then the centralized process, subsequently conducting a comparative analysis based on recall. Data 1 and 4 indicate the recall rate, Data 2 shows 80%, Data 3 shows a recall of 90%, and Data 5 shows 75% in the case of centralized learning. For FL, Data 1 and 2 demonstrate a recall of 90%, Data 3 shows 85%, and Data 4 and 5 exhibit a recall of 83%. In this case, as well, Data 3 shows better results in centralized learning and lower results in the case of FL. Data 4 displays significant variation in terms of recall for FL and centralized learning.

5. Conclusion and Future Work. The primary focus of this paper is the deployment of multi-UAVs and the incorporation of privacy measures through the utilization of FL. This study addresses machine learning-specific challenges, such as centralized training. The proposed model applies FL techniques to train each UAV's data locally and leverages decentralized UAV data to achieve privacy-preserving advantages. Furthermore,

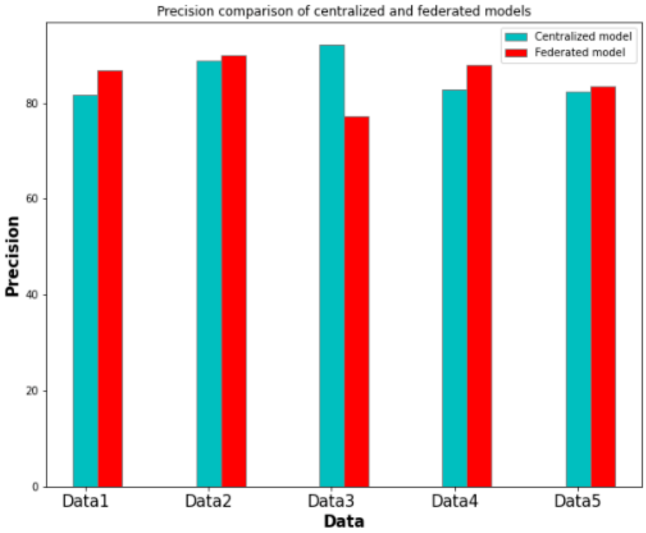

Fig. 4.5: Comparison Graph of Precision of Centralized and Federated Learning

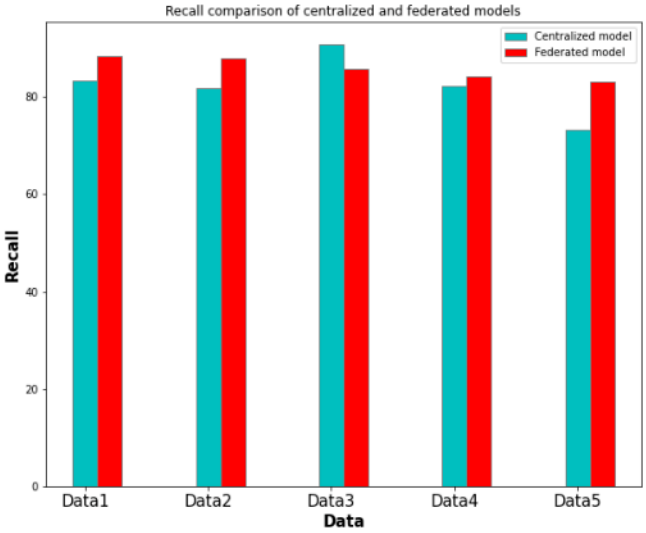

Fig. 4.6: Comparison Graph of Recall of Centralized and Federated Learning

this paper includes a comparative analysis between ML Models and FL Models, evaluating their accuracy, precision, and recall. The findings demonstrate FL's superiority over centralized learning regarding privacy protection, as raw data is not directly transmitted to the server. Instead, UAVs locally train their models, which are subsequently sent to the server for aggregation as a ”global model.” The results reveal enhanced accuracy, precision, and recall in the federated model compared to the local model, providing a comprehensive comparison of traditional centralized versus federated models. Future research endeavors could expand upon the development of UAV networks to facilitate intercommunication among them. Additionally, the optimization of UAV placement in terms of height and angle could be explored to improve coverage, capacity, and secure communication within the network. Furthermore, the integration of FL into a multi-UAV network can enable the implementation of various efficient routing protocols and path planning techniques to enhance quality of service (QoS) metrics.

REFERENCES

[1] S. Al-Emadi, A. Al-Ali, A. Mohammad, and A. Al-Ali, *Audio Based Drone Detection and Identification using Deep Learning,15th International Wireless Communications and Mobile Computing Conference, 2019*, 459-464, doi:10.1109/IWCMC.2019.8766732.

[2] B. Brik, A. Ksentini and M. Bouaziz, *Federated Learning for UAVs-Enabled Wireless Networks: Use Cases, Challenges, and Open Problems*, *IEEE Access*, 8, 53841-53849, 2020, doi: 10.1109/ACCESS.2020.2981430.

[3] M. S. Ahmad, and S. M. Shah, *Mitigating Malicious Insider Attacks in the Internet of Things using Supervised Machine Learning Techniques*, *Scalable Computing: Practice and Experience*, 22(1), 13–28, 2021, https://doi.org/10.12694/scpe.v22i1.1818.

[4] W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, C. Leung, and C. Miao, *Towards federated learning in UAV- enabled Internet of Vehicles: A multi-dimensional contact-matching approach*, CoRR abs/2004.03877, 2020.

[5] H. Yang, J. Zhao, Z. Xiong, K. -Y. Lam, S. Sun, and L. Xiao, *Privacy-Preserving Federated Learning for UAV-Enabled Networks: Learning-Based Joint Scheduling and Resource Management*, *IEEE Journal on Selected Areas in Communications*, 39(10), 3144-3159, Oct. 2021, doi:10.1109/JSAC.2021.3088655.

[6] Z. Yang, M. Chen, W. Saad, C. S. Hong, and M. S. Bahai, *Energy Efficient Federated Learning Over Wireless Communication Networks*, *IEEE Acess*, Nov 2020, (99):1-1 doi: 10.1109/TWC.2020.3037554.

[7] B. Khamidehi, and E. S. Sousa, *Federated Learning for Cellular-Connected UAVs: Radio Mapping and Path Planning*, *IEEE Global Communications Conference*, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322349.

[8] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, *Federated Learning for Drone Authentication*, *Adhoc Networks, Elsevier*, 120, 1-6, 102574, 2021, doi:10.1016/j.adhoc.2021.102574.

[9] S. Tang, W. Zhou, L. Chen, L. Lai, J. Xia, and L. Fan, *Battery constrained federated edge learning in UAV- enabled IoT for B5G/6G networks*, *Physical Communication, Elsevier*, 47, 1-6, August 2021, https://doi.org/10.1016/j.phycom.2021.101381.

[10] R. Wang, and W. T. Tsai , *Asynchronous Federated Learning System Based on Permissioned Blockchains*, *Sensors, MDPI*, 22(4), 1-18, 1672, 2022. https://doi.org/10.3390/s22041672.

[11] J. Huang, C. Xu, Z. Ji, S. Xiao, T. Liu, N. Ma, and Q. Zhou, *An asynchronous, Federated learning privacy-preserving computing model applied to 5G-V2X*, *Security and Communication Networks, Hindawi*, 2022, 1-11, March 2022, doi:https://doi.org/10.1155/2022/9334943.

[12] K. Neeraja, and G. Narsimha, *A Multi-Objective Hybrid Collision-free Optimal Path Finder for Autonomous Robots in Known Static Environments*, *Scalable Computing: Practice and Experience*, 23(4), 389–402, 2022, https://doi.org/10.12694/scpe.v23i4.2049.

[13] C. Zhu, X. Zhu, J. Ren, and T. Qin, *Blockchain Enabled Federated Learning for UAV Edge Computing Network: Issues and Solutions*, *IEEE Access*, 10, 56591 - 56610, 13 May, 10.1109/ACCESS.2022.3174865.

[14] B. Taha, and A. Shoufan, *Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research*, *IEEE Access*, 7, 138669-138682, 2019, doi:10.1109/ACCESS.2019.2942944.

[15] A. Bouguettaya, and H. Zarzour, A. Kechida, *Deep learning techniques to classify agricultural crops through UAV imagery: a review*, *Neural Computer and Application, Springer*, 34, 9511–9536, 2022.

[16] M. Shaheen, M. S. Farooq, T. Umer, and B.-S. Kim, *Applications of Federated Learning; Taxonomy, Challenges, and Research Trends*, *Electronics, MDPI*, 11(4), 1-6, February 2022, https://doi.org/10.3390/electronics11040670.

[17] A. Mishra, S. Lee, D. Kim, and S. Kim, *In-Cabin Monitoring System for Autonomous Vehicles*, *Sensors, MDPI*, 1-21, 2022, 22, 4360. https://doi.org/10.3390/s22124360.

[18] A. Mishra, J. Cha, and S. Kim, *Privacy-Preserved In-Cabin Monitoring System for Autonomous Vehicles*, *Deep Learning for Intelligent Surveillance Systems, Computational Intelligence and Neuroscience, Hindawi*, 1-15, 2022, 5389359, https://doi.org/10.1155/2022/5389359.

Edited by: Pradeep Kumar Singh
Special issue on: Intelligent Cloud Technologies Enabled Solutions for Next Generation Smart Cities
Received: Mar 7, 2023
Accepted: July 28, 2023