Federated Learning: Attacks and Defenses, Rewards, Energy Efficiency: Past, Present and Future

DIMITRIS KARYDAS, HELEN C. LELIGOU
Department of Industrial Design and Production Engineering,
University of West Attica,
250 Thivon & P. Ralli str 122 41 Egaleo,
GREECE

Abstract: - Federated Learning (FL) was first introduced as an idea by Google in 2016, in which multiple devices jointly train a machine learning model without sharing their data under the supervision of a central server. This offers big opportunities in critical areas like healthcare, industry, and finance, where sharing information with other organizations' devices is completely prohibited. The combination of Federated Learning with Blockchain technology has led to the so-called Blockchain Federated learning (B.F.L.) which operates in a distributed manner and offers enhanced trust, improved security and privacy, improved traceability and immutability and at the same time enables dataset monetization through tokenization. Unfortunately, vulnerabilities of the blockchain-based solutions have been identified while the implementation of blockchain introduces significant energy consumption issues. There are many solutions that also offer personalized ideas and uses. In the field of security, solutions such as security against model-poisoning backdoor assaults with poles and modified algorithms are proposed. Defense systems that identify hostile devices, Against Phishing and other social engineering attack mechanisms that could threaten current security systems after careful comparison of mutual systems. In a federated learning system built on blockchain, the design of reward mechanisms plays a crucial role in incentivizing active participation. We can use tokens for rewards or other cryptocurrency methods for rewards to a federated learning system. Smart Contracts combined with proof of stake with performance-based rewards or (and) value of data contribution. Some of them use games or game theory-inspired mechanisms with unlimited uses even in other applications like games. All of the above is useless if the energy consumption exceeds the cost of implementing a system. Thus, all of the above is combined with algorithms that make simple or more complex hardware and software adjustments. Heterogeneous data fusion methods, energy consumption models, bandwidth, and controls transmission power try to solve the optimization problems to reduce energy consumption, including communication and compute energy. New technologies such as quantum computing with its advantages such as speed and the ability to solve problems that classical computers cannot solve, their multidimensional nature, analyze large data sets more efficiently than classical artificial intelligence counterparts and the later maturity of a technology that is now expensive will provide solutions in areas such as cryptography, security and why not in energy autonomy. The human brain and an emerging technology can provide solutions to all of the above solutions due to the brain's decentralized nature, built-in reward mechanism, negligible energy use, and really high processing power In this paper we attempt to survey the currently identified threats, attacks and defenses, the rewards and the energy efficiency issues of BFL in order to guide the researchers and the designers of FL based solution to adopt the most appropriate of each application approach.

Key-Words: - Blockchain Federated Learning, Energy Efficiency, Security, Privacy, Defenses, Rewards.

Received: October 11, 2023. Revised: March 5, 2024. Accepted: May 7, 2024. Published: June 12, 2024.

1 Introduction

Federated Learning (FL) holds significant importance in the current technology landscape due to several key factors. Internet of Things (I.o.T.) applications with the growth of big data can lead to the true implementation of many intelligent situations such as smart cities, smart meters, smart hospitals, etc.. These clever brushes can fuel many critical applications such as smart transfer, smart industries, healthcare, and smart surveillance, [1]. For the successful development of these smart services, a huge number of IoT devices is required which are forecasted to collect around 572 Zettabytes of data, [2]. Such a noticeable increase in the size of the IoT network and the volume of accompanying data open up attractive opportunities a real opportunity for artificial intelligence and mechanical learning. For this purpose, we can train Artificial Intelligence (A.I.) and Machine Learning (M.L.) algorithms via multiple independent sessions, each using our own datasets to optimize these smart IoT applications. Depending on the type of local workers, FL can be divided into cross device and cross silo. Cross-device workers are mostly mobile phones, tablets, speakers, and other IoT terminal appliances. These local workers can log out at any time in the model training process. The cross-silo workers are mostly large institutions that have high data storage and computational capabilities.

In general, the security aspects that are relevant to FL, are confidentiality, availability, and integrity. Data privacy preservation, data sovereignty, decentralization, incentive mechanisms, scalability, cross-organizational collaboration, and resilience to data poisoning attacks are significant topics to be taken into consideration when an FL solution targeting a specific sector is to be designed. FL allows collaborative machine learning models to be trained across multiple decentralized devices without sharing raw data, ensuring sensitive data remains on users' devices. It also maintains data sovereignty for individual users or organizations, particularly in regions with strict data sovereignty laws. FL distributes the training process across a network of nodes, eliminating the need for centralized authority, and enhancing the system resilience. Incentive mechanisms can be implemented, fostering participation and cooperation.

The immutable nature of blockchain provides a transparent and auditable record of model updates, building trust among stakeholders in sectors where this is highly required for example like healthcare and finance sectors. In this way, the data remain in the administrative domain of their owner, and it is only the model updates that are exchanged with all the exchanges/updates being recorded in the blockchain where whatever is written cannot be altered, [3]. Combining FL with blockchain or secure multiparty computer technology, the model update provider cannot be traced and thus, any attack with respect to (inappropriate) model update can be detected, [4]. Although blockchain adds/improves the level of security, it is not a panacea. It is essential for people, businesses, and governments to make proactive efforts to defend against FL attacks, especially those who will adopt this technology, and encourage a culture of total awareness, [5], [6], [7], [8], [9], [10].

Adopting the same principle of performance-related rewarding in blockchain systems, federated learning reward systems are designed to encourage contributions by rewarding participants for their collaboration according to their performance contributions. Examples of applications include centralized machine learning for mobile crowdsensing, distributed energy storage systems, or data marketplaces, [11]. Rewards and “awards” can come in a variety of shapes, such as cash, cryptocurrencies, non-fungible tokens (NFTs), or goodwill. A fair evaluation of the contributions is necessary for the distribution of incentives to be equitable. The main objectives of FL incentive systems are to reward institutions for their participation in FL and to entice institutions to make high-quality contributions to the gradient, [12], [13]. However, the rewarding mechanism is in itself prone to attacks.

Another key issue for FL systems is energy. [14], [15], [16], more specifically, both transmission energy and computational energy usage must be taken into account especially when FL is executed in the far edge of the network systems in devices that may not be connected to permanent energy supply infrastructure, such as low-power computing devices and mobile phones which have limited energy budgets, [17], [18], [19]. Energy consumption becomes an optimization problem with the goal of reducing the system's overall energy usage while observing a delay cap, [20].

To sum up, as shown in Figure 1, the three aspects that have to be thoroughly analyzed by any prospective designer/developer of federated learning-based solution are: the adopted reward mechanism, the defense mechanisms to be put in place, and the energy efficiency depending on the nature of the application and the devices implementing the FL scheme.

Reward mechanis ms
Defence Mechanis ms
Energy Efficiency

Fig. 1: The working gears of a complete FL system must have an enabled defense system it must be energy efficient and it must have reward-based character, [21], [22]

In this paper, we survey the literature relevant to a) attack and related defense mechanisms, b) rewarding mechanisms, and c) energy efficiency as well as present the recent developments relevant to quantum technologies and brain-inspired FL systems. Quantum technologies and brain-inspired FL systems aspire to offer higher energy efficiency and performance together. Our aim is to offer an advanced kick-start to researchers that are interested in the area and most importantly to guide the prospective designers and implementers of FL systems to make appropriate design choices. For example, the rewarding schemes that incentivize citizens are different than those that may incentivize organizations; the security level (measures to defend against a rich or less rich set of attacks) depends on the nature of the application and its specificities. Additionally, we discuss the interplay, [21], [22] among the three dimensions mentioned above and shown in the Figure 1. The importance of this discussion increases if we take into consideration i) the legislation as the General Data Protection Regulation (GDPR), [23] and the California Consumer Privacy Act (CCPA) the US equivalent of GDPR [24], which makes data sharing even less likely to happen and ii) the 2030 Climate Target Plans according to which the EU's ambition is to reduce greenhouse gas emissions to at least 55 percent below 1990 levels by 2030. This is a significant increase compared to the existing target of above the previous target of at least 40 percent, [25].

2 Defense Measures against Attacks in Federated Learning

2.1 Introduction

The standard project of the “Federated Machine Learning Application and architecture framework” was approved by the IEEE Standards Committee in December 2018. As a result of that, an increasing number of academics and technical specialists joined the standards working group and contributed to the creation of IEEE Standards regarding FL, [26]. There are numerous inherent hazards to privacy and security. Malicious local workers may sabotage the availability, confidentiality, and integrity of data before the model is trained, contaminating it. The central server and local clients make up the two main FL roles in general. The antagonist may gain access to the main server or some local clients. The adversary can influence the global model while the model is being trained by managing the samples or model updates. The global model's performance will suffer as a result, or a backdoor will be left open. The adversary can also infer the personal data of additional trustworthy local workers during the model training and prediction phases, including through membership inference and attribute inference. Despite differences in privacy FL has included more privacy-preserving methods, attacks on FL are still possible, [27]. Examining the local workers' data quality prior to the model training phase is one way to guarantee the FL model's validity. High-confidence data can significantly lower the frequency of poisoning attacks and increase the model's efficacy. A different approach is to analyze past local worker and server behavior. Based on the system logs, credibility measurement, and verification procedures should be suggested. Additionally, during the training process, the dependability of the local employees should also be evaluated dynamically. Generally speaking, malicious local employees behave differently from the majority of dependable local employees. Therefore, the unreliable local employees can be removed by auditing the model behavior uploaded to the central server, [28].

The defense systems must identify hostile devices, block them from further data impact, or eliminate the impact they have on the overall model. The defense systems also provide protection from specific types of attacks e.g. poisoning attacks. The suggested approaches are primarily reactive and constantly track client behaviors. The main approach of filtering out rogue clients has been suggested. AI and ML algorithms are used in this strategy to identify model modifications or irregular data distributions. Another approach using the same basic idea, but used to a multi-victim malicious, user attack, is suggested and known as sniper. Sniper gives a different suggestion for defending against poisoning attacks. It’s a different suggestion for defending against poisoning attacks. This method entails evaluating the effectiveness of the global model with each new model update, [11].

In this section, we will discuss those attacks and relevant defense mechanisms.

2.2 Attacks and Defense Measures

We start with the backdoor attack which was introduced earlier. The major strategy of protection from backdoor attacks involves reducing the model's size to lessen its complexity and capacity while maybe increasing its accuracy. Pruning is the name of this method. The resulting model is less expressive, making backdoor assaults more difficult to execute. Such a technique also brings up some advantageous side effects. In fact, the fewer parameters minimize both the likelihood of message interception and the cost of communication, [12]. For the backdoor attack protection in a federated learning system, the authors of this paper [29] suggest Focused-Flip Federated Backdoor Attack (F3BA). It makes use of focused weight sign manipulation to allow the hostile clients to compromise only a tiny portion of the least significant model parameters. Instead of explicitly scaling maliciously uploaded clients' local updates, the attack simply swaps the weights of some inconsequential model parameters. F3BA is able to escape and achieve a high attack success rate in the majority of tests. From this, the authors claim that even while the current stage of backdoor protection offers some robustness, they still expose the vulnerability to advanced backdoor attacks. In [30], FL was analyzed from an adversarial standpoint and created a straightforward defense mechanism, especially for backdoor attacks. The main concept of this defense strategy was to modify the learning rate of the aggregation server, per dimension and every round, based on the sign information of agents' updates. The studies they provide, they demonstrate how this defense significantly lowers backdoor accuracy while just slightly degrading overall validation accuracy. Overall, it outperforms some of the recently proposed defenses in the literature. As a final comment, they believe the insights behind their defense are also related to training in non-. i.d. setting, even in the presence of no adversaries. The differences in local distributions can cause updates coming from different agents to steer the model toward different directions over the loss surface. In a future work, they plan to analyze how Robust Learning Rate (R.L.R.) influences the performance of models trained in different non- i.d. settings.

Another research, [31], focused on the security against model-poisoning backdoor assaults, known as "backdoor data poisoning" that involves the injecting of several watermarked, incorrectly labeled training examples into a training set. On usual data, the watermark has no effect on the model's test-time performance, but on watermarked samples, the model consistently makes mistakes and generates errors, [32]. To solve this problem, authors suggest Robust Filtering of one-dimensional Outliers (RFOut-1d), a defense mechanism based on a robust filtering of one-dimensional outliers in the federated aggregation operator, based on the hypothesis that updates from adversarial clients would represent outliers in the Gaussian distribution of clients' updates. The results of assessing RFOut-1d in a variety of circumstances under various backdoor as-saults and comparing it to state-of-the-art defenses reveal that their claim is correct. As a result, state, RFOut-1d is a highly effective defensive that reduces the effectiveness of backdoor attacks to the point of (nearly) nullifying them throughout the course of all learning cycles. In several cases, RFOut-1d exceeds the results obtained without any attack, demonstrating its ability to filter out clients who impede the training process. In contrast to previous defenses, it does not impede the FL process by maintaining (or even improving) the model's performance in the initial job. By filtering out customers who deviate from this solution, the model's convergence to the common solution is hastened and optimized. To summarize, it is demonstrated that RFOut-1d is a high-quality protection as well as an appropriate federated aggregation operator by effectively halting the effect of attacks while encouraging global model learning.

A dataset could achieve appropriate privacy and utility trade-offs thanks to the noise defense described in this paper [33]. Even though many tasks are straightforward, including signature recognition, with data complexity comparable to the well-known MNIST dataset utilized in the test can benefit from split learning. By post-training the computational server's model segment with noise while keeping the data owner's model segment unchanged, the privacy and utility trade-off could be made better. However, this strategy eliminates the data owner's exclusive means of model inversion defense. Due to its connection to differential privacy, a Laplacian noise distribution was chosen for this study. However, other alternative noise distributions should have a similar protective impact and may potentially offer a better privacy and utility trade-off. The authors showed that, under a split neural network training environment, a user's data is vulnerable to exposure by an opponent. Even with a little understanding of the problem that needs to be solved, this problem still occurs.

In many cases, a malevolent person tries to recover the secret dataset that was used to train a supervised neural network with model inversion attacks, [34]. A model inversion attack that is effective should produce realistic samples from a variety of sources that appropriately reflect each of the classes in the private dataset, [35]. The suggested work is a workable and successful defense against FL model inversion attacks. In order to obscure the gradients of the sensitive data, the authors introduce a concealing sample that mimics the sensitive data. Their suggested method makes sure that the samples that are used to hide sensitive information are visually distinct from the sensitive data in order to obfuscate the created sensitive information. In order to preserve the critical data and prevent performance loss, the samples are concealed using adaptive learning. Studies revealed that this strategy provides the best defense against model inversion attacks without losing FL performance when compared to other similar defense strategies.

Another major issue is that sending the FL updated models to a centralized server may become a difficult task due to privacy issues and significant connection constraints. Thus, a recent paper [36], suggests an efficient approach for user assignment and resource allocation across hierarchical FL solutions designed for IoT heterogeneous systems. The findings of this study showed that, for the same level of model fidelity, the suggested approach may greatly speed up FL training and lower communication overhead by offering a significant reduction in the number of communication rounds between edge nodes and centralized server.

Against Phishing and other social engineering attack that are often used to steal user data, the authors of [37] suggest the use of Phishing Detection with Generative Adversarial Networks (PDGAN). PDGAN is a revolutionary poisoning defense strategy in federated learning. The suggested approach is based on a server-side generative adversarial network that can reconstitute participants' training data. The suggested method verifies the accuracy of each participant's model using the generated data before identifying attackers. Results of the experiment show that by verifying the participant model's accuracy, the PDGAN can successfully reconstruct the training data and defend against the poisoning attack. Authors intend to investigate this poisoning defense for federated learning with differential privacy at the device, class, or user levels as future work.

Anomaly detection methods in data analysis are events or observations that deviate significantly from the majority of the data and do not conform to a well-defined notion of normal behavior. The authors of [38] suggested a federated learning-based anomaly detection system for precisely identifying and categorizing threats in IoT networks. This method can work as an effective defense system. The FL implementation portion of the suggested method shares computing resources with on-device training, and various GRU layers guarantee higher attack classification accuracy rates. The ensemble, which integrates the predictions from various GRU layers, greatly enhances the performance of the technique. The potential advantage of user data privacy is a safer layer to IoT networks, increasing the dependability of IoT devices. Their evaluations show that their suggested method outperforms intrusion detection algorithms that don't support FL. As a future study, we can focus on improving the suggested method using an IoT testbed and evaluating it using real-time data from de-vice-specific data sets that can categorize all known and undiscovered IoT device vulnerabilities.

In the study [39], authors have proven that by alternating between assaulting and operating normally, the adversary evades the defense systems' mechanisms and penalties. This can happen in on/ off label piping, good/bad-mouthing, and on-off free-riding attacks. With good/ bad-mouthing attacks, adversaries send selected gradients that either boost or lessen the influence of the chosen victim's gradients on the global model. They have studied each of these assaults using numerous data sets and proven that they are successful against existing defense systems in federated learning. They have implemented all these attacks on five different FL algorithms using different data sets, and two neural network models. These findings demonstrate that the suggested attacks are successful in each of these scenarios. They have built a new federated learning algorithm which has been proven capable of mitigating each of the proposed assaults concurrently while maintaining effective against previously proposed threats.

Researchers demonstrate that a Distributed Backdoor Attack (DBA) is more persistent and successful than a centralized backdoor attack in typical FL through extensive testing on multiple datasets, including Lending Club Loan Data (LOAN) using image datasets in distinct settings, [40]. In both single-shot and multiple-shot attack scenarios, DBA improves attack resiliency, convergence speed, and attack success rate. Researchers show that DBA is more cunning and is capable of eluding two powerful Federated Learning techniques. Using feature visual interpretation to examine its function in aggregate, the effectiveness of DBA is described. The authors undertake an in-depth investigation of the main variables that are unique to DBA to investigate its properties and limitations. According to the findings, DBA is a fresh and more potent attack against FL than the ones currently used as backdoor attacks. For assessing the adversarial robustness of FL, the study and findings may offer fresh perspectives and new threat assessment techniques. A Trusted Aggregation (TAG): Model Filtering Backdoor Defense in Federated Learning may be an effective method for DBA In this paper [41], motivated by differences in the output layer distribution between models trained with and without the presence of backdoor attacks, authors propose a defense method that can prevent backdoor attacks from influencing the model while maintaining the accuracy of the original classification task. TAG leverages a small validation data set to estimate the largest change that a benign user's local training can make to the output layer of the shared model, which can be used as a cutoff for returning user models. Experimental results on multiple data sets show that TAG defends against backdoor attacks even when 40 percent of the user submissions to update the shared model are malicious.

Researchers from the University of California, Berkeley, [42], describe potential challenges when a consumer with no local data can perform a local gradient update. These consumers with no local data are called ‘Free-riders’. The free rider problem is the burden on a shared resource that is created by its use or overuse by people who aren't paying their fair share for it or aren't paying anything at all. Much attention has been paid to the free-rider challenge of peer-to-peer programs. There are a number of attacks that can be used by an attacker and possible defenses against such attacks. This study shows a new detection method called STD-DAGMM, a high-dimensional anomaly detection method, is proposed. This method is particularly successful in detecting anomalies in model parameters. It was also effective in detecting most “free riders” under most conditions tested. Furthermore, it is found that differential privacy, especially the privacy encouragement approach in combined studies, tends to identify riders who do not participate in the efficacy. The STD-DAGMM method in other attacks can be found in combined studies, such as venom attacks that are attractive for research. The field concluded that much remains to be learned about “free riders” about the autonomy and countermeasures, especially because of the many proposed solutions. It is believed that preliminary research may inform subsequent efforts in this area. In this research and in the same field against “free riders”, [43], it is proposed a new defense method based on the Weight Evolving Frequency model, referred to as WEF-Defense, Authors first collect the weight evolution frequency (defined as WEF-Matrix) during local training. For each client, it uploads the WEF matrix of the local model to the server along with the model weight for each iteration. The server then separates the “free-riders” from the benign clients based on the difference in the WEF matrix. Finally, the server uses a personalized approach to provide different global models for respective clients.

An ethical framework for evaluating and distinguishing between different types of customer privacy attractions has been presented in [44]. By analyzing frequent parameter updates, they show how adversaries can reconnect private local training data. (e.g., local gradient or weight-update vector). The impact of different attack schemes and hyperparameter settings on client private lock cage attacks is identified and analyzed in a federated learning study with four widely used benchmark datasets. Initially, a formal and experimental analysis of attacker potential is presented reverse-engineer private local training data by simply analyzing parameter updates from local training distributed. (e.g., local gradient or weight-update vector). Then the possible effects of different attack algorithm settings and federated learning hyperparameter settings on the attack efficiency and attack cost are investigated. In addition, their approach to communication-efficient FL protocols with different gradient compression ratios tests, measure, and evaluate the client's effectiveness - privacy leakage attacks Their tests also include some early mitigation techniques to demonstrate the importance of providing a systematic attack analysis process towards understanding the loss of client secret lockage threats.

Recent studies have demonstrated that Byzantine assaults launched by erroneous or malevolent clients can be successful against standard federated learning, [45], [46], [47]. Even if there is only one attacker, the accuracy of the model can drop from 100 percent to 0 percent. The accuracy of the combined global model can be reduced to 0 percent maximum probability in the extreme case where the attacker knows the local updates of all non-malicious clients and only needs to configure other terms as opposed to another normal linear combination. Nowadays, with the advent of federated learning, researchers have found a new way to address the security and privacy concerns of dispersed training. Researchers now examine current methods of dealing with

Byzantine invasion. They also offer new attack mechanisms that could threaten current security systems after careful comparison and discussion supported by experimental findings.

Researchers found that local model poisoning attacks, which alter the local models sent from the compromised worker devices to the master device during the learning process, can weaken the federated learning methods. The machine learning algorithms claimed to be resilient against Byzantine failures of some worker devices. In particular, an attacker can modify the local models on the compromised worker devices so that the aggregated global model deviates most from the direction along which the global model would change in the absence of attacks, increasing the error rates of the learned global models. Additionally, the search for such carefully constructed local models might be framed as an optimization problem. To counteract local model poisoning attacks, we can expand already-existing data poisoning attack countermeasures. Such all-encompassing protections work in certain situations but fall short in others. These findings demonstrate the need for new countermeasures to fend off local model poisoning attempts. This research is only applicable to unintended poisoning attacks. De-signing new defense measures against local model poisoning assaults, such as new techniques to find compromised local models and new adversarial resistant aggregation rules, is also important, [48]. As a solution to this, a paper [49] suggests Local Malicious Factor (LoMar), a two-phase defense algorithm. In phase I, LoMar scores model updates from each remote client by measuring the relative distribution over their neighbors using a kernel density estimation method. In phase II, an optimal threshold is approximated to distinguish malicious and clean updates from a statistical perspective. Comprehensive experiments on four real-world datasets have been conducted, and the experimental results show that this defense strategy can effectively provide protection from a poisoning attack on the Federated Learning system.

The weight attack is another attack that is difficult to be mitigated by current defense strategies. The key challenge is that the server cannot immediately assess the caliber of the local data sets of the clients. Researchers then talk about some potential de-fences. Although distance-based methods like Multi-Krum and Fast Aggregation against Byzantine Attacks (FABA) cannot withstand the weight attack, we still believe they are a viable option. Multi-Krum and FABA both fall short because they have a propensity to ignore updates that deviate significantly from the distribution as a whole. They believe that by examining the distribution of local updates, it is possible to directly avoid the "bad" updates by developing a new distance-based technique. Additionally, as demonstrated in trials, performance-based defense strategies like Zeno outperform other methods by a wide margin. This type of protection strategy can perform better in the future because analyzing an update's performance is the simplest way to tell if it is benign or harmful. When the clean test data set is carefully planned for particular investigations, the "bad" updates produced by the weight attack will undoubtedly behave differently. Regarding the statistics-based and target optimization-based mitigation strategies, that they are adamant they can successfully mitigate the weight attack by fully utilizing the statistical properties of local updates or choosing an appropriate loss to optimize the goal function, [50].

2.3 Blockchain-based Security Enhancements for FL

A centralized network built around a single, central server that handles all major model management functions presents vulnerabilities studied in [51]. Its authors proposed Blockchain Assisted Decentralized Federated Learning (BLADE-FL). BLADE-FL is a decentralized FL system that uses blockchain technology to assist the FL system by preventing malicious clients from poisoning the learning process and further providing a self-motivated and trusted learning environment for them. The authors demonstrated how successfully the BLADE-FL can address any potential problems, particularly the single point of failure problem that exists in a conventional FL system. They have also looked into recently emerging challenges like client laziness, resource allocation and privacy. Last but not least, they have also offered additional relevant potential fixes and experimental findings to address these problems, which offer directions for the construction of the BLADE-FL framework. As future possibilities, the research could include some asynchronous and heterogeneous studies for various client capabilities, such as processing power, training data size, and transmitting variety, as well as a smart contract design that offers a fair distribution of incentives between training and mining. Also, a different approach could be by lowering the transmission cost of light-weight models using quantization and quantum technology and sketches.

In principle, using blockchain technology, FL Security can be thought of as a distributed database— a public ledger— that is accessible to everybody. The database verifies and forgery-proofs each new entry. It suggests a method for establishing device trust in which local model validation is carried out by a blockchain network in place of the central server of a traditional centralized FL infrastructure, while model aggregation is done on the client side. Every client updates a network miner that is linked to it. All model updates must be exchanged and verified by miners. A miner executes a Proof of Work (P.o.W.) for a specific operation with the goal of creating a new block stored. The created block also contains the aggregated local model updates that are available for download by other network participants. The global model can then be locally computed by each client. By approving model updates, this method makes poisoning attacks more challenging [50] New literature and research are added every day, vanguard algorithms try to detect and block the threats that appear every day. Of course, the defense mechanisms are always a step behind the attack and there is no safe mechanism that can close all the backdoors. For this reason, increased vigilance is required and no system can be considered safe and reliable at the given time.

3 Rewards and Blockchain in Federated Learning

3.1 Introduction

Rewards and incentives are resource management techniques used by all types of systems. Rewards and incentives are used by a federated learning system to improve the system, to increase productivity, and to encourage members to contribute to better quality work.

3.2 Alternative Approaches

The idea of carrying out more righteous deeds with better experiences occurs in a suggestion of a reward-based participant selection strategy which leverages the special property of the FL. The proposed approach for the FL system chooses participants by taking into consideration rewards, with the goal of prioritizing the use of the better experiences of the agents who do remarkable activities for learning, as shown in Figure 2, [52]. The proposed scheme increases the performance and efficiency of learning, according to the findings of the experiments the authors conducted. Learnings were carried out more quickly and with fewer agents when utilizing the proposed scheme. They intend to do varied evaluations in numerous IoT applications as part of their future work, using the suggested participant selection scheme to a range of IoT systems. Additionally, they will examine the scenario in which the suggested approach is used for FL with devices that operate in highly dissimilar settings.

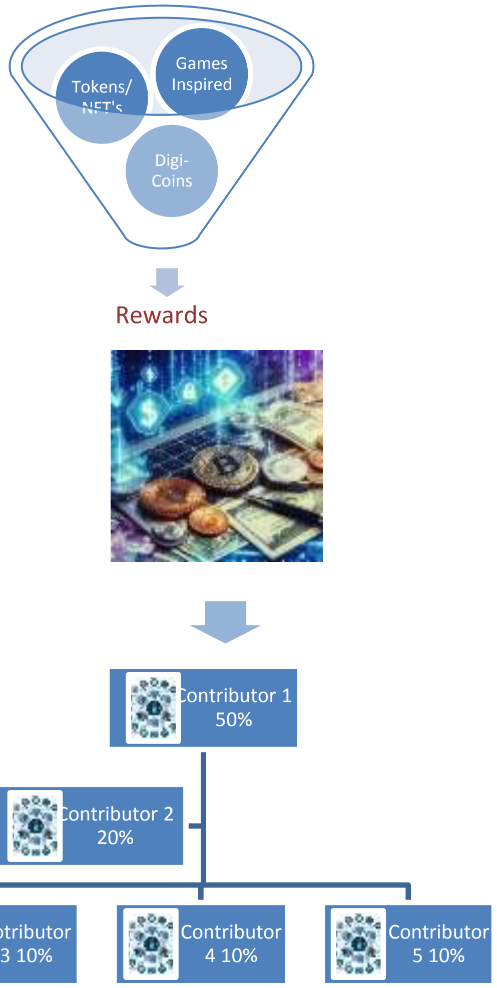

Fig. 2: Rewards in an FL system can take different forms for example, monetary value tokens, or games inspired methods. The fair distribution of rewards depends on a fair quantification of the contributions, [52].

In [53], the authors first assess the contributions of FL institutions to model bias as well as predictive performance. They create incentive systems based on the Shapley Value (S.V.) approximation method that can encourage contributions to trustworthy AI by rewarding results with a good prediction performance and minimal absolute bias. This research adds to the body of knowledge in three different ways. In order to respond to previous requests for study in this area, they begin by analyzing the model bias in a medical FL situation. By doing so, they discover a slight influence of the distribution of chest X-ray scans across various institutions on the FL model bias in some cases. They also show that S.V. approximations can assess bias in medical FL in addition to contributions to predictive performance. Thirdly, they create incentive structures that compensate FL institutions for their contributions to model bias and forecast accuracy. By doing so, they respond to earlier requests for study on FL reward systems and incentives for reliable AI.

The interaction between a server and all participating devices in a federated learning system is modelled in [54] using a Stackelberg game. (The Stackelberg leadership model is a strategic game in economics in which the leader firm moves first and then the follower firms move sequentially). In order to maximize each device's specific utility, the authors search to identify the best training times for the server, reward, and each device. Both the server-side deadline and the device-side upload time are taken into account by their model. Examine how the size-based and accuracy-based incentive rules affect the overall system equilibrium by taking them into consideration. They demonstrate that the suggested game, which has a lower bound on the Price of Anarchy (P.o.A), is a legitimate utility game. The P.o.A., [55] is also a game in algorithmic game theory. Price of Anarchy is the difference between the social cost of the worst Nash equilibrium and the social optimum (i.e., assigning strategies to players to achieve the lowest possible social cost). The typical assessment of the potential efficiency loss owing to individual selfishness, when players are just thinking about their own utility and not the overall welfare of society, is commonly conceived of as this very effective and important notion. By incorporating the uncertainty in the upload time, they also expand their model. Their demonstration shows that in the variable upload time mode, devices spend more time on local training. To put the proposed federated learning system into practice and enable devices to run mining and teaching simultaneously, they construct a blockchain-powered testbed. The presented models and theoretical findings are validated by experiments carried out on top of it.

The authors of [56] used blockchain technology with federated learning to address the issues of data privacy, security, and fair compensation in distributed machine learning. A thorough methodology for scalable recording and rewarding of gradients utilizing a mix of off-chain databases of records and blockchain was provided. In order to validate and verify gradients and choose an appropriate device reward, they proposed Class-Sampled Validation Error Scheme (CSVES). While restricting the amount of uploads and validating the reported data cost per device, they created a Proof of Concept, [57], with a small group of clients and rounds to show that the blockchain does not interfere with the federated learning aggregate. Finally, they create a list of Federated Learning and Blockchain components that need further investigation in order to be implemented as part of future work. As a future study, is the modification of CSVES to be a more accurate system for judging the quality or utility of local data used to train the model would involve more development, testing, and analysis of variations on CSVES. They also intend to research other validation approaches that can precisely estimate the amount of compensation for a gradient upload, either based on the confirmed number of data points or on assessed data model advancement. The need to establish a uniform training method that ensures that two devices using the same data calculate the same gradients has also been highlighted. Adopting this standard would ensure consistency in submitted results and fairness in reward distribution.

The authors of [58], have presented an effective approximation of CGSV with a bounded error and have described a novel Cosine Gradient Shapley Value (CGSV) to fairly evaluate the expected marginal contribution of each agent's uploaded model parameter update/gradient in FL without needing an auxiliary validation dataset. By utilizing the trick of sparsifying the aggregated parameter update gradient downloaded from the server as reward to each agent such that its resulting quality is commensurate to that of the agent's uploaded contributed parameter update gradient, authors have developed a novel training time fair gradient reward mechanism based on the approximate CGSV.

In order to fairly assess the quality and value of the model parameter updates gradients uploaded and contributed by the agents in federated learning (FL) gradient-based collaborative machine learning (CML), the authors [59] introduce a novel formulation based in the same algorithm Cosine Gradient (CGSV) too. Using this formulation again, the authors utilize it to design their corresponding rewards in the form of downloaded gradients. Their strategy guarantees that agents who upload better gradients can also download better gradients, producing better local models with smaller training losses. Scientists theoretically and practically show that their approach is effective in terms of fairness and prediction performance. In addition, their method is non-restrictive and significantly more effective than existing baselines; that is, it takes very little server processing power and no additional dataset. Through a hyperparameter that regulates the level of altruism, their method offers significant flexibility for the trade-off between fairly distributed and precisely just rewards. The research question is: “Can we attain both optimally or is there some sort of unavoidable trade-off between justice and performance?” Interestingly, a greater altruism degree can occasionally result in superior predictive performance. It would be fascinating to think about the idea of fairness when there are some rivals for future work. Additionally, we would think about applying our fairness guarantee and CML work to additional types of cooperative Bayesian optimization, [60].

As a result, an agent should eventually be rewarded with converged model parameters whose resulting training loss (and consequently predictive performance) is closer to that of the server, as demonstrated by fairness guarantee, if they upload con-tribute higher-quality parameter updates gradients throughout the entire training process. On numerous benchmark datasets, they have empirically proven the efficiency of our fair gradient reward method in terms of fairness, predictive performance, and time overhead. Fair gradient reward system, in particular, is substantially more effective than several FL baselines because it only necessitates little server computations.

3.3 Tokens and Cryptocurrency inspired Reward Methods

The authors of this work, [61], have suggested a fresh tokenized reward Federated Learning technique that makes use of tokens make participating clients' contributions and the platform for training that successfully encourages long-term engagement from high-quality data suppliers. Contrary to earlier research, this one includes incentives for both providers, instead of employing loss, and consumes and profiles data quality using accuracy measurement without additional overheads measurement. Clients are compensated as consumers using their novel proposed metrics (i.e., token reduction ratio and utility enhancement ratio based on utility measurement). High-quality clients are frequently chosen as providers with fair compensation using previous accuracy records and random exploration. As a result, their incentive strategy decreases the rounds and tokens issued by malicious providers while boosting the rounds and tokens issued by legitimate providers when compared to the baseline. Therefore, their incentive strategy reveals a token difference between legitimate and malicious providers, improving the final accuracy by up to 7.4 per cent in comparison to the baseline.

A strong integration of clients with diverse profiles for collaborative FL training is made possible by training a FL model in a communication-efficient way. Authors of this research, [62], presented also a tokenized rewards method for clients that provided high-quality updates. They created a comprehensive strategy in which token distribution is structured as quota and is based on the value of contributions made during the model aggregation phase. Subsequently this policy helps better resource sharing due to better visibility of local instance parameters. The suggested tokenized incentive system, which prevents weak updates and attacks on decentralized web architecture expected on Web 3.0 Finally extensive simulations were used to investigate and evaluate the effectiveness of the proposed method.

In the book article [63], authors proposed FedCoin, a blockchain-based payment system to support federated learning procedure. Offerings like FedCoin could add free computing resources to community systems to complete the expensive computing services required by the FL incentive. The proof of the Shapley (PoSap) consensus protocol specifies the Shapley value of each FL client, which represents each client's input in the entire FL model. A well proposed PoSap, which currently builds traditional hash-based protocols instead of a bitcoin-based blockchain payment system. Each payment is recorded invariably in volume. FedCoin FL eliminates the need for a central FL service by rewarding customers with incentives. Research findings show that FedCoin can accurately estimate the Shapley Value-based contributions of FL customers across the FL sample, providing an upper bound on the amount of computational power needed to reach a consensus. By doing so, it provides new opportunities for non-data owners to contribute to the development of the FL environment.

A survey, [64], addressed the question to what extent bias occurs in FL medicine and how to prevent excessive bias through reward systems. We first evaluated how to measure the contribution of medical institutions to predictive performance and bias in medical FL cross silo with a Shapley value approximation method. In a second step, the researchers designed different reward systems that incentivize contributions for high predictive performance or low bias. They proposed a combined incentive reward system. The paper evaluated our work using multiple medical chest X-ray datasets focused on patient subgroups defined by patient gender and age as a first attempt to implement a reward mechanism in the real world.

The reward mechanisms are theoretically infinite. The rise of cryptocurrencies platforms and the connection to the like of Ethereum II can add limitless possibilities. We can create a decentralized application for which the participants of that particular application are the decision-making authority like voting systems, banking systems, shipping and agreements.

4 Energy Efficiency

There are two ways to earn resources either by reward and payment or by saving them. It is important to design computing systems from scratch whose architecture does not require large amounts of energy to operate. For these reasons researchers in theoretical computer science are figuring out strategies to use less energy during computation.

A federated learning system with various wireless or non-wireless networks can be widely used in various fields, including the military, healthcare, and banking e.c.t. However, participants and any kind of device most of the time, have limited resources in terms of power and most of the time from a single battery like mobile phones or many types of sensors.

Many of these devices also usually have little storage capacity and computing power and have other applications to run such as phone calls, instant messaging, cameras e.t.c. Thus, in order to improve the energy efficiency and extend the network bandwidth and battery life cycle, the system must present an energy-efficient clustering and routing approach based on this genetic algorithm. This genetic algorithm will give federated learning to speed up and enhance the whole process.

The researchers have theoretically demonstrated that very straightforward hardware and software adjustments might reduce the energy used to operate today's common software procedures in half. Additionally, they have demonstrated how synchronized modifications to both the hardware and software might multiply the energy efficiency of computing by a million. For routine tasks like searching and sorting, the researchers have already created new energy efficient Artificial Intelligence algorithms that, when used with specially designed computer hardware, should result in significant energy savings. New energy-efficient methods for processing huge data, such as during web searches, will result in even bigger savings, [65].

The study in [66], offers a federated learning method based on a multi-source heterogeneous data fusion method. The approach, which is based on Tucker's decomposition theory, offers multi-modal data fusion and memory usage reduction by building a high-order tensor with spatial dimensions of heterogeneous data, and it is evaluated against many alternative approaches. This technique may successfully combine data from multiple sources that are heterogeneous, lowering the privacy and security obstacles associated with data communication. On the basis of the heterogeneous data structure owned by the training nodes, the approach may simultaneously adapt to various heterogeneous data types, lowering the training size of redundant models and enhancing distributed training effectiveness. The reduction of network impact through maximizing the use of communication resources, cutting down on unnecessary transmission, and decreasing network impact.

Researchers in [67], have looked into the issue of FL resource allocation via wireless communication networks and energy-efficient computation and transmission. They used the convergence rate to derive the time and energy consumption models for FL. To reduce the network's overall computation and transmission energy, they have developed a joint learning and communication problem using these joint learning and communication models. They have presented a low-complexity iterative technique to address this issue, and for each iteration of this process, they have deduced closed-form solutions for the computing and transmission resources. The suggested scheme performs better than traditional schemes in terms of overall energy usage, especially for low maximum average transmit power, according to numerical data.

This research, [68], has looked into how each participating device in federated learning allocates bandwidth, controls transmission power, and changes the CPU frequency. The introduction of the two weight parameters allowed for the optimization of the weighted average of total completion time and energy consumption. It is possible to determine the appropriate resource allocation technique by modifying two weight parameters. Additionally, this increases the flexibility and adaptability of our resource allocation plan to accommodate various FL system requirements. They can attend from the experiments that their resource allocation technique advances the state of the art, particularly in cases where the overall completion time is tightly constrained.

Millions of devices are anticipated to train machine learning models in this paper's [69] as first examination of a sustainable FL model. For devices with intermittent energy availability, this research offers a straightforward and scalable training technique with verifiable convergence guarantees. Authors also demonstrate how the proposed framework can significantly outperform energy-neutral benchmarks in terms of training performance. Their framework is made up of three primary parts: client scheduling, local client training, and server-side global model update. Future research includes investigating other energy arrival model options.

In order to conserve energy from two sides, the central server and edge devices, scientists looked at an energy-efficient federated scheme used in wireless federated edge learning networks. First, using wireless resource management and learning parameter allocation, they created an optimization problem to reduce the energy consumption, including communication and compute energy. Second, by using sparse rather than typical DNN, energy can be further conserved based on the examination of the energy consumption of various learning models. This sparsification and optimization strategy has a significant impact on energy savings, according to numerical results, [70].

In an effort, [71], to practical implementation of federated learning (FL) over wireless networks which are known to require balancing energy efficiency, convergence rate and target accuracy due to the limited available resources of these devices. However, scenarios will not be practically applicable for mobile devices where they have limited resources, as DNNs usually have high computational complexity and memory requirements. Researchers propose a green-quantized FL frame, which represents data with a finite level of accuracy in both local training and uplink transmission. Here they propose and capture through the use of quantized neural networks (QNNs) that quantize the weights and activations in a fixed precision form. In the considered FL model, each device trains its QNN and transmits a quantized training result to the base station. The simulation results show that the proposed Pareto boundary-based FL framework of the problem is characterized to provide efficient solutions using the normal boundary inspection method. Using a design to balance the trade-off between the two objectives while achieving a target accuracy derived from the use of the Nash negotiation solution can reduce energy consumption until convergence by up to 70% compared to a basic FL algorithm that represents data with full accuracy without compromising the convergence rate.

5 Quantum Technology Federated Learning Systems

Reaching a balance between performance and energy consumption has always been a difficult objective to achieve for energy and power-aware applications. It’s hard to achieve a balance between performance and energy efficiency. A relatively recent research field for defense systems for Federated Learning is Quantum Systems according to [72]. Quantum Computing is believed to be more energy efficient compared to classical computing methods especially when high accuracy or complexity is required. According to [73], quantum computers are faster and more accurate. However, the extent to which it can reduce energy usage remains unclear, as experts have not yet agreed on metrics to determine its energy consumption, [74]. The Energy Consumption of a Quantum Computer scales very differently than that of classical computers, a good example of which is the simulation that is used to model the probability of different outcomes in a process that cannot easily be predicted due to the intervention of random variables [72]. In [72], authors compare the differences of Byzantine Attacks problems between classic distributed learning and quantum federated learning. They modify the previously proposed four kinds of Byzantine tolerant algorithms to the quantum version. They conduct simulated experiments to show a similar performance but extreme speed capabilities of the quantum version with the classic version.

In [75], authors suggest quantum federated learning (QFL), or communication-efficient learning of Variational Quantum Algorithm (VQA) from decentralized data. The model is trained using a VQA, which accesses centralized data; distributed computing can greatly reduce training overhead. The information is, however, privacy-sensitive. By aggregating the updates from local computation to share model parameters, they enhance data privacy inspired by the traditional federated learning algorithm. They create an extension of the traditional VQA with the goal of locating ap-approximative optimums in the parameter environment. Finally, they implement a variational quantum tensor networks classifiers, an approximate quantum optimization for the model and a variational quantum eigen solver for molecular hydrogen on the TensorFlow Quantum processor. Their algorithm shows model precision using decentralized data, which performs better on processors available today. Importantly, QFL might stimulate new research in the area of safe quantum machine learning, [76].

Table 1. Comparison between Frontier supercomputer (June 2020) and Quantum D-Wave's 2000 qubit Computer & Quantum Microsoft's Azure quantum computing cloud-based Federated Learning with Quantum Data service, [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87]

Feature	**Frontier supercomputer (June 2020)**	**Quantum D-Wave's 2000 qubit Computer**
Speed [77]	1.102 exaFLOPS	158 million times faster than the most sophisticated
Power Requirements [78]	21 MW	The unit only consumes 25kW of power More energy efficient alternative to classical computing methods.
Cost [79] [80]	$600 million	D-Wave's 2000 qubit quantum computer – $15 million. Microsoft's Azure quantum computing cloud-based service $500 dollars' worth of Azure Quantum Credits for use with each participating quantum hardware provider.
Information needed [81] [82]	Complex information	Complex information (Multi-dimensional analysis in quantum computing)
Processing [83] [84]	Sequential processing & Complete Datasets	Sequential processing & Complete Datasets
Federated Learning Capabilities [85]	On demand (Code enabled)	On demand (Code enabled)
Decentralized Character [86]	On request/ permissions	On request/ pemissions
Rewards [87]	On demand (Code enabled)	N/S (Possible Capability based in other features like Defences and Energy Consumption)

To conclude our reference to quantum computing for federated learning systems, Table 1 presents the comparison between Frontier supercomputer (June 2020) and Quantum D-Wave's 2000 qubit Computer & Quantum Microsoft's Azure quantum computing cloud-based Federated Learning with Quantum Data service. We focus on areas where federated learning has growth potential by the presentation of the problems, we analyze such as energy consumption, reward and defense and security mechanisms, [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87].

6 Brain Inspired Federated Learning Systems.

Neural networks (ANNs) have been used as tools in machine learning and artificial intelligence. We create images, speech, robots, play games in a large and independent palette of applications. Although neural networks were originally based on the biological neuron, there are fundamental and fundamental differences between the operating mechanisms of neural networks (ANNs) and those of the biological brain of any species, particularly in terms of learning processes, biochemical and electrochemical processes of energy autonomy and reward. This paper presents a comprehensive review of current brain-inspired learning representations and artificial neural networks, and why not the application of bio-brains themselves to federated learning based on these advantages such as decentralized nature, embedded reward mechanism, and negligible amounts of energy. We also propose and compare biological mechanisms as a function of cost, type of information, reward, etc. to demonstrate and enhance the capabilities of these networks. Additionally, we delve into the potential advantages and challenges that come with this approach. All this could create many avenues for future research, apart from the bonds of silicon, in this rapidly evolving and amazing field that could bring us closer to understanding matter and intelligence itself.

In order to train energy-demanding models on resource-constrained edge devices, wireless edge artificial intelligence (AI) frequently needs very big and diverse datasets. A Lead Federated Neuromorphic Learning (LFNL) technique is a brain-inspired, decentralized, energy-efficient computing approach built on spiking neural networks, [88], [89]. This method allows edge devices to take advantage of brain-like biophysiological structures to jointly train a global model while assisting in private preservation. According to experimental findings, LFNL achieves recognition accuracy that is similar to that of edge AI methods currently in use, while also significantly reducing data traffic and computational latency. Additionally, LFNL greatly lowers energy consumption when compared to traditional federated learning, with only 1.5 percent accuracy loss. Thus, the suggested LFNL can aid in the advancement of edge AI and computing that is inspired by the human brain.

6.1 Future Potential Technologies using Brain Tissues

Organoids, [90], are three-dimensional tissue cultures usually derived from human pluripotent stem cells. What looks like a cluster of cells can be engineered to function like a human organ, mirroring its basic structural and biological characteristics. Under the right laboratory conditions, genetic instructions from donated stem cells allow or-ganoids to self-organize and grow into any type of organ tissue, including the human brain.

In the future, [91], [92], researchers present a collaborative, iterative multidisciplinary program with the goal of estblishing Organoid Intelligence as a type of real biological computing that uses the scientific and bioengineering methods outlined here in an ethically sound manner to harness brain organoids. The ultimate goal is to usher in a biological computing transformation that could vastly outpace silicon-based computing and AI while having a profound global impact. In particular, they expect Organoid Intelligence-based biocomputing systems to facilitate faster decision-making (including on large, sparse, and heterogeneous datasets that federated learning has major issues), continuous learning throughout tasks, and outstanding improved energy efficiency (that also federated learning has issues) and data structure and economy. Additionally, the creation of "intelligence-in-a-dish" provides unmatched opportunities to understand the biological underpinnings of human cognition, learning, and memory, as well as a variety of disorders linked to cognitive deficits, potentially assisting in the discovery of novel therapeutic strategies to address these issues.

There are already hardware approaches to artificial intelligence that use an adaptive pool computation of biological neural networks in a brain organoid. In this approach - which the scientists call Brainoware - the computation is performed by sending and receiving information from the brain organoid using a high-density multielectrode array. There are no limitations such as high power and time consumption, Neumann congestion (physical separation of data from data processing), and Moore's law slowdown transistor doubling in an integrated circuit, also we must never forget that the human brain has the dopaminergic pathway mostly involved in reward, as shown in Figure 3, [93].

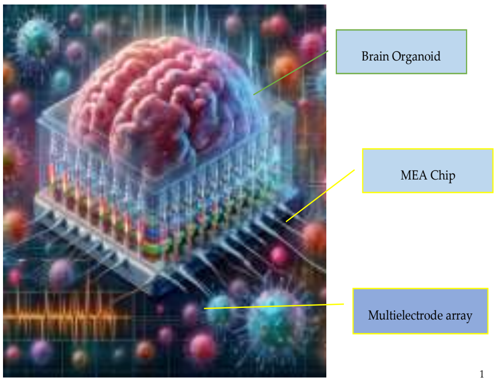

Fig. 3: Brainoware, [93], the computation is performed by sending and receiving information from the brain organoid in an MEA chip using a high-density multielectrode array

In Table 2 the comparison between Frontier supercomputer (June 2020) and the hu-man brain, an area that O.I. inspired, is presented. We focus on areas where we can say ‘’Organoid Intelligence and federated learning’’ has growth potential. The presentation of the problems we analyze such as energy consumption, reward, and security mechanisms that federated learning and O.I. synergy has a future potential.

In conclusion, for all these models and features mentioned in the above chapters although federated learning presents interesting solutions for a number of real-world applications it should be pointed out that successful and continuous development in current systems requires careful consideration of computational overhead. Effective implementation of federated learning solutions is highly dependent on controlling computation costs, and current research and development is focused on improving FL algorithms and infrastructures to make them more scalable and efficient. Real-time processing needs and integration problems are very dynamic. These obstacles can be overcome and the full potential of federated learning can be realized with the help of developments in edge computing, distributed systems, and optimization approaches.

Table 2. Comparison between Frontier supercomputer (June 2020) and Human Brain, [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [90], [91], [92], [93]

Feature	Frontier supercomputer (June 2020)	Human Brain
Speed [77] [90] [91] [92] [93]	1.102 exaFLOPS	~1 exaFLOPS (estimate)
Power Requirements [78] [90] [91] [92] [93]	21 MW (Electricity)	10–20 W (Electrochemistry)
Cost [79] [80] [90] [91] [92] [93]	$600 million	Not applicable
Cabling (Cost depended) [81] [82] [83] [90] [91] [92] [93]	145 km (90 miles)	850,000 km (528,000 miles) of axons and dendrites
Information needed [81] [82] [90] [91] [92] [93]	Complex information	With few and/or uncertain data
Processing [83] [84] [90] [91] [92] [93]	Sequential processing & Complete Datasets	Both sequential and parallel processing & Highly heterogeneous, and incomplete datasets
Federated Learning Capabilities [85] [90] [91] [92] [93]	On demand (Code enabled)	Enabled
Decentralized Character [86] [90] [91] [92] [93]	On request/ permissions	Enabled
Rewards [87] [90] [91] [92] [93]	On demand (Code enabled)	Natural process Bio-electrochemical (Diverse stimuli with a positive or desirable outcome)

7 Overview of the Three Challenges: Attacks and Defenses, Rewards and Energy Efficiency

Federated learning must take into account the protection of privacy and security attacks, as well as the detection of dishonest participants who freely gather incentives or rewards. A collection of these mechanisms is important for federated learning. It will crystal show the challenges and possible future directions. This part defines the topics that will be investigated in future studies. Based on our research, we have compiled the following collection of questions:

We've talked about the attacks that benefited from transmitting fake local model updates. In terms of incentives, adversaries freely obtained the profit and instantly reduced the computational resources that had been employed in the model training process. From an incentive standpoint, the adversary is free to profit and instantly reduces the computational resources employed in the model training process. More study is required on attacks in terms of contribution measurements and rewards. Other incentive strategies to detect spurious model updates should be investigated in future studies, which is a more interesting subject. Some methods, such as giving specific scores to honest and malicious participants after detection, may be useful in identifying malicious participants. At this time, some FL tools are available that are applied in a federated learning environment, such as Federated Learning Protection Frameworks, and are detailed with their features and limitations.

Only a few of these systems currently allow a simulated federated attack in a real environment. As a result, future studies should focus on developing FL frameworks with the goal of providing maximum privacy protection features. Several privacy and security attacks have been discussed, demonstrating that traditional FL does not ensure data protection. The updated global model includes traces that allow private and sensitive data to leak. Previously, in federated learning, some methods were used to protect information from adversaries, but they had some drawbacks, such as hiding specific updates from clients and adding noise, which reduced model accuracy. More cryptographic techniques are needed to withstand potential attacks. They result in significant computation overhead in terms of encryption and transmission costs. It is difficult to train data on multiple devices, and it is critical for federated learning to combine data from multiple devices. Furthermore, when compared to ML, FL has a slower effect on convergence. In this case, training smaller models with compressing methods can accelerate convergence. The development of future algorithms, but dealing with this issue needs additional approaches.

The FL is associated with high latency and low bandwidth speeds. These high latency and low bandwidth speeds affect the entire reach of a network. The yield that is obtained is reduced which leads to a high cost in resources and energy. Resources that could be directed to other vital points of a federated learning system such as defense or retaliation. In traditional cases, minimal latency is required for rapid learning from the backpropagation method, [94], [95]. This job is simple in ML, but it requires the use of millions of devices to train the algorithm. It delays learning and increases latency. Furthermore, because most of the settings in FL are accompanied by Wi-Fi or 5G, bandwidth is a technical problem. The Wi.Fi. or 5G bandwidth is inadequate for the FL environment, resulting in high latency and a relaxed algorithm training process. The device's bandwidth has not improved in comparison to the device's increased computing capability, resulting in a communication bottleneck. It is suggested that in the FL environment, 5G and B5G technologies be used and that communication expenses be addressed by considering model compression and quantization methods.

Integrating data from various devices is crucial for federated learning because training data across different devices is a difficult job. This happens why because federated learning involves training machine learning models on multiple decentralized devices or nodes, each with its own local dataset.

The data show great diversity. Integrating data from various devices enriches the training dataset by capturing a wider range of features and patterns. In this diversity also appear the greatest danger. It is an environment where they can easily hide and prowl. It is in conjunction with maintaining privacy that it is critical to keep the model from collapsing.

Data from different devices helps balance the distribution of training data across the federated learning network, ensuring that the model learns from representative samples of the population, regardless of device type, giving rewards where the samples are truly valuable to it.

Integrating data from various devices involves aggregating model updates or gradients that are computed locally on each device. This aggregation process combines knowledge from different devices, allowing the federated model to benefit from the collective artificial intelligence of the entire network while maintaining the privacy of the individual device and the entire network.

Overall, the integration of data from various devices plays a key role in federated learning by dealing with data heterogeneity through algorithms while preserving privacy, improving model performance, and enabling collaborative learning in decentralized environments with self-rewarding power balancing. model. Once the collective information is leveraged from the various data sources, federated learning empowers organizations to build robust, privacy-preserving machine learning models that can operate efficiently in distributed and dynamic settings for the benefit of the model as well as the participants.

Additionally, compared to ML, FL has a delayed effect on the convergence. In this situation, training smaller models using compressing methods can quicken consensus. All this affects System Heterogeneity and Training.

Regarding the rewards of a federated learning system, the authors propose a reward-based participant selection strategy for the FRL system, which increases the performance and efficiency of learning by prioritizing the better experiences of agents who do remarkable activities. Other researchers assess the contributions of FL institutions to model bias and predictive performance, create incentive systems based on SV applications, and create incentive structures to compensate FL institutions for their contributions. It responds to earlier requests for study on FL reward systems and incentives for reliable AI.

Other authors propose models with the interaction between a server and all participating devices in a federated learning system using a game like Stackelberg game to identify the best training times for the server, reward, and each device. Games like this add an oligopoly market model is a non-cooperative strategic game where one firm moves first and decides how much to produce, while all other firms follow. The Price of Anarchy (P.o.A.) is an algorithmic game theory that is the difference between the social cost of the worst Nash equilibrium and the social optimum (i.e., assigning strategies to players to achieve the lowest possible social cost). By incorporating uncertainty in the upload time, we expand their model and demonstrate that in the variable up-load-time mode, devices spend more time on local training. To put the proposed federated learning system into practice, we can construct a blockchain-powered testbed and validate their models and theoretical findings.

Another concept is to use blockchain technology combined with federated learning to address the issues of data privacy, security, and fair compensation in distributed machine learning. There are proposals like CSVES to validate and verify gradients and choose an appropriate device reward while restricting the amount of uploads and validating the reported data cost per device. We can use a Proof of Concept with a small group of clients and rounds to show that the blockchain does not interfere with the federated learning aggregate. Future studies to assess if CVES may be modified to be a more accurate system for judging the quality or utility of local data used to train the model. Another interesting proposal is that we have developed a novel training time fair gradient reward mechanism based on the Cosine Gradient Shapley value (CGSV) to fairly evaluate the expected marginal contribution of each agent's uploaded model parameter update/gradient in FL without needing an auxiliary validation dataset. On numerous benchmark datasets, they have empirically proven the efficiency of their fair gradient reward method in terms of fairness, predictive performance, and time overhead. The suggestion of a tokenized reward FL technique that makes use of tokens to incentivize long-term engagement from high-quality data suppliers. It decreases the rounds and tokens issued by malicious providers and boosts those issued by legitimate providers. This increases the also and final accuracy.

The tokenized rewards for clients provided high-quality updates to train an FL model in a communication-efficient way. The token distribution is structured as a quota and is based on the value of contributions made during the model aggregation phase. This strategy favors quality participation and allows for the integration of clients with diverse profiles. Simulations were used to evaluate and analyze how well the technique performed.

Novel formulation like cosine gradient Shapley value (CGSV) to assess the quality/value of model parameter updates/gradients uploaded/contributed by agents in federated learning (FL)/gradient-based collaborative machine learning (CML), guarantees that agents who upload better gradients can also download better gradients, producing better local models with smaller training losses. This approach is effective in terms of fairness and prediction performance. This method is non-restrictive and significantly more effective than existing baselines. Through a hyperparameter that regulates the level of altruism, it offers flexibility for the trade-off between fairly distributed and precisely just rewards. It is interesting to note that a greater altruism degree can occasionally result in superior predictive performance. The future is to apply fairness guarantee and CML work to additional types of cooperative Bayesian optimization. Fed-Coin is a blockchain-based payment system similar to cryptocurrencies [96] that uses the Proof of Shapley (PoSap) like Proof or Work [97] consensus protocol to accurately estimate FL client's Shapley Value-based contributions to the overall FL model, providing an upper bound on the amount of computational power necessary to achieve consensus.

All these systems must be energy-neutral especially if portable devices such as mobile phones or similar devices are involved. No one wants to drain a mobile battery while training a federated learning system. Also, the energy has a high cost, [98]. We see a study that offers a federated learning-based multi-source heterogeneous data fusion method based on Tucker's decomposition theory to reduce privacy and security obstacles, adapt to heterogeneous data types, and reduce network impact. We can also use the convergence rate to derive time and energy consumption models for FL and developed a joint learning and communication problem using these models. In this study presented a low-complexity iterative technique to address this issue, deducing closed-form solutions for the computing and transmission resources. The suggested scheme performs better than traditional schemes in terms of overall energy usage, especially for low maximum average transmit power.

We can look also how each participating device in federated learning allocates bandwidth, controls transmission power, and changes CPU frequency. The introduction of two weight parameters allowed for the optimization of the weighted average of total completion time and energy consumption. This method can increase the flexibility and adaptability of the resource allocation plan to accommodate various FL system requirements. This resource allocation technique advances the state of the art, particularly in cases where the overall completion time is tightly constrained. A framework for sustainable federated learning for devices with intermittent energy availability, offering a straightforward and scalable training technique with verifiable convergence guarantees. It outperforms energy-neutral benchmarks in terms of training performance. Future steps include investigating other energy arrival model options.

An energy-efficient federated scheme to conserve energy from two sides, using wireless resource management and learning parameter allocation. By using sparse rather than typical DNN, energy can be further conserved based on the energy consumption of various learning models. Sparsification and optimization strategy shows a significant impact on energy savings, according to numerical results.

There are already defense methods for Byzantine attack protection in Quantum federated learning. Also, there are Variational Quantum Algorithm’s communication efficient learning from decentralized data, which algorithm can reduce training costs and increase the data privacy offered by quantum technologies due to the outstanding processing speed.

The LFNL technique is a brain-inspired, decentralized, energy-efficient computing approach built on spiking neural networks that allows edge devices to take advantage of brain-like biophysiological structure to jointly train a global model while assisting in private preservation. Experimental findings show that LFNL achieves recognition accuracy similar to that of edge AI methods, while also reducing data traffic and computational latency. Additionally, LFNL greatly lowers energy consumption when compared to traditional federated learning, with a small accuracy loss. LFNL can aid in the advancement of edge AI and computing that is inspired by the human brain.

8 Attacks/ Defenses – Rewards – Energy Efficiency Systems and Possible Combinations

It is quite difficult for sure to have a system that combines all of these characteristics described above. It’s hard to provide protection from attacks by having an integrated system of defenses, to provide rewards during its use, and to be energetically neutral. So, we can make some assumptions depending on its use and the reason it will be used. Of course, this should not cut us off from our goal and be an excuse for any concession of one against the other characteristic that such a system should have.

Federated learning systems as we have seen recently, FL can be a reliable sustainable solution for securing critical infrastructure in IoT systems from the perspective of privacy and property preservation, [99]. Such a system certainly cannot discount security issues and provide protection from attacks. Also, because it is aimed at I.o.T. systems and environments, it should be as energy-neutral as possible. The only assumption that could be made in such a system is that it does not have any reward system, especially for industrial use that uses millions of sensors for monitoring industry procedures, since something like that would probably overburden the I.o.T. system.

Also, as we have seen a federated learning system can offer the maximum in maintaining the privacy of medical data. Medical data such as patient X-rays, drug combinations, and biochemical test results are perhaps among the most promising are-as for federated learning, [100]. Such a comprehensive system solely because it addresses medical data must provide maximum security and defense and provide some reward system to incentivize participants to provide their data. If it is not possible to have a reward system, surely there cannot be a discount for security issues. Maintaining confidentiality of data records is of paramount importance. As far as the energy part is concerned, such systems are usually addressed to hospitals, pharmaceutical industries, or medical device companies that can certainly afford the energy cost of such a system.

Furthermore, federated learning has been shown to be particularly efficient in cloud computing in strong privacy preservation environments, [101]. Cloud computing systems are installed in large data centers that undertake energy management. As we know, the authors here did not deal with energy management and reward but focused only on increasing the security level offered by such a system. The same is true of everyday industrial big data such as federal industrial big data mining learning programs, [102]. A large industry would certainly be able to afford and make discounts on energy cost issues if the system is more efficient in terms of safety. It is no coincidence that most articles addressing industrial systems focus on security and proprietary issues.

Banking [103] and open banking [104] enable both banks and individual customers to own their banking data, collaborative learning provides fundamental support for fostering a new ecosystem of buying and selling data and financial services. Both of these papers focus on the security systems that such a banking system should have. Enchased security provides freedom of movement and further opportunities for growth. Of course, because the reward mechanism is essentially a banking product and is the same as security. Security management goes hand in hand with money management.

There are irregular examples that could be analyzed. Surely any retreat should be made to the one that will have the least impact on a federated learning system. This requires an in-depth examination of the background in each dimension that such a system will be installed and an in-depth analysis of costs and operational benefits.

Table 3 (Appendix) summarizes the extant works and their respective characteristics. The potential values per design element (associated with solution characteristics) are Y if the factor is considered in the relevant work, N if it is not, and "N/S" if it isn't defined or supported.

9 Conclusions and Lessons Learned

Since its presentation as an idea initially in 2016, a federated learning system has definitely matured a lot. Such a system must implement the necessary defenses so as to protect its operation. Depending on the nature of the application and the corresponding requirements, the implementation of strong defense measures may be required. In addition, to attract users there should be a fair reward system. This system would also be good to act as a kind of "cryptocurrency" that would potentially attract financiers who would want to buy it without participating in the data exchange. Let's not forget that, for example, bitcoin can either be mined or bought from an exchange. It can also be compounded as parity with any other cryptocurrency. The only thing that is certain is that the reward - parity, whatever it may be, of the one who participates rightfully in such a system must be considered proportionate and given, otherwise, no one has any reason to participate in this particular system. Complex systems, however, usually burden the end users with energy and money. This should not happen in 2023 where everyone is talking about energy, [105].

With the integration of technologies such as the blockchain, transparency was enhanced, and transparency, cost reduction, and decentralization were achieved. The security and system immutability have been enhanced and made immutable etc. Applications such as smart contracts and cryptocurrencies with the ultimate goal of investigating the multifaceted effects of these technological developments in various aspects of human life such as health, the banking sector, etc. Similarly, other researchers have introduced reward mechanisms based on cryptocurrencies such as Fedcoin or even game-inspired reward methods. Various studies have focused on energy-efficient federated learning over wireless communication networks like iterative algorithms at every step of the model, in order to provide solutions for time allocation, bandwidth allocation, power control mechanism, computation frequency, and learning accuracy. Data fusion methods based on game theory are also proposed as optimization techniques that can be used to solve problems in communication environments like federated learning for resource allocation, power management, rewards, and punishments.

Indeed, many have critiqued the foundations of all these technological approaches, and new models are being developed daily, supporting more inclusive and equitable approaches and innovation. By engaging in critical reflection and interdisciplinary dialogue, new technologies and researchers in this field aim to further advance these new technologies such as quantum-federated learning, and strengthen them even more, [106]. Technologies that in the future would seem alien like Lead federated neuro-morphic learning technique which is brain-inspired or even biocomputers and Organoid Intelligence. All of these approaches not only help to preserve user privacy by keeping sensitive data on the device in the epitome of federated learning but in parallel also enable the creation of more powerful and accurate machine learning and artificial intelligence models in areas beyond existing technology by leveraging diversity of data across different devices and locations and in places we are never been before.

We should always keep in mind that it is difficult to find a complete defense system that provides protection from attack, rewards when used, and does not consume energy. So, we can make some assumptions based on its use and why it is used. Of course, this should allow for any concessions to another feature that such a system might have without derailing us from the goal of a complete federated learning system.

Each federated learning approach has its limitations. These limitations have to do with the nature of this technology and the technology used for the implementation that we want to use at any given time. Thus, there are limitations related to the nature of the data, privacy risk limitations, security issues, scalability, and representativeness of the data.

The limitations of energy management and energy efficiency have to do with the required high initial investments, the technological challenges, the unclear landscape in the energy transformation, and the untargeted energy strategy even at the global and local levels.

When it comes to token-based rewards and payments, there are adoption issues like fees, transaction costs, gas fees like Ethereum Blockchain, laws, and tax issues, and most people aren't used to such systems yet. As for the technology, quantum computers and biocomputers proposed as solutions, the limitations are even more, there are limitations in terms of firmware and hardware, cost and access are limited only to certain organizations that are also early adopters, limited and no algorithms, limited networking and communication capabilities usually at the laboratory level, complexity, and limited control, and there are also major issues of bioethics and biosafety. Federated learning can be made more efficient, more privacy-preserving scalable, and secure by enabling the collective training of models on decentralized data sources while maintaining data privacy and security.

These systems must enhance their robustness to security threats, adversaries, and strategies using privacy-preserving techniques, secure model aggregations, federated learning controls, secure device authentication, watermarking, and targeted model verification.

Federal learning must improve energy management practices. Model training at the local level, Edge Computing integration, Real-time feedback, and control, Data interoperability and standardization, Decentralized energy markets, Resilience and robustness, to optimize resource use and support the transition to more sustainable and resilient energy systems.

Also, federated learning reward systems should provide incentives for active, fair, and transparent reward allocation with dynamic reward adjustments, multi-stakeholder incentives, long-term value allocation, token-based incentive systems, implementation of gamification and social rewards, participation, collaboration, and innovation. Leading to the success and long-term sustainability of federal learning ecosystems.

10 Future Directions and Research

In the future, federated learning can be experienced as a personalized service. Such a service is much needed by users and will have a broad perspective. The Google keyboard constitutes an example of personalized federated learning. Users essentially train a linguistic prediction model that aligns their language habits while ensuring that data is kept locally. Personalization isn’t secure and new security and defense issues can arise. On the other hand, in the context of the Internet of Things, personalized federated learning can better mitigate the impact due to the heterogeneity of user data. The idea of federated transfer learning also contributes to personalization, different users learn again the parameters returned by the global model from their own. But are all the users trustworthy or accurate, [107]. Instead of trying to make technology more energy efficient with non-computational consequences we can use big data and federated learning to generate energy efficiency recommendations. Thus, the technology becomes immediately energy efficient since it is applied on a large scale using other applications as platforms, [108]. Time is money and from the training of a model to even the commercial exploitation of the models takes time, [109]. So, there are serious delays before federated Learning can pay and it is really a question if it is capable of repaying the participants. This temporary mismatch between contributions and rewards has not been accounted for and quantified by existing profit-sharing systems. This is definitely one of the issues that needs to be resolved in the future.

Federated Learning is an opportunity for collaboration. The possibilities are practically and essentially unlimited. From the construction of the model, the data production the data extraction, and the technology that is required to implement it. To understand the possibilities of such a collaboration we can see the companies and organizations that can be involved. Between organizations, the goal is to provide each participant with a federated model that performs better than their best local model. In this way, even a global model can be created for the union of all their data, without privacy or scalability problems, [110]. The contribution of this study ις while most of the other studies are based on studying only defensive attack mechanisms that threaten associative learning without a reward mechanism for it and the participants. Also, in a world where energy is money, you cannot have such a system that consumes more (money and resources) than it produces. All of these studies were used as a problem base for us initially and were very helpful for us. In the present paper a more holistic approach to the problem is taken and this is the basis for our concern and that of the readers. We know initially that such work is very difficult. Especially for federated learning systems very holistic approaches are required. One of these is blockchain technology but is not enough. They are certainly very difficult to exist and certainly depend on the applications they will have. Somewhere discounts will be needed where we analyze this in a chapter which can also give food for thought. In order to give more value to our holistic approach as well as to the concerns of future research or to the general reader, we have incorporated technologies such as quantum with the ability to solve and analyze complex strings at unimaginable speeds and also the technology of bio-brains that is actually now emerging. In the current literature, there is virtually no term "Brain Organoid-Based Federated Learning" that connects this federated learning technology to biological molecules that exploit their unique advantages, which is useful for us in this work and as a basis for thinking about others and research.

References:

[1] Khan, L. U., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2020). 6G wireless systems: A vision, architectural elements, and future directions. *IEEE Access*, 8, 147029-147044, https://doi.org/10.1109/ACCESS.2020.3015289.

[2] Statista, R. D. (2019). *Internet of things-number of connected devices worldwide 2015-2025*. Statista Research Department.

statista.com, [Online]. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Accessed Date: September 18, 2023).

[3] Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, 8(16), 12806-12825, https://doi.org/10.1109/JIOT.2021.3072611.

[4] Huang, C., Huang, J., & Liu, X. (2022). *Cross-silo federated learning: Challenges and opportunities*. arXiv preprint arXiv:2206.12949.

[5] Mell, P., Scarfone, K., & Romanosky, S. (2007, June). A complete guide to the common vulnerability scoring system version 2.0. In Published by *FIRST-forum of incident response and security teams* (Vol. 1, p. 23).

[6] Mishra, B., Jena, D., & Patnaik, S. (2023). Fine-grained access control of files stored in cloud storage with traceable and revocable multi-authority CP-ABE scheme. *International Journal of Grid and Utility Computing*, 14(4), 320-338, https://doi.org/10.1504/ijguc.2023.132615.

[7] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on risk and insurance-Issues and practice*, 47(3), 698-736.

[8] National Research Council, Division on Engineering, Physical Sciences, Computer Science, Telecommunications Board, Commission on Physical Sciences, Mathematics, Applications and System Security Study Committee, 1990. Computers at risk: safe computing in the information age. *National Academies Press*.

[9] Liu, Ji, Jizhou Huang, Yang Zhou, Xuhong Li, Shilei Ji, Haoyi Xiong, and Dejing Dou. "From distributed machine learning to federated learning: A survey." Knowledge and Information Systems 64, no. 4 (2022), 885-917, https://doi.org/10.48550/arXiv.2104.14362.

[10] Fang, M., Cao, X., Jia, J., & Gong, N. (2020). Local model poisoning attacks to {Byzantine-Robust} federated learning. In *29th USENIX security symposium (USENIX Security 20)* (pp. 1605-1622).

[11] Zhu, J., Cao, J., Saxena, D., Jiang, S., & Ferradi, H. (2023). Blockchain-empowered federated learning: Challenges, solutions, and future directions. *ACM Computing Surveys*, 55(11), 1-31, https://doi.org/10.1145/3570953.

[12] Kumar, Yogesh, and Ruchi Singla. "Federated learning systems for healthcare: perspective and recent progress." *Federated Learning Systems: Towards Next-Generation AI* (2021): 141-156.

[13] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H.R., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B.A., Maier-Hein, K. and Ourselin, S., 2020. *The future of digital health with federated learning. NPJ digital medicine*, 3(1), pp.1-7, https://doi.org/10.1038/s41746-020-00323-1.

[14] Burkacky, O., Goke, S., Nikolka, M., Patel, M., & Spiller, P. (2022). Sustainability in semiconductor operations: Toward net-zero production. McKinsey & Co, [Online]. https://www.mckinsey.com/industries/semiconductors/our-insights/sustainability-in-semiconductor-operations-toward-net-zero-production (Accessed Date: August 5, 2023).

[15] Way, Rupert, Penny Mealy, and J. Doyne Farmer. *Estimating the costs of energy transition scenarios using probabilistic forecasting methods*. No. 2021-01. INET Oxford Working Paper, 2020.

[16] Lee, Joohyung, Daejin Kim, and Dusit Niyato. "A novel joint dataset and incentive management mechanism for federated learning over MEC." IEEE Access 10 (2022): 30026-30038, https://doi.org/10.1109/ACCESS.2022.3156045.

[17] Lim, Wei Yang Bryan, Jer Shyuan Ng, Zehui Xiong, Jiangming Jin, Yang Zhang, Dusit Niyato, Cyril Leung, and Chunyan Miao. "Decentralized edge intelligence: A dynamic resource allocation framework for hierarchical federated learning." *IEEE Transactions on Parallel and Distributed Systems*, 33, no. 3 (2021): 536-550, https://doi.org/10.1109/TPDS.2021.3096076.

[18] Espinosa, J. Alberto, and Frank Armour. "The big data analytics gold rush: a research framework for coordination and governance." *In 2016 49th Hawaii International Conference on System*

Sciences (HICSS), pp. 1112-1121. IEEE, 2016, https://doi.org/10.1109/HICSS.2016.141.

[19] Desharnais, G., J. P. Paiement, D. Hatfield, and N. Poupart. "Mining BIG data: The future of exploration targeting using machine learning." *In Proceedings of Exploration 17: Sixth Decennial International Conference on Mineral Exploration*, vol. 2017, pp. 319-323. 2017.

[20] Chen, Mingzhe, Zhaohui Yang, Walid Saad, Changchuan Yin, H. Vincent Poor, and Shuguang Cui. "A joint learning and communications framework for federated learning over wireless networks." *IEEE Transactions on Wireless Communications* 20, no. 1 (2020): 269-283, https://doi.org/10.1109/TWC.2020.3024629

[21] United Nations. "Inequality in a rapidly changing world." Chapter 3: Climate Change: Excacerbating Poverty and Inequality. (2020), [Online]. https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/02/World-Social-Report2020-FullReport.pdf (Accessed Date: August 15, 2023).

[22] Revinova, S., and DP Chavarry Galvez. "E-government and government support for the digital economy in Latin America and the Caribbean." In *2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)*, pp. 1003-1011. Atlantis Press, 2020.

[23] Song, Tianshu, Yongxin Tong, and Shuyue Wei. "Profit allocation for federated learning." In *2019 IEEE International Conference on Big Data (Big Data)*, pp. 2577-2586. IEEE, 2019.

[24] Stamenkov, Gjoko. "Genealogy of the fair information practice principles." *International Journal of Law and Management*, 65, no. 3 (2023): 242 - 260, https://doi.org/10.1108/IJLMA-07-2022-0149.

[25] Siddi, Marco. "Coping with turbulence: EU negotiations on the 2030 and 2050 climate targets." *Politics and Governance*, 9, no. 3 (2021):327-336, https://doi.org/10.17645/pag.v9i3.4267.

[26] Yang, Qiang, Lixin Fan, Richard Tong, and Angelica Lv. "White paper-IEEE federated machine learning." *IEEE Federated Machine Learning-White Paper (2021)*: 1-18.

[27] Cheu, Albert, Adam Smith, and Jonathan Ullman. "Manipulation attacks in local differential privacy." In *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 883-900. IEEE, 2021.

[28] Akujuobi, Uchenna, Han Yufei, Qiannan Zhang, and Xiangliang Zhang. "Collaborative graph walk for semi-supervised multi-label node classification." In *2019 IEEE International Conference on Data Mining (ICDM)*, pp. 1-10. IEEE, 2019.

[29] Fang, Pei, and Jinghui Chen. "On the vulnerability of backdoor defenses for federated learning." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 10, pp. 11800-11808. 2023, https://doi.org/10.48550/arXiv.2301.08170.

[30] Ozdayi, Mustafa Safa, Murat Kantarcioglu, and Yulia R. Gel. "Defending against backdoors in federated learning with robust learning rate." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, no. 10, pp. 9268-9276. 2021.

[31] Rodríguez-Barroso, Nuria, Eugenio Martínez-Cámara, M. Victoria Luzón, and Francisco Herrera. "Backdoor attacks-resilient aggregation based on Robust Filtering of Outliers in federated learning for image classification." *Knowledge-Based Systems*, 245 (2022), 108588, https://doi.org/10.1016/j.knosys.2022.108588.

[32] Manoj, Naren, and Avrim Blum. "Excess capacity and backdoor poisoning." *Advances in Neural Information Processing Systems*, 34 (2021): 20373-20384.

[33] Titcombe, Tom, Adam J. Hall, Pavlos Papadopoulos, and Daniele Romanini. "*Practical defences against model inversion attacks for split neural networks*." arXiv preprint arXiv:2104.05743 (2021), https://doi.org/10.48550/arXiv.2104.05743.

[34] Wu, Jing, Munawar Hayat, Mingyi Zhou, and Mehrtash Harandi. "*Defense against privacy leakage in federated learning*." arXiv preprint arXiv:2209.05724 (2022), https://doi.org/10.48550/arXiv.2209.05724.

[35] Wang, Kuan-Chieh, Yan Fu, Ke Li, Ashish Khisti, Richard Zemel, and Alireza Makhzani. "Variational model inversion attacks." *Advances in Neural Information Processing Systems*, 34 (2021): 9706-9719.

[36] Abdellatif, Alaa Awad, Naram Mhaisen, Amr Mohamed, Aiman Erbad, Mohsen Guizani, Zaher Dawy, and Wassim Nasreddine. "Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data." *Future Generation Computer Systems*, 128 (2022): 406-419, https://doi.org/10.1016/j.future.2021.10.016

[37] Zhao, Ying, Junjun Chen, Jiale Zhang, Di Wu, Jian Teng, and Shui Yu. "PDGAN: A novel poisoning defense method in federated learning using generative adversarial network." In *Algorithms and Architectures for Parallel Processing: 19th International Conference, ICA3PP 2019*, Melbourne, VIC, Australia, December 9–11, 2019, Proceedings, Part I 19, pp. 595-609. Springer International Publishing, 2020.

[38] Mothukuri, Viraaji, Prachi Khare, Reza M. Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, and Gautam Srivastava. "Federated-learning-based anomaly detection for IoT security attacks." *IEEE Internet of Things Journal*, 9, no. 4 (2021): 2545-2554, https://doi.org/10.1109/JIOT.2021.3077803.

[39] Lewis, Cody, Vijay Varadharajan, and Nasimul Noman. "Attacks against federated learning defense systems and their mitigation." *Journal of Machine Learning Research*, 24, no. 30 (2023): 1-50.

[40] Xie, Chulin, Keli Huang, Pin-Yu Chen, and Bo Li. "Dba: Distributed backdoor attacks against federated learning." *In International conference on learning representations*. 2019.

[41] Lavond, Joseph, Minhao Cheng, and Yao Li. "*Trusted Aggregation (TAG): Model Filtering Backdoor Defense In Federated Learning*." (2022).

[42] Lin, Jierui, Min Du, and Jian Liu. "*Free-riders in federated learning: Attacks and defenses*." arXiv preprint arXiv:1911.12560 (2019), https://doi.org/10.48550/arXiv.1911.12560.

[43] Chen, Jinyin, Mingjun Li, Tao Liu, Haibin Zheng, Hang Du, and Yao Cheng. "Rethinking the defense against free-rider attack from the perspective of model weight evolving frequency." *Information Sciences* (2024): 120527, https://doi.org/10.48550/arXiv.2206.05406.

[44] Wei, Wenqi, Ling Liu, Margaret Loper, Ka-Ho Chow, Mehmet Emre Gursoy, Stacey Truex, and Yanzhao Wu. "*A framework for evaluating gradient leakage attacks in federated learning*." arXiv preprint arXiv:2004.10397 (2020), https://doi.org/10.48550/arXiv.2004.10397.

[45] Tolomei, Gabriele, Edoardo Gabrielli, Dimitri Belli, and Vittorio Miori. "*A Byzantine-Resilient Aggregation Scheme for Federated Learning via Matrix Autoregression on Client Updates*." arXiv preprint arXiv:2303.16668 (2023), https://doi.org/10.48550/arXiv.2303.16668.

[46] Roushdy Elkordy, Ahmed, Saurav Prakash, and A. Salman Avestimehr. "*Basil: A Fast and Byzantine-Resilient Approach for Decentralized Training*." arXiv e-prints (2021): arXiv-2109.

[47] Wainakh, Aidmar, Ephraim Zimmer, Sandeep Subedi, Jens Keim, Tim Grube, Shankar Karuppayah, Alejandro Sanchez Guinea, and Max Mühlhäuser. "Federated learning attacks revisited: A critical discussion of gaps, assumptions, and evaluation setups." *Sensors*, 23, no. 1 (2022), 31, https://doi.org/10.3390/s23010031.

[48] Fang, Minghong, Xiaoyu Cao, Jinyuan Jia, and Neil Gong. "Local model poisoning attacks to {Byzantine-Robust} federated learning." In *29th USENIX security symposium (USENIX Security 20)*, pp. 1605-1622. 2020.

[49] Li, Xingyu, Zhe Qu, Shangqing Zhao, Bo Tang, Zhuo Lu, and Yao Liu. "Lomar: A local defense against poisoning attack on federated learning." *IEEE Transactions on Dependable and Secure Computing*, 20, no. 1 (2021): 437-450.

[50] Shi, Junyu, Wei Wan, Shengshan Hu, Jianrong Lu, and Leo Yu Zhang. "Challenges and approaches for mitigating byzantine attacks in federated learning." In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 139-146. IEEE, 2022.

[51] Ma, Chuan, Jun Li, Long Shi, Ming Ding, Taotao Wang, Zhu Han, and H. Vincent Poor. "When federated learning meets blockchain: A new distributed learning paradigm." *IEEE Computational Intelligence Magazine*, 17, no. 3 (2022): 26-

33, https://doi.org/10.1109/MCI.2022.3180932.

[52] Lee, Woonghee. "Reward-based participant selection for improving federated reinforcement learning." *ICT Express*, 9, no. 5 (2023): 803-808, http://doi.org/10.1016/j.icte.2022.08.008.

[53] Pandl, Konstantin D., Florian Leiser, Scott Thiebes, and Ali Sunyaev. "*Reward Systems for Trustworthy Medical Federated Learning*." arXiv preprint arXiv:2205.00470 (2022), https://doi.org/10.48550/arXiv.2205.00470.

[54] Jiang, Suhan, and Jie Wu. "A reward response game in the blockchain-powered federated learning system." *International Journal of Parallel, Emergent and Distributed Systems*, 37, no. 1 (2022): 68-90.

[55] Computing, Ph D–Human-Centered, and Sc B. Neuroscience. "*Evan Barba*." PhD diss., Georgia Institute of Technology, 2008.

[56] Martinez, Ismael, Sreya Francis, and Abdelhakim Senhaji Hafid. "Record and reward federated learning contributions with blockchain." In *2019 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*, pp. 50-57. IEEE, 2019, https://doi.org/10.1109/CyberC.2019.00018.

[57] Duy, Trần Quang, and Minh Hoang Trong. "A blockchain-based Certificate Management System using the Hyperledger Fabric Platform." *Thang Long Journal of Science: Mathematics and Mathematical Sciences*, 2, no. 8 (2023).

[58] Xu, Xinyi, Lingjuan Lyu, Xingjun Ma, Chenglin Miao, Chuan Sheng Foo, and Bryan Kian Hsiang Low. "Gradient driven rewards to guarantee fairness in collaborative machine learning." *Advances in Neural Information Processing Systems*, 34 (2021): 16104-16117.

[59] Nguyen, Quoc Phong, Bryan Kian Hsiang Low, and Patrick Jaillet. "Trade-off between payoff and model rewards in Shapley-fair collaborative machine learning." *Advances in Neural Information Processing Systems*, 35 (2022): 30542-30553.

[60] Sim, Rachael Hwee Ling, Yehong Zhang, Bryan Kian Hsiang Low, and Patrick Jaillet. "Collaborative Bayesian optimization with fair regret." In *International Conference on Machine Learning*, pp. 9691-9701. PMLR, 2021.

[61] Han, Jingoo, Ahmad Faraz Khan, Syed Zawad, Ali Anwar, Nathalie Baracaldo Angel, Yi Zhou, Feng Yan, and Ali R. Butt. "Tiff: Tokenized incentive for federated learning." In 2022 *IEEE 15th International Conference on Cloud Computing (CLOUD)*, pp. 407-416. IEEE, 2022.

[62] Pandey, Shashi Raj, Lam Duc Nguyen, and Petar Popovski. "*Fedtoken: Tokenized incentives for data contribution in federated learning*." arXiv preprint arXiv:2209.09775 (2022), https://doi.org/10.48550/arXiv.2209.09775.

[63] Liu, Yuan, Zhengpeng Ai, Shuai Sun, Shuangfeng Zhang, Zelei Liu, and Han Yu. "Fedcoin: A peer-to-peer payment system for federated learning." In *Federated learning: privacy and incentive*, pp. 125-138. Cham: Springer International Publishing, 2020.

[64] Pandl, Konstantin D., Florian Leiser, Scott Thiebes, and Ali Sunyaev. *"Reward Systems for Trustworthy Medical Federated Learning*." arXiv preprint arXiv:2205.00470 (2022).

[65] Stauffer, Nancy W., MIT Energy Initiative, and MIT Energy Initiative. "Energy futures." *MIT Energy Initiative Magazine*, (2012): 5-7.

[66] Soni, Mukesh, Nihar Ranjan Nayak, Ashima Kalra, Sheshang Degadwala, Nikhil Kumar Singh, and Shweta Singh. "Energy efficient multi-tasking for edge computing using federated learning." *International Journal of Pervasive Computing and Communications* (2022). Article publication date: 8 July 2022.

[67] Yang, Zhaohui, Mingzhe Chen, Walid Saad, Choong Seon Hong, and Mohammad Shikh-Bahaei. "Energy efficient federated learning over wireless communication networks." *IEEE Transactions on Wireless Communications*, 20, no. 3 (2020): 1935-1949.

[68] Zhou, Xinyu, Jun Zhao, Huimei Han, and Claude Guet. "Joint optimization of energy consumption and completion time in federated learning." In *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*, pp. 1005-1017. IEEE, 2022.

[69] Guler, Basak, and Aylin Yener. "*Sustainable federated learning*." arXiv preprint arXiv:2102.11274 (2021).

[70] Shi, Dian, Liang Li, Rui Chen, Pavana Prakash, Miao Pan, and Yuguang Fang. "Toward energy-efficient federated learning over 5g+ mobile devices." *IEEE Wireless Communications*, 29, no. 5 (2022): 44-51.

[71] Kim, Minsu, Walid Saad, Mohammad Mozaffari, and Merouane Debbah. "Green, quantized federated learning over wireless networks: An energy-efficient design." *IEEE Transactions on Wireless Communications*, (2023).

[72] Xia, Qi, Zeyi Tao, and Qun Li. "Defending against byzantine attacks in quantum federated learning." In *2021 17th International Conference on Mobility, Sensing and Networking (MSN)*, pp. 145-152. IEEE, 2021.

[73] Computing, Green Quantum, and Milou van Nederveen. "*Green Quantum Computing*.", [Online]. https://www.publicnow.com/view/5B728240130A3F2069241CBAB82FC50277011F65?1683553541 (Accessed Date: July 1, 2023)

[74] Chen, Sophia. "Are quantum computers really energy efficient?." *Nature Computational Science*, 3, no. 6 (2023), 457-460, https://doi.org/10.1038/s43588-023-00459-6.

[75] Huang, Rui, Xiaoqing Tan, and Qingshan Xu. "Quantum federated learning with decentralized data." *IEEE Journal of Selected Topics in Quantum Electronics 28, no. 4: Mach. Learn. in Photon. Commun. and Meas. Syst.* (2022): 1-10, http://dx.doi.org/10.1109/JSTQE.2022.3170150.

[76] Yen-Chi Chen, Samuel, and Shinjae Yoo. "*Federated Quantum Machine Learning*." arXiv e-prints (2021): arXiv-2103, https://doi.org/10.3390/e23040460.

[77] Smith, Mark. "*Quantum computing: Definition, facts & uses*." Live Science, livescience. com (2022).

[78] Balasubramanian, Vijay. "Brain power." *Proceedings of the National Academy of Sciences*, 118, no. 32 (2021): e2107022118.

[79] Dolan, Peter. "The Future Possibility of Consumer-Grade Quantum Computers." *Missouri S&T's Peer to Peer*, 2, no. 1 (2018): 6, [Online]. https://scholarsmine.mst.edu/peer2peer/vol2/iss1/6 (Accessed Date: July 28, 2023).

[80] Golestan, Saeed, M. R. Habibi, SY Mousazadeh Mousavi, Josep M. Guerrero, and Juan C. Vasquez. "Quantum computation in power systems: An overview of recent advances." *Energy Reports*, 9 (2023): 584-596, http://dx.doi.org/10.1016/j.egyr.2022.11.185.

[81] Kujala, Tuomo, and Otto Lappi. "Inattention and uncertainty in the predictive brain." *Frontiers in Neuroergonomics*, 2 (2021): 718699.

[82] Züfle, Andreas, Tobias Emrich, Klaus Arthur Schmid, Nikos Mamoulis, Arthur Zimek, and Matthias Renz. "Representative clustering of uncertain data." In *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 243-252. 2014.

[83] Sigman, Mariano, and Stanislas Dehaene. "Brain mechanisms of serial and parallel processing during dual-task performance." *Journal of Neuroscience*, 28, no. 30 (2008), 7585-7598, https://doi.org/10.1523/JNEUROSCI.0948-08.20.

[84] Breckels, Lisa M., Sean B. Holden, David Wojnar, Claire M. Mulvey, Andy Christoforou, Arnoud Groen, Matthew WB Trotter, Oliver Kohlbacher, Kathryn S. Lilley, and Laurent Gatto. "Learning from heterogeneous data sources: an application in spatial proteomics." *PLoS computational biology*, 12, no. 5 (2016): e1004920, https://doi.org/10.1371/journal.pcbi.1004920.

[85] Khan, Latif U., Walid Saad, Zhu Han, Ekram Hossain, and Choong Seon Hong. "Federated learning for internet of things: Recent advances, taxonomy, and open challenges." *IEEE Communications Surveys & Tutorials*, 23, no. 3 (2021): 1759-1799, http://dx.doi.org/10.1109/COMST.2021.3090430.

[86] Da Rocha, Armando Freitas, Fábio Theoto Rocha, and Eduardo Massad. "The brain as a distributed intelligent processing system: an EEG study." *PLoS One*, 6, no. 3 (2011), e17355, https://doi.org/10.1371/journal.pone.0017355.

[87] Lewis, Robert G., Ermanno Florio, Daniela Punzo, and Emiliana Borrelli. The Brain's reward system in health and disease. *Springer International Publishing*, 2021, http://dx.doi.org/10.1007/978-3-030-81147-1_4.

[88] Smirnova, Lena, Brian S. Caffo, David H. Gracias, Qi Huang, Itzy E. Morales Pantoja, Bohao Tang, Donald J. Zack et al. "Organoid intelligence (OI): the new frontier in biocomputing and intelligence-in-a-dish." *Frontiers in Science*, 1 (2023): 1017235, http://dx.doi.org/10.3389/fsci.2023.1017235

[89] Yang, Helin, Kwok-Yan Lam, Liang Xiao, Zehui Xiong, Hao Hu, Dusit Niyato, and H. Vincent Poor. "Lead federated neuromorphic learning for wireless edge artificial intelligence." *Nature communications*, 13, no. 1 (2022): 4269, https://doi.org/10.1038/s41467-022-32020-w.

[90] Capatina, Laura, Alexandra Cernian, and Mihnea Alexandru Moisescu. "Efficient training models of Spiking Neural Networks deployed on a neuromorphic computing architectures." In *2023 24th International Conference on Control Systems and Computer Science (CSCS)*, pp. 383-390. IEEE, 2023.

[91] Quirion R, (2023) Brain organoids: are they for real? *Frontiers in Science*, 1, 1148127, http://dx.doi.org/10.3389/fsci.2023.1148127

[92] Morales Pantoja, Itzy E., Lena Smirnova, Alysson R. Muotri, Karl J. Wahlin, Jeffrey Kahn, J. Lomax Boyd, David H. Gracias et al. "First Organoid Intelligence (OI) workshop to form an OI community." *Frontiers in Artificial Intelligence*, 6 (2023), 1116870, http://dx.doi.org/10.3389/fsci.2023.1148127

[93] Cai, Hongwei, Zheng Ao, Chunhui Tian, Zhuhao Wu, Hongcheng Liu, Jason Tchieu, Mingxia Gu, Ken Mackie, and Feng Guo. "Brain organoid reservoir computing for artificial intelligence." *Nature Electronics*, 6, no. 12 (2023): 1032-1039.

[94] Rajagopal, Shinu M., M. Supriya, and Rajkumar Buyya. "FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated Edge-Fog-Cloud computing environments." *Internet of Things*, (2023): 100784, http://dx.doi.org/10.1016/j.iot.2023.100784.

[95] Lu, Yunlong, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks." *IEEE Transactions on Industrial Informatics*, 17, no. 7 (2020): 5098-5107, http://dx.doi.org/10.1109/TII.2020.3017668.

[96] Lianos, Ioannis, Philipp Hacker, Stefan Eich, and Georgios Dimitropoulos, eds. Regulating blockchain: techno-social and legal challenges. *Oxford University Press*, 2019.

[97] Porat, Amitai, Avneesh Pratap, Parth Shah, and Vinit Adkar. "*Blockchain Consensus: An analysis of Proof-of-Work and its applications.*" (2017), Corpus ID: 32100244.

[98] Laport-López, Francisco, Emilio Serrano, Javier Bajo, and Andrew T. Campbell. "A review of mobile sensing systems, applications, and opportunities." *Knowledge and Information Systems*, 62, no. 1 (2020): 145-174, https://link.springer.com/article/10.1007/s10115-019-01346-1 (Accessed Date: September 19, 2023).

[99] Ghimire, Bimal, and Danda B. Rawat. "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things." *IEEE Internet of Things Journal*, 9, no. 11 (2022), 8229-8249, https://doi.org/10.1109/JIOT.2022.3150363.

[100] Singh, Saurabh, Shailendra Rathore, Osama Alfarraj, Amr Tolba, and Byungun Yoon. "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology." *Future Generation Computer Systems*, 129 (2022), 380-388, https://doi.org/10.1016/j.future.2021.11.028

[101] Fang, Chen, Yuanbo Guo, Na Wang, and Ankang Ju. "Highly efficient federated learning with strong privacy preservation in cloud computing." *Computers & Security*, 96 (2020): 101889, http://dx.doi.org/10.1016/j.cose.2020.101889.

[102] Zhao, Bin, Kai Fan, Kan Yang, Zilong Wang, Hui Li, and Yintang Yang. "Anonymous and privacy-preserving federated learning with industrial big data." *IEEE Transactions on Industrial Informatics*, 17, no. 9 (2021): 6314-6323, https://doi.org/10.1109/TII.2021.3052183.

[103] Chatterjee, Pushpita, Debashis Das, and Danda B. Rawat. "*Use of federated learning and blockchain towards securing financial services.*" arXiv preprint arXiv:2303.12944

(2023), https://doi.org/10.48550/arXiv.2303.12944.

[104] Long, Guodong, Yue Tan, Jing Jiang, and Chengqi Zhang. "Federated learning for open banking." In *Federated Learning: Privacy and Incentive*, pp. 240-254. Cham: Springer International Publishing, 2020.

[105] Schmidt, John, and F. Powell. "Why Does Bitcoin Use So Much Energy." *Forbes Advisor* (2022), [Online]. https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/ (Accessed Date: September 10, 2023)

[106] Kiktenko, Evgeniy O., Nikolay O. Pozhar, Maxim N. Anufriev, Anton S. Trushechkin, Ruslan R. Yunusov, Yuri V. Kurochkin, A. I. Lvovsky, and Aleksey K. Fedorov. "Quantum-secured blockchain." *Quantum Science and Technology*, 3, no. 3 (2018): 035004.

[107] Zhang, Kaiyue, Xuan Song, Chenhan Zhang, and Shui Yu. "Challenges and future directions of secure federated learning: a survey." F*rontiers of computer science*, 16 (2022): 1-8.

[108] Varlamis, Iraklis, Christos Sardianos, Christos Chronis, George Dimitrakopoulos, Yassine Himeur, Abdullah Alsalemi, Faycal Bensaali, and Abbes Amira. "Using big data and federated learning for generating energy efficiency recommendations." *International Journal of Data Science and Analytics*, 16, no. 3 (2023): 353-369.

[109] Yu, Han, Zelei Liu, Yang Liu, Tianjian Chen, Mingshu Cong, Xi Weng, Dusit Niyato, and Qiang Yang. "A sustainable incentive scheme for federated learning." *IEEE Intelligent Systems*, 35, no. 4 (2020): 58-69.

[110] d'Hondt, T. (2020). *Federated learning over local learning: an opportunity for collaboration* (Doctoral dissertation, Master's thesis, Eindhoven University of Technology). (Accessed 10 October 2023)

Glossary

Term	Definition
BLADE-FL	Blockchain Assisted Decentralized Federated Learning
CCPA	California Consumer Privacy Act
CGSV	Cosine Gradient Shapley Value
CML	Collaborative Machine Learning
CSVES	Class-Sampled Validation Error Scheme
DBA	Distributed Backdoor Attack
DNN	Deep Neural Network
F3BA	Focused-Flip Federated Backdoor Attack
FABA	Fast Aggregation against Byzantine Attacks
Fed-Coin,	A blockchain-based payment system to support federated learning procedure
GDPR	General Data Protection Regulation
LFNL	Lead Federated Neuromorphic Learning
Lo-Mar	Local Malicious Factor
NFTs	Non-Fungible Tokens
O.I.	Organoid Intelligence
MEA chip	Microelectrode arrays (MEAs) are devices that contain multiple (tens to thousands) microelectrodes through which neural signals are obtained or delivered for in vitro studies.
P.o.A.	Price of Anarchy
P.o.W.	Proof of Work
PDGAN	Phishing Detection with Generative Adversarial Networks
PoSap	Proof of Shapley
QFL	Quantum Federated Learning
R.L.R.	Robust Learning Rate
RFOut-1d	Robust Filtering of one-dimensional Outliers
S.V.	Shapley Value
VQA	Variational Quantum Algorithm
WEF-Defence	Weight Evolving Frequency model

APPENDIX

Table 3. Design elements implemented in each work, [29], [30], [31], [33], [34], [36], [37], [38], [39], [42], [44], [48], [51], [52], [53], [54], [55], [56], [58], [59], [61], [62], [63], [66], [67], [68], [69], [70], [71], [72], [75], [88], [89]

Design Elements/ Ref Title	Attacks	Defenses	Rewards	Energy Efficiency
[29] On the Vulnerability of Backdoor Defenses for Federated Learning	Y (Backdoor Attacks)	Y (Various defense measures)	N	N
[33] Practical defenses against model inversion attacks for split neural networks	Y (Model inversion attack)	Y (Simple additive noise method)	N	N
[34] Defense against Privacy Leakage in Federated Learning	Y (Stronger attacks and exhibit a poor trade-off)	Y (Defence strategy based on obfuscating the gradients)	N	N
[30] Defending against backdoors in federated learning with a robust learning rate	Y (Backdoor Attacks)	Y (Carefully adjusting the aggregation server's learning rate)	N	N
[36] Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data.	Y (Imbalanced Data)	Y (Optimized solution for user assignment and resource allocation on multiple edge nodes)	N	Y (Reduce communication overhead)
[37] PDGAN: A novel poisoning defense method in federated learning using the generative adversarial network.	N (Poisoning attacks by uploading malicious updates)	Y (Novel poisoning defense generative adversarial network)	N	N
[38] Federated-learning-based anomaly detection for IoT security attacks.	Y (Federated-learning (FL)-based anomaly detection approach to proactively)	Y (Recognise intrusion in IoT networks using decentralized on-device data)	N	N
[51] When federated learning meets blockchain: A new distributed learning paradigm.	Y (Single central server falls apart & server behaves maliciously)	Y (Blockchain-assisted decentralized FL (BLADE-FL) framework)	N/S	N
[31] Backdoor attacks-resilient aggregation based on Robust Filtering of Outliers in federated learning for image classification.	Y (Model-poisoning backdoor attacks)	Y (Robust Filtering of one-dimensional Outliers (RFOut-1d), a resilient defensive mechanism)	N	N
[39] Attacks against federated learning defense systems and their mitigation.	Y (On-off attacks, label flipping, and free riding)	Y (Mitigation strategy)	N	N
[42] Free-riders in federated learning: Attacks and defenses	Y (Free rider attacks)	Y (New high dimensional detection method)	N	N
[44] A framework for evaluating gradient leakage attacks in federated learning.	Y (Gradient leakage attacks)	Y (Preliminary mitigation strategies)	N	N
[48] Local model poisoning attacks to {Byzantine-Robust} federated learning.	Y (Byzantine failures e.g., system failures, adversarial manipulations)	Y (Two defenses generalization)	N	N
[52] Reward-based participant selection for improving federated reinforcement learning.	N	N	Y (Reward-based participant selection for improving federated reinforcement learning)	N/S
[53] Reward Systems for Trustworthy Medical Federated Learning.	N	N	Y (An integrated reward system successfully incentivizes contributions toward a well-performing model with low bias)	N/S

Design Elements/ Ref Title	Attacks	Defenses	Rewards	Energy Efficiency
[54] A reward response game in the blockchain-powered federated learning system	N	N	Y (An accurate model by paying them based on their individual contributions)	N
[56] Record and reward federated learning contributions with blockchain.	N/S	N/S	Y (A novel validation error-based metric upon which we qualify gradientuploads for paymet)	N
[58] Gradient-driven rewards to guarantee fairness in collaborative machine learning.	N	N	Y (A novel cosine gradient Shapley value (CGSV) to fairly evaluate the expected marginal contribution)	N/S
[61] Tiff: Tokenized incentive for federated learning.	N	N	Y (TIFF, a novel tokenized incentive mechanism, where tokens are used as a means of paying)	N/S
[62] Fedtoken: Tokenized incentives for data contribution in federated learning.	N	N	Y (A contribution-based tokenized incentive scheme, namely FedToken)	N
[59] The trade-off between payoff and model rewards in Shapley-fair collaborative machine learning	N	N	Y (An allocation scheme that distributes the payoff fairly)	N/S
[63] Fedcoin: A peer-to-peer payment system for federated learning. In Federated learning: privacy and incentive	N	N	Y (FedCoin, a blockchain-based peer-to-peer payment system for FL to enable a feasible SV based profit distribution)	N
[66] Energy-efficient multi-tasking for edge computing using federated learning	N/S	N/S	N	Y (Improvement of the existing edge computing to maintain a balanced energy usage)
[67] Energy efficient federated learning over wireless communication networks.	N	N	N	Y (An iterative algorithm solution for time allocation, bandwidth allocation, power control, computation frequency, and learning accuracy are derived)
[68] Joint optimization of energy consumption and completion time in federated learning.	N	N	N	Y (A resource allocation algorithm CPU, frequency, for each participating device)
[69] A framework for sustainable federated learning.	N	N	N	Y a practical framework that utilizes intermittent energy arrivals for training
[70] Toward energy-efficient federated learning over 5g+ mobile devices..	N	N	N	Y (Energy-efficient learning techniques (gradient scarification, weight quantization, pruning, etc).
[71] Green, quantized federated learning over wireless networks: An energy-efficient design.	N	N	N	Y (Pareto boundary using the normal boundary inspection method)
[72] Defending against byzantine attacks in quantum federated learning.	Y (Byzantine attacks)	Y (Emulated experiments to show a similar performance of the quantum version with the classic version)	N	N/S
[75] Quantum federated learning with decentralized data.	Y (Improvement data privacy by aggregating updates from local	Y (Improvement data privacy by aggregating updates from local	N/S	Y (Communication-efficient learning of VQA from decentralized data)

Design Elements/ Ref Title	Attacks	Defenses	Rewards	Energy Efficiency
	computation to share model parameters)	computation to share model parameters)		
[89] Lead federated neuromorphic learning for wireless edge artificial intelligence.	Y (Enable edge devices to exploit brain-like biophysiological structure to collaboratively train a global model)	Y (Enable edge devices to exploit brain-like biophysiological structure to collaboratively train a global model)	N	Y (A lead federated neuromorphic learning technique)
[88] Organoid intelligence (OI): the new frontier in biocomputing and intelligence-in-a-dish. Frontiers in Science.	N/S	N/S	N/S	Y (Stimulus-response training and organoid-computer interfaces)

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

The work reported in this manuscript has been funded by University of West Attica.

Conflict of Interest

The authors have no conflicts of interest to declare.