SURVEY ON TECHNICAL ADVANCEMENTS AND RENOVATIONS IN FEDERATED LEARNING

S.Balaji[1*], Shobhit Tulshain[1], Manan Modi[1], Asutosh Dalei[1] and Sumathi D[2]

[1]School of Electrical Engineering,
Vellore Institute of Technology,
Vellore, India

[2]School of Computer Science Engineering and Information Systems,
Vellore Institute of Technology,
Vellore, India

Emails:sbalaji@vit.ac.in[1*](Corresponding Author), shobhittulshain@gmail.com[1],
mananmodi.0108@gmail.com[1], asutoshdalei@gmail.com[1], dsumathi@vit.ac.in[2]

ABSTRACT

With the rapid increase in IoT devices and advanced machine learning and deep learning techniques, there has been a growing concern about computational cost and data privacy issues since the data coming from IoT devices is non-independent identically distributed (non-IID). However, the implementation of the federated learning algorithm has proven to be a booster in the performance and a solution to the existing data privacy concerns. This paper gives insight into topics such as Blockchain, Unmanned Aerial Vehicles (UAV), Wireless communication, Vehicular Internet of Things, Healthcare, and Cloud Computing and how they have been implemented and co-related to federated Learning and the application and the emerging use cases in the field of federated learning (FL) with respect to the above-mentioned topics have also been discussed. This paper uniquely shows how federated learning has an edge over the traditional machine learning and deep learning techniques in IoT infrastructure since computing nodes are trained using local models on the devices and then these local models are uploaded to the central global server instead of data directly into a global model on a central server ensuring data privacy.

Keywords: Federated Learning; Blockchain; Vehicular IoT; Unmanned Aerial Vehicles; Cloud Computing; Healthcare; Wireless Communication networks

1.0 INTRODUCTION

In recent years, the rise and increase in the number of IoT edge devices, mobile technologies, and applications of machine learning have increased by a significant factor and have resulted in a huge amount of data traffic, which prompts the prosperity of complex machine learning and deep learning technologies analysis [1]. There have been constant efforts made to upgrade the existing technologies and simultaneously build more and more efficient devices, but all these upgrades and modifications have led to complex algorithms that require devices with essentially more computation power, thereby increasing the cost of the device. Machine learning algorithms generally work efficiently on good hardware specifications to obtain the results [2] and cannot be executed on edge devices since their computation power is limited. So these devices often make use of the cloud services available out there like Amazon Web Services, Google Cloud Platform, or Digital Ocean to get the desired data from the IoT device and send those data to the cloud where the processing is done and finally, instructions are sent back to the device where a specific task is executed, however, this has led to a major concern of data privacy, data stealth, data tampering and misuse of information by the hackers as the information is sent directly on a central platform for processing, which can disrupt the working of the device significantly [3]. So one needs to do a proper analysis of threats, vulnerabilities, and risks before performing any internet-related task.

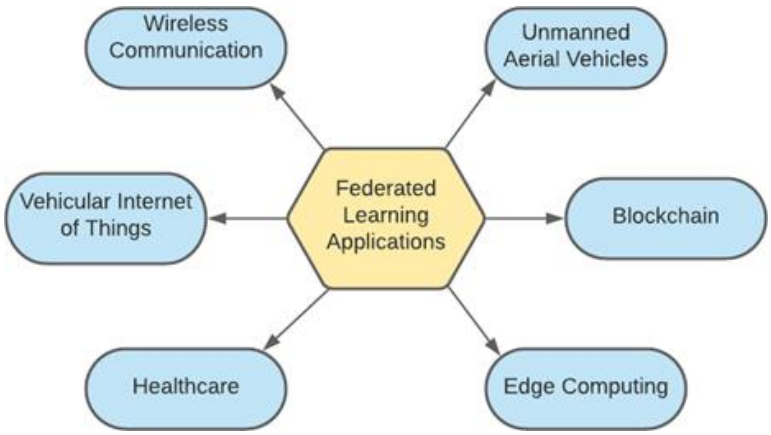

Figure 1: Applications of Federated Learning

Federated Learning applications have spread over a large area as shown in Fig. 1, covering very important fields like Blockchain, Unmanned Aerial Vehicles, Wireless communications, Vehicular Internet of Things, Healthcare, and Cloud Computing and neither of the above-mentioned industries can share private information of their users with anyone. Since these fields are major data handling industries, they become even more susceptible to various attacks like protocol attacks, eavesdropping attacks, cryptographic algorithm, and key management attacks, spoofing and masquerading (authentication attacks), operating system and application integrity attacks, denial of service and jamming, physical security attacks (for example, tampering, interface exposures) and access control attacks (privilege escalation).

So in order to overcome these attacks and risks, federated learning was first introduced by Google with an aim of ensuring data security and efficient management of data. It is an advanced concept of machine learning whose main focus is to train the machine learning models on the local device itself based on local information and send only the locally trained parameters of the model to a central server which collects similar information from the other devices as well. Now when the model parameters are collected from the other devices, a global model is trained based on the parameter values received and now this trained model is sent to the local devices for further training [4]. This step is executed iteratively until an efficient model is obtained which provides good accuracy. This decentralized method does not involve any transfer of raw sensor data collected by the local device and only the model parameters are transferred which has no meaning without the availability of the model architecture thus ensuring data secrecy and non-exposure of information directly. Table 1 lists the far contrast between centralized and decentralized machine learning techniques. One of the first implementations of this method was on one of Google's own services, the Google Keyboard, or the GBoard [5].

Moreover, to mitigate privacy leakage concerns, optimization of FL should include differential privacy (DP) scheme, the addition of noises in DP schemes, effective and lightweight authentication schemes, and various encryption standards. While optimizing one must make a trade-off between performance, communication overhead, complexity, convergence time, accuracy, etc. Byzantine-Fault Tolerant (BFT) decentralized FL, Truth Discovery based FL, Federated Opportunistic Block Dropout approach, Social-aware Clustered FL technique, and privacy-preserving momentum FL are some of the techniques advocated in recent literature for ensuring trustworthiness in FL. By using the secure procedures incorporating the secure schemes and calculating the performance index one can easily make the users periodically participate in FL.

In this paper, the use cases and applications of federated learning and their implementation in IoT infrastructure have been discussed. Like when it comes to wireless communication, one of the major challenges is the distribution and scalability of data, as there are billions of devices, generating data at any moment, be it through the inbuilt software, or the hardware sensors. Federated Learning with its ability to handle data in the most secure manner through the updated fedAvg mechanism [6], which uses deep neural networks on client's distributed data to provide and communicate efficient network. Vehicular IoT is also an emerging use case of federated learning, as it collects data from all its sensors such as Global Positioning System (GPS), camera, radar, accelerometer, etc., and based on the values from these sensors, the data is processed rapidly for making decisions.

Table 1: Centralized vs. Decentralized Machine Learning

Centralized Machine Learning	**Decentralized Machine Learning**
Data from each of the connected devices is transferred to a central server where a global ML model is trained.	The ML model runs and processes data on-site, onboard each connected device.
Irrespective of confidentiality, all data must be transferred to the central server to be trained.	There is no need to move.
Powerful computers are required to process the vast amount of data received.	The idle processing power of connected devices is taken into use.
Devices must be connected to the internet to transfer the data to the central server.	Since the processing is being done on board, an internet connection is required only to receive commands and transfer trained models.
Data processing and model training are limited only by a single central computer.	Data processing and model training could be limited by the multiple connected devices, since all may not have the same processing power.
It becomes difficult for the model to explain all variations in the data by the devices and the environment they are in.	Access to individual devices facilitates more accurate and adaptive models.

However, the users are slightly hesitant to send their information into a global network directly [3]. There are a few considerations regarding the collection and transfer of data, as the data has to be sent to the global cloud server and then the data is processed and the information is sent back to the device, which requires a high bandwidth eventually resulting in a delay. To the aforementioned issues, Federated learning stands as a reliable solution that proposes a collaborative model-based approach, where the data is jointly trained using local data sets and further these models contribute it to a central server using stochastic gradient descent, and hence a global model is formed using the local updates and data privacy is retained [7].

In today's world, the data is being generated in large amounts, which can be fed to machine learning models and neural networks to obtain valuable insights into the data. The only issue is that the data is distributed, in other words, the data have settled in clusters. As discussed earlier, the collection of this data in a centralized platform upon which the complex machine learning and neural network models can be trained does pose a security and privacy threat to the data itself, and at every step, there is a risk of malicious attacks. The concept of federated learning provides a great advantage on edge devices. These devices have low power consumption, interconnected bodies, and sufficient processing power to train on local data. In fact, edge computation [8] in a well-interconnected distributed manner not only ensures the privacy of data but also provides low latency and highly efficient use of network bandwidth. Several such protocols have been implemented on the scale, such as PySyft, LEAF, FATE, etc. Also in order to address the security issues blockchain can be efficiently used to take care of all the threats using the concept of differential learning and smart contract technologies [9], blockchain-based federated learning which includes committee consensus [10], and also the use of the differential private multiparty data model method as proposed in [11].

Being one of the greatest technological innovations, the Internet of Things has today been implemented in nearly every other field. This coupled with the rapidly developing healthcare monitoring devices, procedures, etc, have resulted in large amounts of data being produced. As discussed, naturally the choice of approach now would be complex machine learning and deep neural network, models. However, the transfer of this data to a centralized platform for training could suffer security breaches, how secure the platform is. Medical information [12] is highly private to the patients and people would naturally avoid their health information being shared. As a solution to major problems discussed previously in this paper, the federated learning-based approach finds a viable solution here as well.

'Jupiter', an advanced federated learning-based infrastructure with API support along with augmentations, filters, and sessions has been discussed in [13]. The platform is one of many implementations that result in well well-trained final model without any compromise in privacy. Unmanned Aerial Vehicles or UAVs are also one such field in which the technologies and advancements are rapidly growing and the data collected by these drones is very important as it provides aerial data that is not easily available. There are Drones as a Service providers which are major sources of these kinds of data but in order to perform complex machine learning algorithms, the raw data is sent to the cloud servers for processing which again poses a threat of data

stealth, tampering, and alteration, but with the use of federated learning this problem can be overcome by sending the model parameters instead of the raw sensor data for training and the getting the final global model from the central server [14]. Multi-UAV networks can also be used for accomplishing high-level tasks using ground fusion centers, forming the basis of communication as discussed in [15]. The major contributions and the research work related to the applications of federated learning are shown in Table 2.

Federated Learning Algorithms operate through a series of well-defined steps, transforming collaborative model training while prioritizing data privacy. The process commences with the central server initializing a global model, which is then disseminated to participating devices. Local training unfolds autonomously on each device, refining the model exclusively concerning its local dataset, thus upholding data privacy. Following local training, the updated models from all devices are aggregated on the central server. This aggregation involves combining the knowledge gleaned from disparate local models to construct an improved global model. The refined global model is then communicated back to all participating devices, constituting a cycle of iterative updates. This iterative process repeats for a predetermined number of epochs, progressively enhancing the global model's performance. Optionally, the final global model can undergo evaluation on a validation set before deployment. This meticulous sequence of steps characterizes Federated Learning Algorithms, offering a groundbreaking approach to collaborative machine learning while addressing concerns associated with centralized data management.

Table 2: Major Contributions in Federated Learning

Reference	UAV	Blockchain	Healthcare	Edge Computing	Vehicular IoT	Wireless Communi-cations
[9]		✓				
[11]		✓				
[18]				✓		✓
[35]				✓		✓
[36]		✓			✓	
[42]			✓			✓
[43]			✓			
[45]				✓		✓
[58]	✓			✓		✓
[60]	✓					

Federated learning employs various hardware sensors and boards for model training across diverse devices while prioritizing data privacy. Examples encompass smartphone brands like the iPhone and Samsung, IoT devices such as Raspberry Pi(4 Model B, 3B+) and Arduino Nano 33 BLE Sense and Rock64, wearables like Fitbit and Apple Watch, edge computing platforms including NVIDIA Jetson Nano and Intel NUC, embedded systems such as BeagleBone Black and Arduino, specialized-sensor-equipped medical devices, and autonomous vehicles with LiDAR and Radar. The compatibility of hardware is contingent on specific use case requirements, allowing flexibility to adapt to diverse environments while maintaining data confidentiality in federated learning implementations. Some low power consumption components like GPS sensor RS232, accelerometer, and gyroscope module GY291 ADXL345, and RPLIDAR AIM8 360 LIDAR version can be used in federated learning applications. This hardware diversity highlights the adaptability of federated learning across various domains, enabling collaborative model training without compromising sensitive data.

Throughout this paper, federated learning and its applications and use cases in the fields of Wireless Communication, Vehicular IoT, Healthcare, Edge Computing, Blockchain, and Unmanned Aerial Vehicles have been defined in Section II. An attempt to support the various use cases has also been made with a detailed description and table consisting of previously done research work in their respective fields along with a visual illustration. In section III, the open issues and the future research directions for the above-listed use cases and applications in federated learning have been listed. Finally, the paper concludes in Section IV with an extensive discussion of the various use cases.

2.0 RELATED WORK

2.1 Federated Learning for Wireless Communication

With the advancement in computing and research on data handling tools, the use of machine and deep learning has emerged as a very powerful tool for system design and analysis for wireless communication, because the pre-existing model-driven approaches had never shown enough capabilities to capture the complexity and variations in the modern wireless networks [16]. In wireless networks, the data is generated and distributed over a large number of devices (roughly in billions) and hence the implementation of these Machine Learning algorithms on large-scale data to maintain efficiency and scalability is a great challenge [17]. Therefore, the necessity to work on decentralized learning triggers the idea of a Federated Learning Framework, where the model is trained in a decentralized manner and data is kept and trained wherever it is generated over the traditional centralized model approaches.

The objective of the federated learning framework is basically to keep the training data set wherever it is generated and perform model training in the local devices at their own level. After this local model training, the local model parameters are used to develop a global model which is eventually made in feedback with the local models to improve the model performance without compromising on data privacy [18]. However, this model can be further improved by using a more advanced federated learning framework, Federated Averaging Learning Algorithm (FedAvg) which is a booster in the performance and a solution to the existing data privacy concerns. In this algorithm, Deep Neural Networks (DNNs) are trained on the client's distributed data from the local devices and are periodically averaged and sent to the central edge server each round. These DNNs use mini-batch Stochastic Gradient descent(mb-SGD) and hence the weights are updated and multiplied with a constant learning rate throughout.

But when it comes to the implementation, the FedAvg algorithm has a few problems attached to it which are, the weights in this algorithm are very large in number and hence it makes the model very huge, which eventually increases the communication (between the client device and edge sever) cost per round. Hence a Robust and Communication Efficient FedAvg Algorithm is used, which reduces the number of rounds per convergence, and the total data uploaded per round over FedAvg and uses the sparse compression ternary compression technique without any compromise in the data privacy [19], [20]. This Algorithm has been very efficient and has been used in 5G core networks [18]. The data distribution algorithm is provided in the federated learning environment to increase the learning performance for balancing the data distribution on different participants in the proposed 6G mobile connections [22]. FedAvg mainly contributes to reducing the communication cost. It established the model averaging, accuracy, and data compression and takes much more time to converge. To overcome the convergence issue one can parallelize the FedAvg which has been attempted by one of the recent research. This allows continuous local model training without any blocking caused by frequent communication. Table 3 below shows the contributions and the limitations of various other papers that have played a significant role in federated learning in wireless communications. Methods like deep deterministic policy gradient, reinforced learning, Q-learning, and federated reinforced learning can be used for optimizing performance like load balancing, and latency in 6G networks. Moreover, the principal merit of FL is that it has the inherent ability to provide multilateral demands of 6G.

The incorporation of the Analytical Model of Federated Learning represents a pivotal advancement in the enhancement of wireless networks, effectively addressing the intricacies associated with decentralized machine learning. This model offers a tailored solution for resource-constrained wireless environments, allowing devices to collaboratively train a global model without the need to disclose sensitive raw data. The analytical framework inherent in Federated Learning plays a crucial role in optimizing communication efficiency, a critical consideration given the inherent limitations of bandwidth in wireless networks. Techniques such as model compression are instrumental in minimizing communication overhead and facilitating collaborative learning without imposing undue strain on the network infrastructure. Importantly, the analytical approach is designed to accommodate the diverse landscape of devices within wireless networks, adapting flexibly to variations in computational capabilities and energy resources. The integration of privacy-preserving strategies further enhances the security paradigm, fostering trust among users and device owners. The inclusion of the Analytical Model of Federated Learning in this research framework enriches the overall methodology, providing a robust solution that harnesses the potential of machine learning while seamlessly aligning with the constraints and privacy considerations inherent in wireless network environments.

2.2 Federated Learning for Vehicular Internet of Things

Vehicular IoT deals with a lot of sensors that provide GPS (Global Positioning System) coordinates, Camera output, Gyroscope, Radar, LIDAR, and so on, they provide data which is further used by the system to make decisions timely. Machine learning and deep learning have already been consistently adopted in vehicular networks for object detection, autonomous driving, safety prediction, etc. [34]. In the machine learning-driven vehicular network, the whole dataset consisting of the various sensor values is sent to the cloud for Model training, through a supervised learning scheme. Once training is done, the parameters are sent to the devices for prediction. This approach faces a lot of challenges as the size of data generated by the vehicular devices is massive (approximately in GB per second) and hence the model has to be very complex (with deeper neural nets) for successful training, with that training a model from the device to cloud center in a reliable manner would be very expensive.

The current vehicular systems only depend on the collection of vehicle data and pushing it to the cloud whereas the emerging vehicular IoT system involves a larger amount of sensor data values and application in complex environments that use minimal computing and storage resources to provide a better Quality of Service (QoS). Hence, a system that is capable of computing decentralized data with collaboration among different vehicles is needed. These requirements can be efficiently fulfilled by federated learning, as shown in Fig. 2, where multiple devices collaborate to form and train a deep neural network on a global server. The global server first distributes an initial model for training using this neural network and then each device calculates its local updates using stochastic gradient descent, which is trained locally. Further, the FedAvg algorithm is used for collecting the local models generated by different devices [35]. Table 4 highlights the various contributions that have been made so far in the field of vehicular Internet of Things and federated learning together. Considering the limited computation resources and complex design of vehicular networks Mobile Edge Computing (MEC) is being used for end-users by performing edge data caching and computation for edge devices [36].

In the realm of applying Federated Learning (FL) to Vehicular Networks, the meticulous selection of relevant parameters is imperative to ensure the accuracy of predictive models. The dataset chosen to drive FL algorithms must encompass pivotal characteristics intrinsic to vehicular environments. Fundamental spatial parameters, such as latitude, longitude, and altitude, provide a comprehensive geographical understanding, while temporal features, including timestamps, enable the model to discern time-dependent variations in traffic conditions. Variables such as vehicle speed, acceleration/deceleration, and type contribute to a nuanced depiction of traffic dynamics, while metrics related to communication strength and connectivity status are essential for reliable data exchange in Vehicular Ad Hoc Networks (VANETs). Moreover, considerations for environmental variables, such as weather conditions and visibility, alongside traffic density and flow metrics, offer a holistic view of the vehicular landscape. Event and incident data, encompassing accident reports and roadwork information, further refine the predictive capabilities of the model. Integrating these parameters into the FL dataset establishes a robust foundation for accurate predictions, allowing the model to discern patterns and optimize decision-making in Vehicular Networks. As reported recently by some works, FL protocols should be configured and developed to support efficient deployment in vehicular networks.

2.3 Federated Learning in Healthcare

“Health is wealth” is one of the oldest sayings of our society and has always been proven to be true. In simpler terms, Healthcare is the maintenance or improvement of health through treatment, diagnosis, cure, recovery, and most importantly, prevention from diseases from injuries, etc. With the significant development in microcontrollers and small-scale electronics, wearable technologies have become better, efficient more accessible. One specific application of wearable technologies discussed in [40] was health monitoring. Certain daily activities give an early indication of a few diseases in a person’s lifestyle. Wearable healthcare has a critical potential to provide early indications of diseases such as Parkinson’s disease, small vessels, or fits. Moreover, they are capable of mental health assessment, sports monitoring, and fall detection. Healthcare application is also one of those industries that produce heavy amounts of data, and hence Machine Learning and Deep Learning models can be easily implemented. However, there are two specific challenges to this:

a) Even if there is plenty of data, it is not possible to share the data due to privacy and security concerns.
b) Even if plenty of user data is acquired and the machine learning model is trained, the touch of personalization would be lost. Since not all humans are created equal, a general model to define their health is not sufficient. Hence a federated learning model is proposed.

Focus/Scheme	Ref. no	Contribution / Methodology	Limitations / Gaps
Performance Optimization	[22]	The joint learning, wire- less resource allocation and user selection problem is formulated.	The optimization of loss function with FL approach is minimal even with including the wireless factorsjoint optimization is proposed by considering limitedusers.
	[23]	Under long term energy constraint, bandwidth allocation and client selection are proposed.	Non uniform resource allocation for different priority clients.
	[24]	Channel prediction and scheduling policies areincorporated in both perfect and imperfect channel state regime.	It is reported that without data size distribution and channelstate information, high training accuracyor fairness cannotbe obtained under communication constraints.
Quality of Service (QoS)	[25]	Proposed federated learning- based cooperation and augmentation forpower allocation.	Fixed decision trajectory length is used to mitigate the difficultyof convergence of algorithm.
	[26]	Performance of FL in wireless networks fo scheduling and interference management.	Trade-off between the number of scheduled UEs and the subchannelbandwidth in optimizing the FL convergence rate is to exploit.
Noise	[27]	Robust design using federated learning to reduce the noise effects is pro- posed.	Missing of optimalpoint in trainingprocess due to random division of data samplesamong the nodes.
	[28]	Broadband analogaggregation technique is proposed for quantifying learning performance innetwork planning and optimization.	SNR – truncation trade-off and reliability – quantity trade off re- quired for aggregation and scheduling of cell interior devices.
MIMO	[29]	Federated learning framework for cell free massive MIMO is proposed for optimization of networkresources.	The data rate is significantly low for larger number of user equipment, and also training update transmission time requires long time.
	[30]	Using inherent superposition of radio frequencysignals, communication efficiency is optimized.	More slots are used to update the data simultaneously from clientsides.
	[31]	FL is demonstrated tohave more tolerant to the imperfections and corruptions in the channel data.	Showed performanceloss compared to existing methods.
NOMA	[32]	The authors investigated the efficient performanceof FL update by exploiting non orthogonal multiple access (NOMA) and adaptive gradient quantification the at mobile edge devices.	Aggressive Compression strategyis required when usersparticipate in model updates simultaneously with NOMA.
	[33]	Authors demonstratedmethod to minimize the learning optimalitygap for adaptive power allocation in wireless transmission.	Fixing scaling and clipping thresholds controlling the performance.

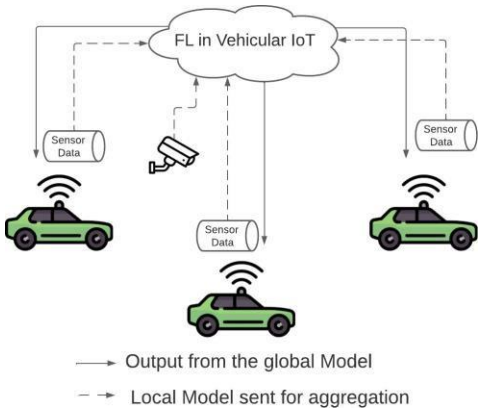

Table 3: Federated Learning in Wireless Communications

Figure 2: Federated Learning in Vehicular IoT

A healthcare process based on this mechanism has the ability to achieve accurate personal health without a slight compromise on data privacy [40]. A typical implementation would follow steps where a server-based cloud model is initially trained based on public datasets then the cloud model is distributed to all users. Here each of them can train their own model based on their personal data. The user-based models are then uploaded to the cloud to help train a new model by model aggregation. Each individual can now train personalized models by utilizing the cloud model and their personalized local data. It is expected to have a large divergence between server data and user data, hence, differences in their model as well. Transfer learning is performed to make the model more efficient for the user. Here the Federated Learning-based IoT model is the main infrastructure behind this implementation. It opens new doors of research in this domain of healthcare.

In order for this implementation to take place, Electronic Health Records, or EHRs play a vital role [41]. EHRs are generated in the healthcare industry and contain extensive information about the patient, such as diagnosis, complications, diseases, medications, etc. The best part of these EHRs is that they are stored and maintained in a digital format. In order to achieve complete inference and advantage of this information, this data can be pre-processed and fed into Machine Learning and deep neural network models [40]. These models can significantly improve the efficiency of healthcare diagnosis and early signs recognition. As discussed earlier, health data is sensitive data and a patient would prefer not to share his/her information. In order to tackle this issue, federated learning was proposed, which would significantly achieve the goals of a common machine learning/ deep learning model while ensuring the privacy of patient EHR data. SVM, single-layer perceptron, and logistic regression are usually used to compute global models by taking into account of sensitive data of EHR. One such proposal of Federated Learning is the Privacy-Aware Resource Saving Collaborative Learning protocol. A typical PRCL model would consist of parts as shown in Fig. 3

Table 4: Federated Learning in Vehicular IoT

Focus of Re-search	**Ref.no**	**Major Contribution**	**Approach/ Major Highlight**
Selective Model Aggregation Approach	[37]	Deep Neural Network are deployed for model training and then based evaluation on Image quality and computation capability of vehicular clients, further data is sent to the global cloud.	Two Dimension contact Theory
Feasibility of FL in Vehicular IoT	[34]	Analysis of challenges with respect to Learning - Data Training and Model Training, and Communication data rate, reliability, transmission delay and resource management	Efficient Reinforcement Learning
FedAvg	[19]	Low Communication Overhead, Better Suitability of non IID data, Larger Dataset for Training purposes	Stochastic gradient descent (SGD)
Convolutional Neural Networks for Autonomous Driving	[38]	The Author has described image recognition based on deep learning techniques and their brief implementation in autonomous driving where the core component is generally divided into three major categories, namely perception, planning, and control.	Image Feature Extraction and Classification using Deep Learning.
	[39]	The Author proposed a method to improve the accuracy of the autonomous driving by using CNNs along with the traditional computer vision techniques to provide a safe autonomous drive. It uses CNN for steering the car using images from a front center camera video.	Deep learning Techniques along with Traditional Computer Vision Techniques.
FL for Dis- tributed Train ing In Vehicular Networks	[34]	The Federated Learning Techniques along with Dis- tributed Training Methods makes the distribution of data more feasible and mini-batch learning technique, where dataset is di- vides into smaller parts for parameter updates instead of the whole data set.	Mini Batch-Learning
Recent Advances and Open Issues	[35]	This Paper discusses about the existing studies in FL and their implementation in Wireless IoT along with advantages and disadvantages of it in Vehicular IoT based on privacy sensitive data and ease of autonomous driving and intelligent Transport Systems.	FedAvg Technique in Wireless IoT and Vehicular Networks

Here, the TA is a fully trustable entity since it has the very authority to manage all private/public keys to the model. After the training, the prediction phase occurs, where every individual has the authority to choose the method of prediction. If the device has sufficient performance abilities, the user can perform the prediction task on the device as well. In case the device is not sufficient to perform the prediction task, it can be performed on the server and the results can be shared with the user in an encrypted format and decrypted for the user in the service. This ensures privacy is strictly maintained throughout the user experience.

There is no mention of encryption bit type, however, Bluetooth, 5G, and Xigbee have been used in several works. The same mechanisms have been used in these works to deliver the parameters of the PRCL model. The above process can be explained schematically in Figure 4.

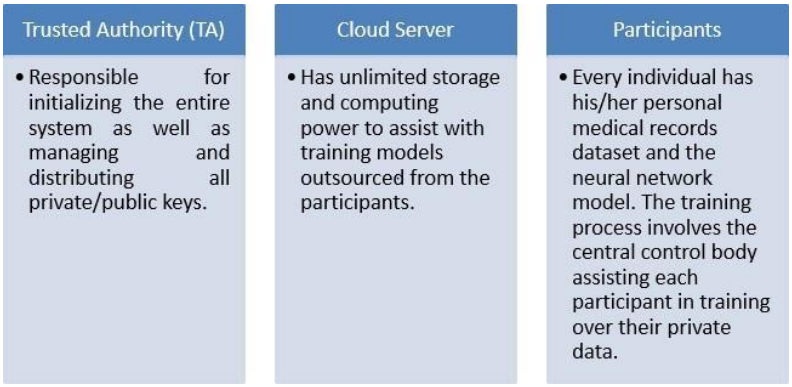

Figure 3: Parts of a PRCL Model

It can be concluded from here that PRCL is one of the best examples of implementing a federated learning-based IoT infrastructure in the field of medical healthcare. Jupiter Another such implementation of a federated learning-based IoT infrastructure in the field of medical healthcare on a regional level [42] is:

1) Jupiter: Federated Learning has been continuously proving itself as an efficient mechanism in many fields. Jupiter [13], has the capability to support data tuning, along with providing a Federated Learning facility. Besides, the infrastructure also exposes rich APIs for operations like augmentations, eliminations, and filters, etc. Hence, developers can efficiently make changes without having to restart the entire design procedure. The model, which is in a continuous development phase is managed as sessions, which are identified by a token. For the purpose of secure aggregation, the model is based on Intel SGX [13]. Intel SGX is a set of instructions that increases the security of application code and data, giving them more protection from disclosure or modification. Developers can partition sensitive information into enclaves, which are areas of execution in memory with more security protection. Unlike traditional federated learning infrastructure that serves mobile applications, Jupiter takes a model on top of dedicated communication links between users and hospitals. As a result, the model parameters are aggregated in a streaming style, and all the related information is tracked and preserved inside the encrypted memory (EPC). Jupiter works on three specific steps as represented in Fig. 5. Table 5 shows the focus of research in healthcare, their contributions, and key terms along with Federated Learning.

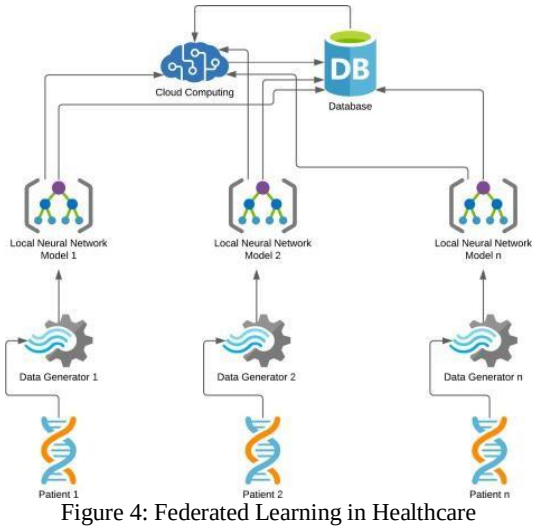

Figure 4: Federated Learning in Healthcare

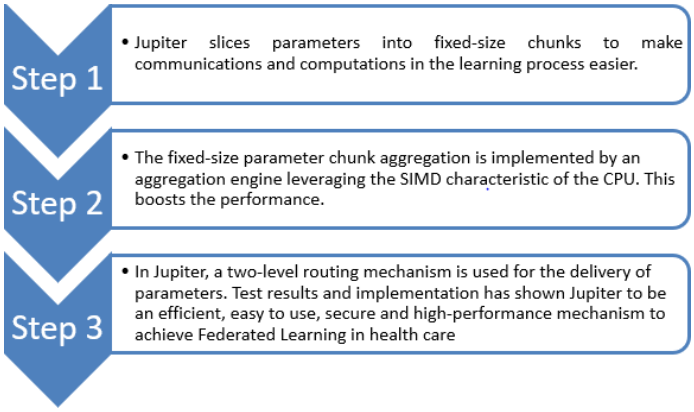

Figure 5: Jupiter Working

Table 5: Federated Learning in Healthcare

Ref.no	Focus of Research	Contributions	Key Terms
[13]	Federated Learning Platform for Regional Medical Care	Provides a Federated Learning platform called Jupiter, which can be implemented for regional medical. It involves use of optimizations and leverages SDN, DPDK and Intel SGX	TEE technology, Intel SGX, MetaData
[40]	Privacy- aware and Resource- saving Federated Learning forhealthcare	Provides a reinforcement learning based approach, called PRCL, a secure and efficient approach to medical learning. The overall model is split into 3 parts with each having a specificpurpose	CIFAR-10, Backpropagation, Paillier cryptosystem, Cryptographic Primitives, VGG-16
[41]	Wireless Body Area Network for IoT Connected Healthcare Applications	Provides an in-depth in- sight on Wireless Body Area Networks (WBAN) can be deployed for continuous monitoring of bodyparameters. The paper alsoprovides an implementation of this in the form of a Bluetooth connected solar powered device	Bluetooth, Photoplethysmography, Magneticresonance imaging, MPPT,TEG, Photovoltaic
[42]	Healthcare Information Exchange in RegionaleHealth Networks	Provides a survey and methodology of healthcare information sharing	Regional eHealth networks (RHIN),ICT
[43]	Federated Learning Framework for WearableHealthcare	Provides an implementation of FedHealth. It is a FL based framework designed for wearable technologies. The framework gives the ability to integrate multiple forms of wearable technology	Deep transfer learning, convolutional neural network, KNN, SVM, Random forest (RF), MaximumMean Discrepancy
[44]	Overview of Distributed Federated Learning: Healthcare Applications	Provides an in-depth analysis on how FL is beingactively studied today, its foundations and implementations. It also discusses two major models in the domain of FL	Over fitting, SplitLearning

2.4 Federated Learning for Edge Computing

As technology grew, the concept of the Internet of Things along with its implementation proved to be a major adoption into human lives. IoT soon turned into a very essential element where all products were connected to one another [45]. Until a few years now, the single paradigm of IoT infrastructure was that all connected devices would have to transfer data to one connected central body, the cloud server, that would process the data into useful information. With the advent of cheaper electronics and sufficient processing power on a small scale, the definition of IoT has been slowly coming to a change.

The consequence of this heavy workload on cloud server processing is Edge Computing or Fog Computing [46]. Here, the data is processed in situ or, the data is processed in the device and valuable information is sent over to the cloud. As discussed earlier, federated learning, as a concept, has the heavy potential to change the definition of IoT in a new way. Edge or Fog Computing is how this change would occur. Edge computing would enable the training of various distributed datasets without the actual movement of the data to a central body, hence providing a level of privacy and a lighter workload [47]. Machine learning and deep neural networks are computationally expensive tasks and hence are not easy to implement on smaller less powerful hardware. The above mechanism is well supported through Fig. 7. In order to tackle this issue, active learning is proposed. Active learning is an efficient framework where selective data samples are chosen that may contain critical input to the model. It is an appropriate choice when [48] labeling data is expensive and data collection is limited, as supported in Fig. 6.

It is an efficient solution to federated learning in an edge computing situation, where user privacy, data size, training cost, and uploading are the main issues to address [49]. All these should be taken into consideration while creating a scalable, reliable, secure, and distributed edge computing system [50]. This model has a significant capability to reduce the training cost by applying active learning while preserving user privacy [51] and reducing communication by use of federated learning. The various contributions and the focus of the research in edge computing together with federated learning are highlighted clearly in Table 6 which gives an insight into the topic briefly.

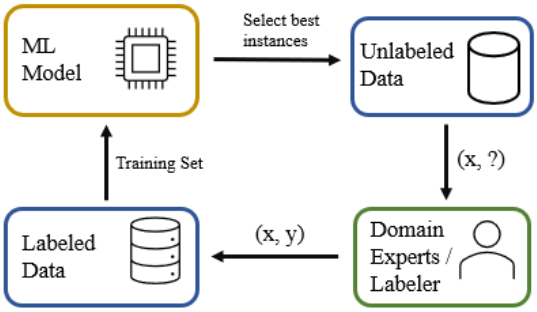

Figure 6: Active Learning Framework

1) Reinforcement Learning: Another development of edge computing on a federated learning IoT infrastructure is the implementation of reinforcement learning. Reinforcement learning is one of the most recently studied domains of machine learning. Here, agents are made to learn optimal control policy by repeated trial and error. Once optimized, they are mostly used to control real devices, such as the robotic arm. One of the first actual showcases of reinforcement learning and its abilities was Google DeepMind's Deep Q Network, which was applied to Atari Games in 2015. Since then, reinforcement learning has been applied to most games and software environments, until a few years back when it was implemented into real-world control systems, such as inverted pendulums, robot arms, quadcopters, continuum manipulators, etc.

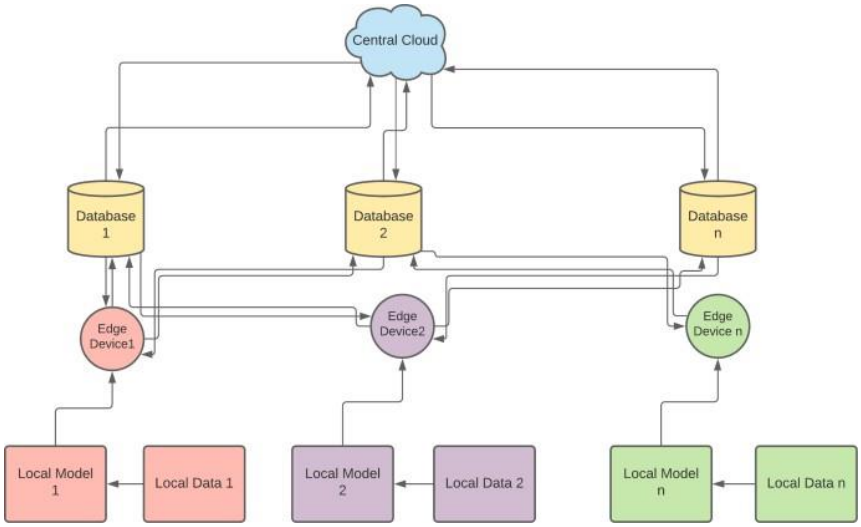

Figure 7: Federated Learning in Edge Computing

Table 6: Federated Learning in Edge Computing

Ref.no	Focus of Research	Contributions	Key Terms
[8]	Federated reinforcement learning for controlling multiple rotary inverted pendulums	Provides a reinforcement learning based approach for a federated model on edge platform. The paper aims to develop a model to control multiple rotaryinverted pendulums	Actor-Critic, Stochastic Gradient Descent, Quanser QUBE, GAE parameter
[45]	Survey of Federated Learning in Mobile Edge Networks	Provides an in-depth insight on how federated learning can be implemented on mobile devices, which also act as edge de- vices	FedAvg, resource allocation, SupportVector Machines, Stochastic Gradient Descent
[46]	DistributedActive Learning Strategies	Provides several strategies of active learning model implementations on Fog Computing platforms. Moreover, the paper provides evidence of its capabilities with reduced communication overhead, latency, and several other benefits	CNN, AcquisitionNumber, Acquisition Function, BALD, Entropy
[50]	Secure Edge Computing	Provides a review of the concepts, features, security, and applications of edge computing. Case studiesare also provided in this review	Two-Factor Authentication, Artificial intelligence, Point of Presence(POPs)
[52]	Deep Reinforcement Learning for IoT Network on Edge Computing platforms	Provides an implementation of a Deep Q-learning Network (DQN) model on edge platform. The experimental results that the implemented model can achieve higher scores when compared totraditional methodology	Deep Q-Learning Network, Q-Value, Edge Servers, Load-Balancing

As discussed earlier, machine learning and its forms are computationally expensive, and hence federated learning could be a new approach to leaving with such problems. As discussed earlier, the federated learning mechanism would enable efficient training of distributed data present on multiple interconnected devices. The combination of federated and reinforcement Learning is an approach, capable of making proper use of the joint observations from an environment. It has been observed to outperform Google's Deep Q Network under the same environment and conditions.

Federated reinforcement learning has also been applied to autonomous self-driving cars [8], [52] where the participating agents make the steering control using the knowledge of other agents. Moreover, FRL has made multiple robot models to transfer and combine knowledge to form a final robot that is capable of adapting to unknown environments quickly. The experiment was performed on a Rotary Inverted Pendulum, where the main state contains the following information pendulum angle, pendulum angular velocity, motor angle, and motor angular velocity. After every step, this information is provided to the model along with the corresponding reward, which learns them and acts accordingly. The reward is a critical component of each worker's reinforcement learning task. The federated reinforcement learning infrastructure can effectively facilitate the learning process for multiple devices [54]. Moreover, it can enhance learning speed if more agents are involved.

2.5 Federated Learning for Blockchain

IoT-based smart home devices, discussed in [9], and Industrial IoT (IIoT), discussed in [11] have gained a lot of popularity in recent years with the upcoming of the IoT-enabled smart devices and applications like communications and edge computing, artificial intelligence and big data. The generation of a large amount of data through these devices can help in providing quality service. However, since most of the computation like machine learning is not feasible to be done on the devices themselves, access to cloud services is required which involves wireless sharing of data, but data leakage, security, and privacy are serious threats and concerns when dealing with these technologies. In order to overcome this privacy preserved blockchain-based technique is used which ensure data privacy and these blockchain-based networks can also be used to store the federated learning parameters as discussed in [10].

[9] proposes a blockchain-based federated learning-based IoT smart home system that ensures the privacy and security of the data using Differential Privacy in which the machine learning models can be trained on local IoT

devices using FL and then the blockchain smart contract is leveraged to generate a global model by aggregating all the local models submitted by the local users, in this way the data security and privacy are maintained These models will be encrypted and using the mechanism of the signing of the model and having the private and public keys, verification by the miners for each model update moreover incentive-based approach for the miners to actively participate in the verification process, the security and privacy of the complete data are maintained without any fear of the breach of data.

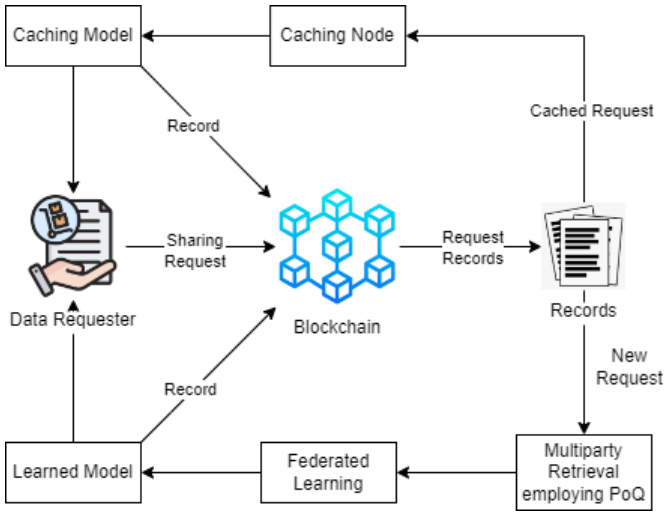

Figure 8: Data Sharing employing Permissioned Blockchain

The manufacturers first raise a request for crowd-sourcing a federated learning task and deploy a basic pre-initialized model that is available on the blockchain which can be downloaded and trained locally. The customers extract their data's features in mobile and add noise as a privacy guarantee to modify the extracted features. Next, the customers train the layers of the model with the modified features in the Mobile Edge Computing (MEC) server, and above all the traditional batch normalization has been improved by removing constraints of mean value and variance. After the training is completed the customer's signature on hashes of the encrypted models along with the private keys and deploys the trained model on the blockchain. Few miners verify senders and find the global models by aggregation and one miner encrypts the model and deploys it to the blockchain. This is an incentive-based task that motivates people to join the process. Now from the customer's side, each customer can take part in the training process using the data gathered from several IoT edge devices primarily from mobile phones, and send the updates to the network which can be then aggregated to form a new global network. The differential privacy technique, encryption, and the signing of the model by the sender prevent the attackers to steal the model or derive the original contents through reverse engineering. The crowd-sourcing methods often cause a delay in the training and process involved in the deployment and aggregation of the global model.

Ref.[11] discusses the method of data sharing where they propose a differentially private multiparty data model method of sharing based on permission blockchain. The raw data is mapped into corresponding data models by incorporating federated learning algorithms using machine learning and a new collaborative architecture is introduced for sharing data over distributed multiple parties and integrating differential privacy for further data privacy. There are three threats to the approach, first is the quality of the data provided may be good and the dishonest providers may provide inaccurate results. The second is data privacy where dishonest providers may infer the data which may lead to data leakage and the third is data authority management where the owner of the data might lose control and the data might be shared with unauthorized people or entities. The proposed method has two modules, the permission blockchain, and the federated learning module. The former establishes secured connections between the end IoT devices using its encrypted records. Retrieval and data-sharing transactions are two types of transactions in permissioned blockchain.

Table 7: Federated Learning in Blockchain

Focus /Scheme	Ref.no	Contribution / Methodology	Limitations / Gaps
Differential Privacy	[9]	Blockchain based FL IoT smart home system which uses differential privacy where models trained on local devices can be aggregated by leveraging blockchain smart contract system.	Since this is a blockchain based system, a dishonest mining network can lead to disruption in the entire network. The crowd sourcing scheme may lead to lag and delay in the training and deploying and model aggregation process.
	[11]	Differentially private multiparty data model method of sharing on the basis of permissioned blockchain where the blockchain is used only for data retrieval. Proof of training Quality (PoQ) protocol has been introduced for a new provider whose identity is stored by means of merkle tree.	As this is a data dependent process, data tampering by the dishonest miners is possible or the data owner might accidentally share the data to unauthorized parties which might be misused and lastly a dishonest mining network may lead to downfall of the blockchain network.
FLChain.	[54]	FL Chain is proposed to build a public auditable, decentralized ecosystem replacing the traditional federated learning parameters in a decentralized manner ensuring trust and providing incentive.	FL Chain requires cooperation and transparency between all the participants in the model. However, there may arise chances of misbehavior, where a miscreant may upload incorrect masked gradient which would result in an unwanted final model.
Defense	[55]	A distributed defense framework is proposed using blockchain technology and federated learning which also addresses the scarcity of training data available at local devices.	Difference in experimental and real time deployment of the model, where there is a high chance of non-participation of the participants in the during training phase iterations leading to development of a separate model whose accuracy was different from ideal experimental model.

As the data is sensitive and quite large it might be a heavy task to upload the data on the blockchain network and there are privacy issues. Due to these concerns, permissioned blockchain is used only for the retrieval of data. The real data is stored by the users locally. Upon the inclusion of a new data provider in the system, its Unique Identity (ID) is logged as a transaction on the blockchain. This transaction encompasses the profiles of the data it contributes, detailing information such as data categories, types, and sizes. The blockchain records these data profiles as transactions, collectively capturing insights from various participants. To ensure data integrity and validation, the blockchain nodes employ a Merkle tree framework for verification. This process establishes a secure and transparent record of participant identities and their corresponding data attributes within the blockchain system.

In this method, federated learning empowered consensus method Proof of training Quality or PoQ protocol is introduced instead of using the existing method of Proof of Work which requires high computation and communication resources. Fig. 8 explains the above mechanism briefly. Table 7 shows the integration of Federated Learning and Blockchain based on the previous publications highlighting the area of focus, methodologies, and limitations in a crisp manner. The differentially private federated learning mechanism, where the data as per the user's request is transferred to normalized graph vectors and the model is trained locally and since this model will be shared among other people, to protect privacy, the model is trained with noised data and once the model is received a new model will be trained based on the local data and this is done iteratively and finally a global model is generated. In [10] a blockchain-based federated learning framework is introduced which discusses the model storage patterns scalability of the network and training process of the machine learning models. In [55], FLchain has been introduced which can replace the existing federated learning parameters whose computed results might already be present in the network and it also provides a healthy environment for training models collaboratively. Blockchain combined with federated learning can also be used to establish a sustainable society by building a distributed computing defense framework by leveraging blockchain technology [56]. [57] Proposed a privacy-preserving FL platform focused on the blockchain, which secured the model update using the immutability and decentralized properties of the blockchain.

2.6 Federated Learning for Unmanned Aerial Vehicles

There has been a lot of UAV-based research in recent years with the advancement in technologies and are gaining popularity because of their widespread applications in almost all fields like surveillance and monitoring, delivery of medical supplies, military, etc. because of the flexibility and adaptability to specific applications [58]. The wireless communications associated with it can pose a huge privacy and security threat if the information about the UAV or the information it is carrying is leaked and also causes network congestion as a large amount of data will be transferred wirelessly causing lag and bandwidth issues. The data captured by the UAV can be used for various deep learning applications and hence the privacy of the information cannot be compromised. Federated deep learning is one such approach that is proposed in [59] which has three steps namely training initialization, UAV's model's training, and the global model aggregation. The basic working principle is demonstrated in Fig. 9. One of the major problems in UAVs is the communication between the device and the ground. This communication is affected by path loss and delay fading and spread. UAV trajectory planning is also important which gives the data about its energy consumption metrics hence for this FDL can be used along with Long Short-Term Memory (LSTM) for the recurrent neural network which helps in remembering the past [60].

The LSTMs make use of three gates that control the flow of information which makes them effective for sequential data. First is the input gate which determines which information should be stored from the current input in LSTM memory. Second is the forget gate which decides what information from the cell state should be discarded from the current time step and the third one is the output gate which determines what information from the cell state should be passed as output. Another problem is the data routing between the UAV and the ground station which involves transferring packets containing information like spend, location, and trajectory of the UAV which again involves security issues and can be solved using FDL incorporating LSTM for remembering history and Convolution Neural Networks.

Table 8: Federated Learning in UAVs

Focus / Scheme	Ref.no	Contribution / Methodology	Limitations / Gaps
Energy	[64]	UAV scheduling and charging are proposed for maximizing the coverage and energy efficiency.	Dynamic and adaptive control of overlappingto be incorporated.
	[65]	Maximization of deployment profitability of UAV through optimal trajectory is discussed. Jointly considered thenumber of users served by UAV, maintenance cost, and energy harvesting for trajectory planning.	Operation time of the foraging algorithmgiven depends on the group of users of UAV.
	[66]	Cognitive radio-based UAV to utilize the radio spectrum for energy maximization	Meager throughput improvement was achieved with respect to un-optimized algorithm.
Remote Sensing	[67]	Proposed airborne hyper spectral imagery of Arctic Sea ice with UAV and evaluate two atmospheric correction approaches	Use of federated learning with specific models to be explored.
	[68]	Proposed computer vision system for terrain classification using RGB camera with gimbal for stabilization.	To improvise the robustness the system studied, height of UAV and cameras consideredto be kept large.

There are many Drones as Service (DaaS) providers and it would be a major advancement if the data collected by all the providers could benefit each other, preserving privacy in terms of machine learning and data among the independent DaaS providers for the development of an intelligent transport system and internet of vehicles which is discussed in [14] and leveraging on self-revealing properties of multidimensional contract for correct reporting of UAV types. The model owner assigns a federated learning task such as collecting the information of a particular area. That area is then subdivided into sub-regions and the DaaS providers assign the drones in those sub-regions and collect the data. The training occurs in the particular drone itself and then, all the updated models from the respective drones are combined to form the global model. This method ensures data privacy as

only the trained models are sent and not the actual data. But it may happen that the model may be trained on false data by the DaaS providers or the model owners choose only the optimal UAVs which can perform the task at the lowest cost.

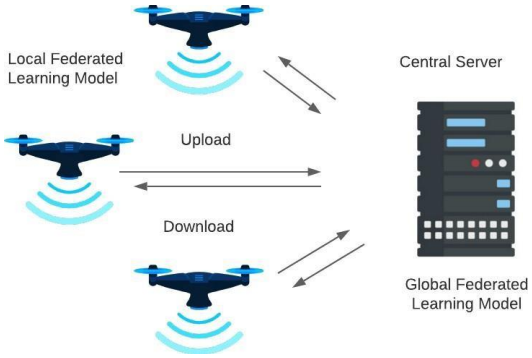

Figure 9: Federated Learning in UAVs

To avoid this multidimensional, a contract-matching incentive mechanism is designed so that the best UAV can be associated with a sub-region. The contracts can be decentralized so that traditional FL single point of failure can be avoided. Contracts operated on the basis of blockchains will be in a decentralized manner and traditional encryption algorithms can provide data security along with this. In traditional UAV swarm robotics, as discussed in [61], it becomes a difficult task in path planning and decision making by the UAVs, hence in that scenario; the centralized controlling mechanism would not be of much use. Therefore, federated Learning can be used with one leading UAV and the others as the following UAVs. A local FL model is trained by the individual UAVs which is then sent to the lead UAV who then combines all models into a global model and distributes it among all the UAVs. [61] also discusses the impacts of wireless factors such as antenna angle deviations and transmission delay affecting the convergence of federated learning. The convergence is optimized by jointly scheduling the UAV network and designing power allocation. An asynchronous federated learning (AFL) framework for multi-UAV-enabled networks can be incorporated to address the unique challenges and requirements of Unmanned Aerial Vehicles (UAV) data processing and analytics thereby ensuring security and efficient model training.

Since drones work on wireless networks, there is a high possibility of attacks like jamming which disrupt communication [62]. In order to avoid this, [63] proposes jamming attack detection security architecture based on federated learning. Flying Ad-hoc Network (FANET) along with federated learning has been used for the on-device attack detection. The UAV clients communicate and collect the global model weights from the centralized controller and update the weights into the local model which helps in local training. Since only the weight updates are sent to the global model, the privacy of the data collected by the sensors is maintained. Next, a Dempster-Shafer theory-based client group prioritization method is proposed by which the global model has the ability to select the UAV clients for global model weight updating from a group of clients that are exposed to different environments and also based on the regular contributions of the respective client. [64] also discusses Flying Ad-hoc Networks (FANET), where a number of UAVs can interact in an ad hoc way with each other. Table 8 deals with the various approaches, limitations, and schemes showcased in the respective publications in the field of Unmanned Aerial Vehicles along with federated learning.

3.0 FUTURE RESEARCH DIRECTIONS AND OPEN ISSUES

In this section, an extensive discussion on the use cases has been provided and their coalesce with federated learning and highlight the open issues and existing challenges that call for the need for further future research in this field.

- **Wireless Communication:** In wireless communication, physical layer quantization, and client selection for optimizing the resource allocation can be explored using federated learning. Data aggregation, information fusion, and scheduling in industrial wireless communication may pose a significant challenge and can be a new research direction in federated learning. The effect of Intercell interference, and cochannel interference while updating the local gradients is also a significant research problem in federated learning applications.

- **Vehicular Internet of Things:** In the federated Learning- based Vehicular IoT systems, the data collected from different edge devices is usually very different, for example, the images taken in autonomous driving by different vehicles are different, and hence it tends to have a huge variation in the data and models collected from

different edge devices which are training the local models. This causes a greater variance and deviation in the distributed data and essentially the convergence rate of the global models is decreased by a great margin. Another issue that calls for future research opportunities is to ameliorate the vehicular IoT environment as there are a lot of sensors that are involved in architecture which are an essential part of training and with varying weather and conditions between all the edge devices there are major drop-outs and garbage values which affect the precision and accuracy of the decision. When it comes to the federated learning-based Vehicular IoT architecture there are several devices such as central servers, edge servers, automation-related sensors, cameras, etc. Hence an effective combination is another futuristic research topic of interest that could handle the client's data in all possible conditions and can handle all the potential privacy risks and server crashes.

• **Healthcare:** Quality health service is a necessity and is as important as any other form of service. By the deployment of simple, yet significant technologies into healthcare, there can be much better healthcare services benefiting many people. With the development of technologies such as Jupiter or FedHealth etc, significant changes have been brought to how healthcare service is provided to people. The computer's greatest application was in the medical field where it revolutionized the way healthcare service was provided. Now, with the advent of machine learning models and federated learning infrastructures, healthcare would surely be moved to a much higher level of quality, without risking the security of personal medical information.

• **Edge Computing:** With electronics getting cheaper, the Internet of Things has flourished. Smart devices are becoming accessible to nearly everyone, leading to a great amount of data being gathered. In a future trend, it is not affordable to construct large computers to process such data. With edge devices, computers are getting smaller and more powerful. Computing such a vast amount of data is only possible with a lot of such edge devices. With computational power getting cheaper in a way, models can be trained to learn by practice. Each failure or success would teach a model to perform in a justifiable manner. This may eventually lead to a future with self-taught neural network models being deployed in various cases.

• **Blockchain:** In spite of the number of available techniques to integrate blockchain with federated learning, complete privacy assurance of data is an open issue that can be overcome by security threat analysis. Limited device resources also pose challenges to the utility and efficiency of data. These problems can be overcome by integrating modern cutting-edge machine learning and cryptography technologies with federated learning along with blockchain to prevent a breach of data and improve data sharing and transfer [70]. Since blockchain involves the so-called miners upon which the whole network depends, it becomes very important to maintain those miners, and to do so, a more practically feasible and efficient reliability method, planning, and structuring of incentive strategy mechanisms.

• **Unmanned Aerial Vehicles:** To improve the performance of federated learning in UAV, a mechanism for hostile UAV identification and segregation techniques is to be devised. Trajectory optimization, inter-UAV communication optimization, and client group prioritization are the need of the hour to further reduce communication costs. this will in turn reduce the jamming attack problems and may find a way for easy gradient update in training the federated models. Moreover, in UAV-based image classification and segmentation algorithms, the time-varying nature of the wireless channel will be one of the interesting open research problems. Joint updates of learning models with respect to channel information, fading, transmission delay, and antenna positions in UAV-based wireless networks will pose a significant challenge and result in new research directions. To better optimize the UAV performance balance needs to be arrived between computation, communication latencies, and the model learning accuracy. Also, the interrelationship between channel fading, local training, and the client's energy consumption plays a pivotal role in the frequency of model updates, convergence, and aggregation rate.

4.0 CONCLUSION

In this paper, federated learning is discussed as how its decentralized approach wherein the models are initially trained locally on the user's edge devices. Then, the parameters of the local models are uploaded to a global central cloud server for further training, and the final averaged model is sent back to the user's device, without compromising the user's data privacy. The various aspects of federated learning, its applications, and its implementations in IoT industries comprising technologies such as Blockchain, Unmanned Aerial Vehicles, Vehicular IoT, Wireless Communication, Edge computing, and IoT Healthcare have gained immense popularity and major technical advancements. In these use cases, Federated Learning has been proven to be a performance booster and has bridged the gap between high-performance computation and data security issues. Hence, overcoming the issues faced by traditional machine learning complex algorithms.

Federated Learning, particularly through the Federated Average algorithm, represents a promising approach for machine learning in scenarios where data privacy and decentralization are paramount.

The methodology's ability to train models collaboratively across distributed devices without exchanging raw data addresses privacy concerns effectively. However, the performance of Federated Learning varies based on factors such as communication efficiency, model architecture, data heterogeneity, the number of participants, and the robustness of security measures. While it offers clear advantages in preserving privacy and accommodating decentralized data sources, challenges such as communication overhead and security considerations must be carefully managed. A nuanced evaluation of its performance against traditional machine learning models is essential, taking into account specific use cases, data characteristics, and performance metrics. The potential benefits of Federated Learning underscore its relevance in contemporary machine learning landscapes, where the balance between data utility and privacy is of paramount importance.

REFERENCES

[1] K. Yang, T. Jiang, Y. Shi and Z. Ding, "Federated Learning Based on Over-the-Air Computation," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761429.

[2] Merenda M, Porcaro C, Iero D. Edge Machine Learning for AI-Enabled IoT Devices: A Review. Sensors (Basel). 2020;20(9):2533. Published 2020 Apr 29. doi:10.3390/s20092533

[3] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, 2012, pp. 647-651, doi: 10.1109/ICCSEE.2012.193.

[4] Yang, Qiang and Liu, Yang and Chen, Tianjian and Tong, Yongxin. (2019). Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology*. 10. 1-19. 10.1145/3298981.

[5] Y. Zhan, P. Li, Z. Qu, D. Zeng and S. Guo, "A Learning-Based Incentive Mechanism for Federated Learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6360-6368, July 2020, doi:10.1109/JIOT.2020.2967772.

[6] Q. Wu, K. He and X. Chen, "Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge Based Framework," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 35-44, 2020, doi: 10.1109/OJCS.2020.2993259.

[7] T. Li, A. K. Sahu, A. Talwalkar and V. Smith, "Federated Learn- ing: Challenges, Methods, and Future Directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50-60, May 2020, doi: 10.1109/MSP.2020.2975749.

[8] H. Lim, J. Kim, C. Kim, G. Hwang, H. Choi and Y. Han, "Fed- erated Reinforcement Learning for Controlling Multiple Rotary In- verted Pendulums in Edge Computing Environments," *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Fukuoka, Japan, 2020, pp. 463-464, doi: 10.1109/ICAIIC48513.2020.9065233.

[9] Y. Zhao et al., "Privacy-Preserving Blockchain-Based Federated Learn- ing for IoT Devices," *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2020.3017377.

[10] Li, Yuzheng, et al. "A blockchain-based decentralized federated learning framework with committee consensus." *IEEE Network 35.1* (2020): 234-241.

[11] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177-4186, June 2020, doi: 10.1109/TII.2019.2942190.

[12] V. Casola, A. Castiglione, K. R. Choo and C. Esposito, "Healthcare- Related Data in the Cloud: Challenges and Opportunities," *IEEE Cloud Computing*, vol. 3, no. 6, pp. 10-14, Nov.-Dec. 2016, doi: 10.1109/MCC.2016.139.

[13] J. Xing, Z. Jiang and H. Yin, ”Jupiter: A Modern Federated Learning Platform for Regional Medical Care,” 2020 *IEEE International Confer- ence on Joint Cloud Computing*, Oxford, United Kingdom, 2020, pp. 21-21, doi: 10.1109/JCC49151.2020.00012.

[14] Lim, W.Y.B., Huang, J., Xiong, Z., Kang, J., Niyato, D., Hua, X.S., Leung, C. and Miao, C., 2021. “Towards federated learning in uav-enabled internet of vehicles: A multi-dimensional contract-matching approach”. *IEEE Transactions on Intelligent Transportation Systems*, 22(8), pp.5140-5154.

[15] H. Zhang and L. Hanzo, ”Federated Learning Assisted Multi-UAV Networks,” *IEEE Transactions on Vehicular Technology*, doi: 10.1109/TVT.2020.3028011.

[16] A. Zappone, M. Di Renzo and M. Debbah, ”Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?,” *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 7331-7376, Oct. 2019, doi: 10.1109/TCOMM.2019.2924010

[17] Y. Sun, M. Peng, Y. Zhou, Y. Huang and S. Mao, ”Application of Ma- chine Learning in Wireless Networks: Key Techniques and Open Issues,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 3072- 3108, Fourthquarter 2019, doi: 10.1109/COMST.2019.2924243.

[18] S. Niknam, H. S. Dhillon and J. H. Reed, ”Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges,” *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46-51, June 2020, doi: 10.1109/MCOM.001.1900461.

[19] J. Mills, J. Hu and G. Min, ”Communication-Efficient Federated Learning for Wireless Edge Intelligence in IoT,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5986-5994, July 2020, doi: 10.1109/JIOT.2019.2956615.

[20] F. Sattler, S. Wiedemann, K. -R. Mu¨ller and W. Samek, ”Robust and Communication-Efficient Federated Learning From Non-i.i.d. Data,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 9, pp. 3400-3413, Sept. 2020, doi: 10.1109/TNNLS.2019.2944481

[21] Zhao, J., Feng, Y., Chang, X., Xu, P., Li, S., Liu, C. H., ... Crowcroft, J. (2022). “Energy-Efficient and Fair IoT Data Distribution in Decentralised Federated Learning”, *IEEE Transactions on Network Science and Engi- neering.*

[22] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor and S. Cui, ”Performance Optimization of Federated Learning over Wireless Net- works,” 2019 *IEEE Global Communications Conference (GLOBE-COM)*, Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBE- COM38437.2019.9013160.

[23] J. Xu and H. Wang, "Client Selection and Bandwidth Allocation in Wireless Federated Learning Networks: A Long-Term Perspective,", *IEEE Transactions on Wireless Communications*, vol. 20, no. 2, pp. 1188-1200, Feb. 2021, doi: 10.1109/TWC.2020.3031503.

[24] M. M. Wadu, S. Samarakoon and M. Bennis, "Federated Learning under Channel Uncertainty: Joint Client Scheduling and Resource Allocation," 2020 *IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, Korea (South), 2020, pp. 1-6, doi: 10.1109/WCNC45663.2020.9120649..

[25] M. Yan, B. Chen, G. Feng and S. Qin, ”Federated Cooperation and Aug- mentation for Power Allocation in Decentralized Wireless Networks,” *IEEE Access*, vol. 8, pp. 48088-48100, 2020, doi: 10.1109/AC- CESS.2020.2979323.

[26] H. H. Yang, Z. Liu, T. Q. S. Quek and H. V. Poor, ”Scheduling Policies for Federated Learning in Wireless Networks,” *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 317-333, Jan. 2020, doi: 10.1109/TCOMM.2019.2944169.

[27] F. Ang, L. Chen, N. Zhao, Y. Chen, W. Wang and F. R. Yu, ”Robust Federated Learning With Noisy Communication,” *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3452-3464, June 2020, doi: 10.1109/TCOMM.2020.2979149.

[28] G. Zhu, Y. Wang and K. Huang, ”Broadband Analog Aggregation for Low-Latency Federated Edge Learning,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 491-506, Jan.

2020, doi: 10.1109/TWC.2019.2946245.

[29] T. T. Vu, D. T. Ngo, N. H. Tran, H. Q. Ngo, M. N. Dao and R. H. Middleton, ”Cell-Free Massive MIMO for Wireless Federated Learning,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6377-6392, Oct. 2020, doi: 10.1109/TWC.2020.3002988.

[30] Huang, T., Ye, B., Qu, Z., Tang, B., Xie, L., and Lu, S. (2020). Physical- Layer Arithmetic for Federated Learning in Uplink MU-MIMO Enabled Wireless Networks. In IEEE INFOCOM 2020 - *IEEE Conference on Computer Communications* (pp. 1221–1230). IEEE Press.

[31] A. M. Elbir and S. Coleri, ”Federated Learning for Hybrid Beamforming in mm-Wave Massive MIMO,” *IEEE Communications Letters*, doi: 10.1109/LCOMM.2020.3019312.

[32] H. Sun, X. Ma and R. Q. Hu, ”Adaptive Federated Learning With Gradient Compression in Uplink NOMA,” *IEEE Transactions on Vehicular Technology*, doi: 10.1109/TVT.2020.3027306.

[33] D. Liu and O. Simeone, ”Privacy For Free: Wireless Federated Learning Via Uncoded Transmission With Adaptive Power Con- trol,” *IEEE Journal on Selected Areas in Communications*, doi: 10.1109/JSAC.2020.3036948.

[34] Elbir, Ahmet M., Burak Soner, Sinem Çöleri, Deniz Gündüz, and Mehdi Bennis. "Federated learning in vehicular networks." *In 2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pp. 72-77. IEEE, 2022.

[35] Z. Du, C. Wu, T. Yoshinaga, K. A. Yau, Y. Ji and J. Li, ”Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues,” *IEEE Open Journal of the Computer Society*, vol. 1, pp. 45-61, 2020, doi: 10.1109/OJCS.2020.2992630

[36] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen and M. Chen, ”In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communi- cation by Federated Learning,” *IEEE Network*, vol. 33, no. 5, pp. 156-165, Sept.-Oct. 2019, doi: 10.1109/MNET.2019.1800286.

[37] D. Ye, R. Yu, M. Pan and Z. Han, ”Federated Learning in Vehicular Edge Computing: A Selective Model Aggregation Approach,” *IEEE Access*, vol. 8, pp. 23920-23935, 2020, doi: 10.1109/ACCESS.2020.2968399.

[38] Hironobu Fujiyoshi, Tsubasa Hirakawa, Takayoshi Yamashita, “Deep learning-based image recognition for autonomous driving,” *IATSS Re- search*, Volume 43, Issue 4, 2019, Pages 244-252, ISSN 0386-1112, https://doi.org/10.1016/j.iatssr.2019.11.008.

[39] M. A. A. Babiker, M. A. O. Elawad and A. H. M. Ahmed, ”Convolu- tional Neural Network for a Self-Driving Car in a Virtual Environment,” *2019 International Conference on Computer, Control*, Electrical, and Electronics Engineering (ICCCEEE), Khartoum, Sudan, 2019, pp. 1-6, doi: 10.1109/ICCCEEE46830.2019.9070826.

[40] M. Hao, H. Li, G. Xu, Z. Liu and Z. Chen, ”Privacy-aware and Resource- saving Collaborative Learning for Healthcare in Cloud Computing,” *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148979.

[41] T. Wu, F. Wu, J. Redoute´ and M. R. Yuce, ”An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications,” *IEEE Access*, vol. 5, pp. 11413-11422, 2017, doi: 10.1109/ACCESS.2017.2716344.

[42] Harno, K., Nykänen, P., Ohtonen, J., Seppälä, A. and Kopra, K., 2009, February. “Healthcare information exchange in regional eHealth networks implications for initiatives in advancing shared care”, *International Conference on eHealth, Telemedicine*, and Social Medicine, pp. 42-45, IEEE, 2009.

[43] K. Harno, P. Nykänen, J. Ohtonen, A. Seppälä and K. Kopra, "Healthcare Information Exchange in Regional eHealth Networks Implications for Initiatives in Advancing Shared Care," *2009 International Conference on eHealth, Telemedicine, and Social Medicine*, Cancun, Mexico, 2009, pp. 42-45, doi: 10.1109/eTELEMED.2009.24.

[44] Y. Chen, X. Qin, J. Wang, C. Yu and W. Gao, ”FedHealth: A Feder- ated Transfer Learning Framework

for Wearable Healthcare,", *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 83-93, 1 July-Aug. 2020, doi: 10.1109/MIS.2020.2988604.

[45] J. Jeon, J. Kim, J. Huh, H. Kim and S. Cho, "Overview of Distributed Federated Learning: Research Issues, Challenges, and Biomedical Ap- plications," *2019 International Conference on Information and Commu- nication Technology Convergence (ICTC)*, Jeju Island, Korea (South), 2019, pp. 1426-1427, doi: 10.1109/ICTC46691.2019.8939954.

[46] W. Y. B. Lim et al., "Federated Learning in Mobile Edge Net- works: A Comprehensive Survey,", *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 2031-2063, thirdquarter 2020, doi: 10.1109/COMST.2020.2986024.

[47] J. Qian, S. P. Gochhayat and L. K. Hansen, "Distributed Active Learning Strategies on Edge Computing," *2019 6th IEEE Interna- tional Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, Paris, France, 2019, pp. 221-226, doi: 10.1109/CSCloud/EdgeCom.2019.00029.

[48] M. Leo, F. Battisti, M. Carli and A. Neri, "A federated ar- chitecture approach for Internet of Things security," *2014 Euro Med Telco Conference (EMTC)*, Naples, 2014, pp. 1-5, doi: 10.1109/EMTC.2014.6996632.

[49] B. Anggorojati, P. N. Mahalle, N. R. Prasad and R. Prasad, "Capability- based access control delegation model on the federated IoT network," *The 15th International Symposium on Wireless Personal Multimedia Communications*, Taipei, 2012, pp. 604-608.

[50] S. Savazzi, M. Nicoli and V. Rampa, "Federated Learning With Coop- erating Devices: A Consensus Approach for Massive IoT Networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4641-4654, May 2020, doi: 10.1109/JIOT.2020.2964162.

[51] M. Alrowaily and Z. Lu, "Secure Edge Computing in IoT Sys- tems: Review and Case Studies," 2018 *IEEE/ACM Symposium on Edge Computing (SEC)*, Seattle, WA, 2018, pp. 440-444, doi: 10.1109/SEC.2018.00060.

[52] P. Watson, "Application Security through Federated Clouds," in *IEEE Cloud Computing*, vol. 1, no. 3, pp. 76-80, Sept. 2014, doi: 10.1109/MCC.2014.46.

[53] Q. Liu, L. Cheng, T. Ozcelebi, J. Murphy and J. Lukkien, "Deep Reinforcement Learning for IoT Network Dynamic Clustering in Edge Computing," 2019 *19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Larnaca, Cyprus, 2019, pp. 600- 603, doi: 10.1109/CCGRID.2019.00077.

[54] G. De Luca and Y. Chen, "Semantic Analysis of Concurrent Computing in Decentralized IoT and Robotics Applications," 2019 *IEEE 14th International Symposium on Autonomous Decentral- ized System (ISADS)*, Utrecht, Netherlands, 2019, pp. 1-8, doi: 10.1109/ISADS45777.2019.9155627.

[55] X. Bao, C. Su, Y. Xiong, W. Huang and Y. Hu, "FLChain: A Blockchain for Auditable Federated Learning with Trust and Incentive," 2019 *5th International Conference on Big Data Computing and Communications (BIGCOM), QingDao*, China, 2019, pp. 151-159, doi: 10.1109/BIG-COM.2019.00030.

[56] Sharma, PK, Park, JH & Cho, K 2020, "Blockchain and federated learning-based distributed computing defence framework for sustainable society", *Sustainable Cities and Society*, vol. 59, 102220.

[57] S. Awan, F. Li, B. Luo, and M. Liu, "Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain," *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2561–2563.

[58] H. Shakhatreh et al., "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," *IEEE Access*, vol. 7, pp. 48572-48634, 2019, doi: 10.1109/ACCESS.2019.2909530.

[59] B. Brik, A. Ksentini and M. Bouaziz, "Federated Learning for UAVs- Enabled Wireless Networks: Use Cases, Challenges, and Open Prob- lems," *IEEE Access*, vol. 8, pp. 53841-53849, 2020, doi: 10.1109/AC- CESS.2020.2981430.

[60] Sherstinsky, Alex. "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network." *Physica D: Nonlinear Phenomena* 404 (2020): 132306..

[61] T. Zeng, O. Semiari, M. Mozaffari, M. Chen, W. Saad and M. Bennis, ”Federated Learning in the Sky: Joint Power Allocation and Scheduling with UAV Swarms,” *ICC 2020 - 2020 IEEE International Confer- ence on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148776.

[62] Yaacoub JP, Noura H, Salman O, Chehab “A. Security analysis of drones systems: Attacks, limitations, and recommendations”. *Internet of Things*. 2020;11:100218. doi:10.1016/j.iot.2020.100218

[63] N. I. Mowla, N. H. Tran, I. Doh and K. Chae, ”Federated Learning- Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Net- work,” *IEEE Access*, vol. 8, pp. 4338-4350, 2020, doi: 10.1109/AC- CESS.2019.2962873.

[64] M. Mozaffari, W. Saad, M. Bennis, Y. Nam and M. Debbah, ”A Tutorial on UAVs for Wireless Networks: Applications, Chal- lenges, and Open Problems,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2334-2360, thirdquarter 2019, doi: 10.1109/COMST.2019.2902862.

[65] Y. Cai, Z. Wei, R. Li, D. W. Kwan Ng and J. Yuan, "Energy-Efficient Resource Allocation for Secure UAV Communication Systems," 2019 *IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakesh, Morocco, 2019, pp. 1-8, doi: 10.1109/WCNC.2019.8885416..

[66] X. Liu, M. Chen, S. Wang, W. Saad and C. Yin, ”Trajectory Design for Energy Harvesting UAV Networks: A Foraging Approach,” 2020 *IEEE Wireless Communications and Networking Conference (WCNC)*, Seoul, Korea (South), 2020, pp. 1-6, doi: 10.1109/WCNC45663.2020.9120514.

[67] Y . Pan, X. Da, H. Hu, Z. Zhu, R. Xu and L. Ni, ”Energy-Efficiency Optimization of UAV-Based Cognitive Radio System,” *IEEE Access*, vol. 7, pp. 155381-155391, 2019, doi: 10.1109/ACCESS.2019.2939616.

[68] König, Marcel, Gerit Birnbaum, and Natascha Oppelt. 2020. "Mapping the Bathymetry of Melt Ponds on Arctic Sea Ice Using Hyperspectral Imagery" *Remote Sensing* 12, no. 16: 2623.

[69] Matos-Carvalho, J.P.; Moutinho, F.; Salvado, A.B.; Carrasqueira, T.; Campos-Rebelo, R.; Pedro, D.Campos, L.M.; Fonseca, J.M.; Mora, A. “Static and Dynamic Algorithms for Terrain Classification in UAV Aerial Imagery”, *Remote Sens*. 2019, 11, 2501

[70] Aledhari, M., Razzak, R., Parizi, R.M. and Saeed, F., 2020. “Federated learning: A survey on enabling technologies, protocols, and applications”, *IEEE Access*, 8, pp.140699-140725