IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 23, 2021, accepted October 5, 2021, date of publication October 6, 2021, date of current version October 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3118642

Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis

MOHAMED AMINE FERRAG[1], OTHMANE FRIHA[2], LEANDROS MAGLARAS[3], (Senior Member, IEEE), HELGE JANICKE[4], (Member, IEEE), AND LEI SHU[5,6], (Senior Member, IEEE)

[1]Department of Computer Science, Guelma University, Algeria 24000, Algeria
[2]Networks and Systems Laboratory (LRS), Badji Mokhtar-Annaba University, Annaba 23000, Algeria
[3]School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, U.K.
[4]Cyber Security Cooperative Research Centre (CSCRC), Edith Cowan University, Perth, WA 6027, Australia
[5]College of Engineering, Nanjing Agricultural University, Nanjing 210095, China
[6]School of Engineering, University of Lincoln, Lincoln LN6 7TS, U.K.

Corresponding author: Mohamed Amine Ferrag (ferrag.mohamedamine@univ-guelma.dz)

This work was supported by the Cyber Security Cooperative Research Centre (CSCRC) and Edith Cowan University, Australia.

ABSTRACT In this article, we present a comprehensive study with an experimental analysis of federated deep learning approaches for cyber security in the Internet of Things (IoT) applications. Specifically, we first provide a review of the federated learning-based security and privacy systems for several types of IoT applications, including, Industrial IoT, Edge Computing, Internet of Drones, Internet of Healthcare Things, Internet of Vehicles, etc. Second, the use of federated learning with blockchain and malware/intrusion detection systems for IoT applications is discussed. Then, we review the vulnerabilities in federated learning-based security and privacy systems. Finally, we provide an experimental analysis of federated deep learning with three deep learning approaches, namely, Recurrent Neural Network (RNN), Convolutional Neural Network (CNN), and Deep Neural Network (DNN). For each deep learning model, we study the performance of centralized and federated learning under three new real IoT traffic datasets, namely, the Bot-IoT dataset, the MQTTset dataset, and the TON_IoT dataset. The goal of this article is to provide important information on federated deep learning approaches with emerging technologies for cyber security. In addition, it demonstrates that federated deep learning approaches outperform the classic/centralized versions of machine learning (non-federated learning) in assuring the privacy of IoT device data and provide the higher accuracy in detecting attacks.

INDEX TERMS Federated learning, intrusion detection, deep learning, cyber security, the IoT, blockchain.

I. INTRODUCTION

The Internet of Things (IoT) is defined as the use of communication protocols and sensing equipments such as sensors, laser scanners, radio frequency identification, etc., to enable control system devices to be connected to the Internet. During the last few years, IoT technology has been widely used in the following areas: Internet of Vehicles, Manufacturing industry, Internet of Drones, Internet of Healthcare Things, Mobile Crowdsensing, Cyber physical systems, Agriculture, etc [1]. As IoT technology develops rapidly, there are millions of embedded physical devices, where each IoT device is interconnected and exposing data that can potentially affect the privacy and personal well-being of their users. In the absence of a credible security defense systems implemented on the IoT devices, they can be attacked by hackers [2] and are representing a large attack surface that is actively exploited.

The availability of modern Machine Learning (ML) is gaining more attention than ever before for its potential to extract useful and complex data models using large datasets from a central location [3]. With traditional machine learning, the learning data is collected on a centralized server. without

The associate editor coordinating the review of this manuscript and approving it for publication was Vicente Alarcon-Aquino.

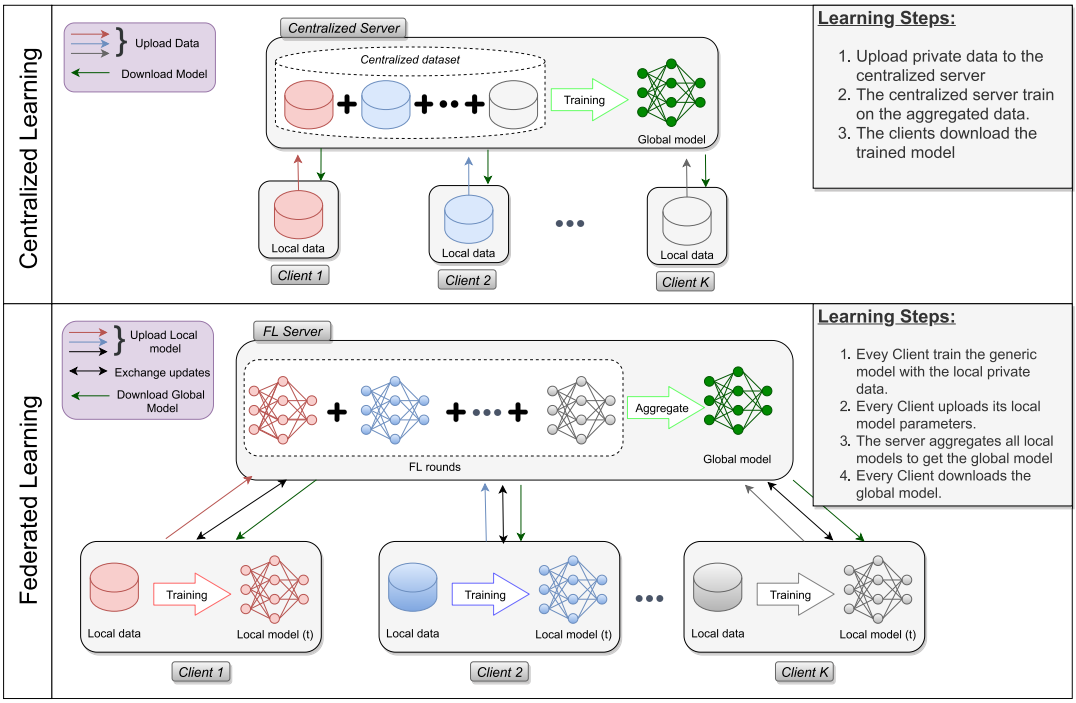


FIGURE 1. Centralized vs. Federated learning.

addressing the privacy concerns as well as reducing data transmission cost. In addition to other security measures, such as Blockchain and authentication [4], [5], the machine learning techniques can be used by intrusion detection systems in order to identify normal and malicious actions [6], [7].

The term of privacy-preserving machine learning has become popular nowadays [8]. The idea of federated learning is proposed by Google [9] to overcome data privacy issues by leveraging collaborative learning across a wide range of devices (i.e., IoT devices). However, there are various limitations to the application of traditional federated learning in IoT applications, including, the reliability of the learning model as well as of the central server. By modifying the local model, if the central server (i.e., Edge server) crashed or modified the global model maliciously, updating accuracy of all local models at IoT devices will be significantly affected [10]–[16]. The constraint of power in IoT devices is a major issue for the deployment of federated learning. This resource limitation requires that energy consumption should be optimized for the implementation of federated learning [17].

The federated learning achieves great success and is widely used in many fields, e.g., mobile edge network optimization [18], Google keyboard query suggestions and prediction [19], [20], COVID-19 detection [21]–[23], vehicles communications [24], Internet of Drones [25], Augmented reality [26], Intrusion detection [27]–[29] etc. Therefore, many cyber security researchers have difficulty in finding the best learning type (i.e., centralized or federated learning) to test and evaluate their proposed security methods in IoT applications, and selecting an appropriate federated deep learning method is an essential issue in this field. Hence, we are motivated to realize a comprehensive study with an experimental analysis of the use of federated deep learning for cyber security in the Internet of Things.

A. CENTRALIZED VS. FEDERATED LEARNING TYPES

Fig 1 illustrates the main difference between federated learning and centralized learning.

1) CENTRALIZED LEARNING

Machine learning for IoT applications has conventionally been performed by uploading all the data from each IoT device connected with the cloud servers to build a standard model which can be shared and implemented across devices. The main benefit of centralized learning is the ability of the model to perform generalization using data from a cluster of IoT devices and then work with other relevant IoT devices instantaneously. However, there are some issues for traditional centralized learning such as privacy, latency, bandwidth, and connectivity.

2) FEDERATED LEARNING

The core concept of federated learning is to create machine learning models that are built on distributed datasets across different devices while avoiding the leakage of data. Specifically, federated learning is a new technique where the current model is downloaded and an updated model is computed on IoT devices using the local IoT data. These locally trained models are then returned from the IoT devices to the central server for aggregation, (e.g., the weights are averaged)

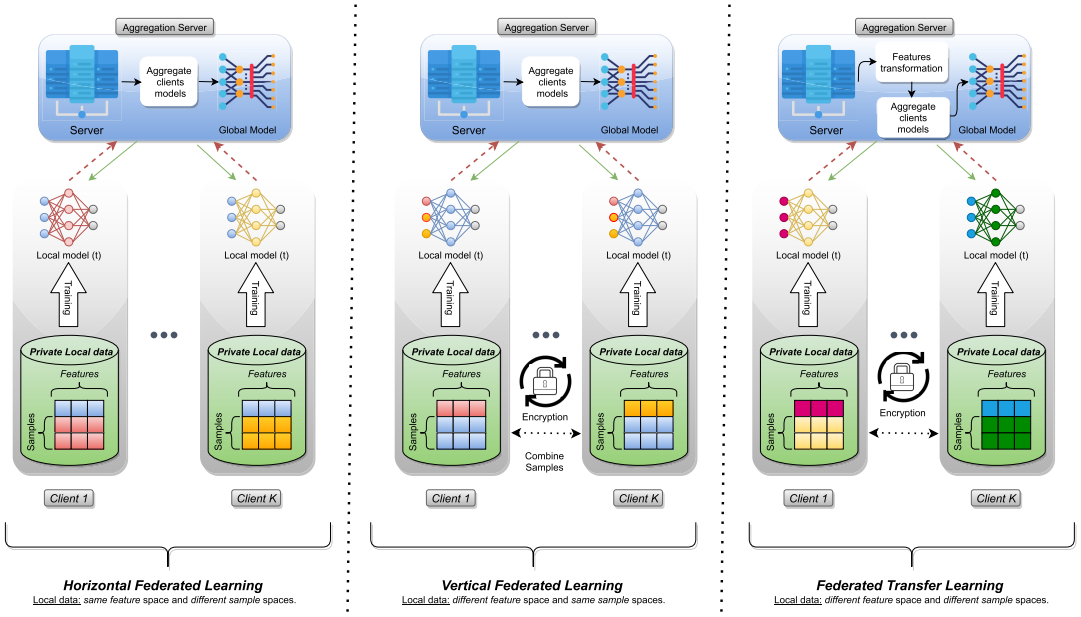


FIGURE 2. Federated learning types.

and then a combined and enhanced single global model is returned to IoT devices. The distribution of data is important in terms of federated learning deployment and the associated practical and technical challenges. There are currently the following three federated learning types, as presented in Fig 2:

- Horizontal federated learning: This type is implemented in situations in which the data sets share the same feature space but differ in the sampling space.
- Vertical federated learning: This type is implemented in the situations in which the data sets differ in the feature space but share the same sampling space.
- Federated transfer learning: This type is implemented in the situations where the data sets has different feature space as well as different sampling space.

B. RELATED SURVEYS AND OUR CONTRIBUTIONS

There are many surveys in the literature that have covered different aspects of federated learning-based frameworks for IoT. As shown in Tab. 1, we classify the federated learning surveys based on the following dimensions:

- *IoT application:* It indicates whether the survey presented a taxonomy for federated learning-based frameworks for cyber security in the internet of things.
- *Federated learning-based IDS:* It reports whether the study provided a taxonomy for federated learning-based cyber security intrusion detection systems for the IoT.
- *Federated learning-based blockchain:* It indicates whether the survey reviewed federated learning-based frameworks coupled with blockchain technology for cyber security in the internet of things.
- *Threat models in federated learning:* It indicates whether the survey considered threat models in federated learning-based frameworks for cyber security in IoT.
- *Experimental analysis in IoT:* It indicates whether the survey provided an experimental analysis of federated deep learning for cyber security in IoT.

Almost all of the surveys on federated learning for IoT applications present security and privacy countermeasures without focusing on an experimental analysis. Yang *et al.* [30] proposed a review of a secure federated-learning framework, which includes federated transfer learning, vertical federated learning, and horizontal federated learning. Aledhari *et al.* [32] a review of federated learning algorithms, which includes use-cases, real-life applications, and hardware platforms. Liu *et al.* [33] provided an introduction about the integration of federated learning in the context of 6G communications. Jiang *et al.* [34] presented the challenges and opportunities of the application of federated learning in smart city sensing. Mothukuri *et al.* [36] provided a comprehensive survey on privacy threats of federated learning, but without an experimental analysis in IoT networks. Kholod *et al.* [37] analyzed the open-source federated learning frameworks for IoT applications without focusing in cyber security. Rahman *et al.* [38] provided a comprehensive taxonomies covering privacy and security, resource management, application areas, system models and designs. Nguyen *et al.* [39] provided a comprehensive survey about the recent advances in federated learning and IoT applications. Wahab *et al.* [41] presented a multi-level classification of federated machine learning in communication and networking systems. Ali *et al.* [42] provided an overview about the integration of federated learning and blockchain for IoT applications. Imteaj *et al.* [43] analyzed the implementation challenges of federated

TABLE 1. Related surveys on federated learning for IoT networks.

Reference	Year	IoT application	FL-based IDS	FL-based blockchain	Threat models in FL	Experimental analysis in IoT	Main focus/contributions
Yang et al. [30]	2019	No	No	Partial	No	No	A review of a secure federated-learning framework.
Lim et al. [31]	2020	Partial	No	Partial	Yes	No	A comprehensive review of federated learning as an enabler for the optimization of mobile networks at the edge.
Aledhari et al. [32]	2020	Partial	Partial	Partial	No	No	An overview of technical details of federated learning enabling technologies.
Liu et al. [33]	2020	No	No	No	No	No	An introduction about the integration of 6G communications-based federated learning.
Jiang et al. [34]	2020	No	No	No	No	No	An overview of challenges and opportunities of the application of federated learning in smart city sensing.
Lyu *et al.* [35]	2020	No	Partial	No	Partial	No	A brief introduction to the FL idea, along with a classification of threat models.
Mothukuri et al. [36]	2021	No	No	No	Yes	No	A comprehensive survey on privacy threats of federated learning.
Kholod et al. [37]	2021	Yes	No	No	No	No	A review on open-source federated learning frameworks for IoT applications
Rahman et al. [38]	2021	Yes	No	No	Partial	No	A comprehensive taxonomies covering application areas of federated learning.
Nguyen et al. [39]	2021	Yes	No	Yes	Yes	No	A comprehensive survey about the recent advances in federated learning and IoT applications.
Nguyen et al. [40]	2021	Yes	No	Yes	No	No	An overview of the fundamental concepts about the integration of federated learning and blockchain.
Wahab et al. [41]	2021	Yes	No	Partial	Yes	No	A multi-level classification of federated machine learning in communication and networking systems.
Ali et al. [42]	2021	Yes	No	Yes	No	No	An overview about the integration of federated learning and blockchain for IoT applications.
Imteaj *et al.* [43]	2021	Yes	No	Partial	No	No	An overview the implementation challenges of federated learning algorithms for resource-constrained IoT devices.
Our survey	/	Yes	Yes	Yes	Yes	Yes	A comprehensive review with experimental analysis of federated deep learning for cyber security in IoT applications.

learning algorithms for resource-constrained IoT devices. Nguyen *et al.* [40] provided an overview of the essential notions about the integration of federated learning and blockchain in mobile edge computing networks. All these related surveys did not cover the application of federated deep learning for cyber security in IoT applications with focusing on experimental analysis.

Lyu *et al.* [35] provided a brief introduction into FL, alongside a classification for threat models into two major attacks: poisoning and inference attacks. The study points out the insights, the core techniques together with the fundamental assumptions embraced by the different attacks. The FL context brings an additional threat, which is model poisoning, distinct from traditional data poisoning. The goal is to make the global model incorrectly classify a given set of inputs. To explore this issue, Bhagoji *et al.* [44] conducted a range of attack scenarios, including: targeted model poisoning by intensifying the malicious agent update, improving attack stealth through the use of an alternating minimization strategy, and bypassing Byzantine-resistant aggregation strategies. Which validated the vulnerabilities of FL-based settings to model poisoning attacks. Xu *et al.* [45] proposed a FL-based privacy preservation scheme, called VerifyNet, which manages the verification of the training process, with homomorphic encryption, pseudo-random technology, and a double-masking protocol to ensure user privacy, verifiability, and confidentiality during the FL process. Results from experiments with real-world data have proved that VerifyNet is practical.

A notable exception is Goa et al.'s [46] recent work that reviews split and federated learning approaches with respect to their communication overheads and conducts an experimental evaluation against two established data-sets for Speech Command and ECG in a Raspberry Pie setup. In this context, we highlight the following research questions (i.e., Fig 17 that need to be solved:

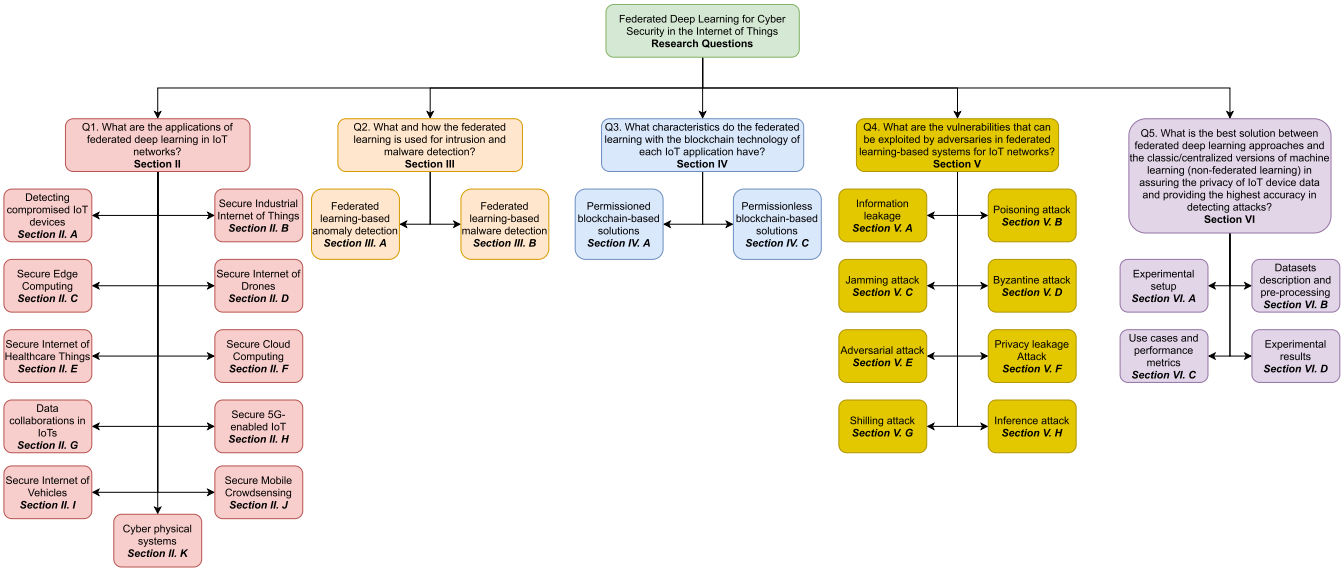


FIGURE 3. Discussed questions per article section.

- Q1. What are the applications of federated deep learning in IoT networks?
- Q2. What and how is the federated learning used for intrusion and malware detection?
- Q3. What characteristics do the federated learning approaches with blockchain technology have for each of the IoT applications?
- Q4. What are potential vulnerabilities that can be exploited by adversaries in federated learning-based systems for IoT networks?
- Q5. What is currently the best solution between federated deep learning approaches and the classic/centralized versions of machine learning (non-federated learning) in assuring the privacy of IoT device data and providing the highest accuracy in detecting attacks?

To answer the previous questions, the main contributions of this work are:

- We review the federated learning-based security and privacy systems for several types of IoT applications.
- We review the federated learning-based cyber security intrusion detection systems.
- We present the use of federated learning with blockchain for IoT applications.
- We review vulnerabilities that can be exploited by adversaries in federated learning-based security and privacy systems.
- We provide an experimental analysis of federated deep learning with three deep learning approaches, namely, RNN, CNN, and DNN. For each deep learning model, we study the performance of centralized and federated learning under three new real IoT traffic datasets, namely, the Bot-IoT dataset, the MQTTset dataset, and the TON_IoT dataset.

TABLE 2. Acronyms used in this survey.

Acronym	Description
FL	Federated Learning
IoT	Internet of Things
IIoT	Industrial Internet of Things
AI	Artificial Intelligence
IDS	Intrusion Detection System
DNN	Deep Neural Network
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
ML	Machine Learning
MEC	Mobile Edge Computing
UAV	Unmanned Aerial Vehicle
RF	Radio Frequency
HE	Homomorphic Encryption
DP	Differential Privacy
SGD	Stochastic Gradient Descent
DRL	Deep Reinforcement Learning
EV	Electric Vehicle
DDoS	Distributed Denial of Service
DoS	Denial of Service
IoHT	Internet of Health Things
PoCI	Proof of Common Interest
GAN	Generative Adversarial Network
IID	Independent and Identically Distributed
Non-IID	Non-Independent and Identically Distributed
ROC	The Receiver Operating Characteristic
MQTT	Message Queue Telemetry Transport
FNN	Feed-forward Neural Network
SNN	Self-normalizing Neural Network

The rest of this paper is organized as follows. Section II presents the federated learning-based security and privacy systems for several types of IoT applications. In Section III, we provide the federated learning-based cybersecurity intrusion detection systems. In Section IV, we clearly highlight the use of federated learning with blockchain for IoT applications. Then, we review vulnerabilities that can be exploited by

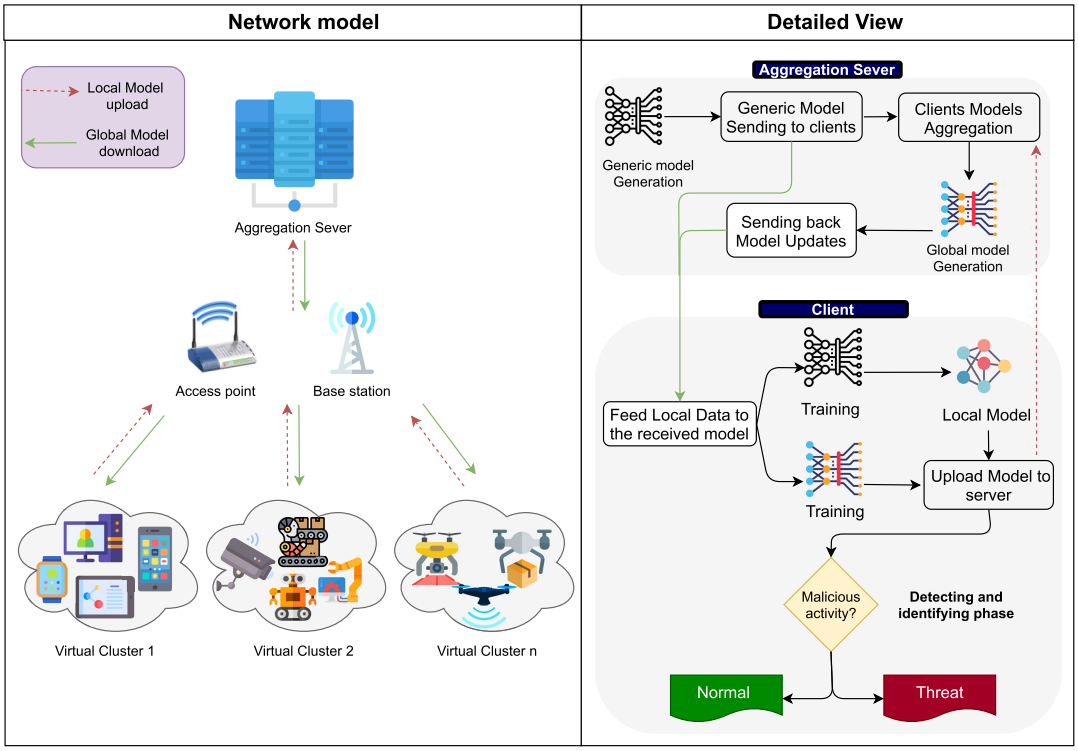


FIGURE 4. Federated learning for IoT networks.

adversaries in federated learning-based security and privacy systems in Section V. Section VI provides an experimental analysis of federated deep learning with three deep learning approaches. Section VII highlight the importance of the study and discuss the significance of our research on the future of the IoT and its applications, together with current open challenges. Lastly, Section VIII presents our conclusions.

II. FEDERATED MACHINE LEARNING APPROACHES FOR THE IoT APPLICATIONS

Fig 4 shows the federated learning-based cybersecurity for IoT. Tab. 2 provides the acronyms used in this study. Tab. 3 presents the federated learning-based solution for cybersecurity in IoT applications.

A. DETECTING COMPROMISED IoT DEVICES

IoT devices are being increasingly deployed in the everyday life. Many of those devices, however, are susceptible to attack through unsafe design, deployment, and configurations. Accordingly, many existing systems already contain vulnerable IoT devices that are open to being compromised, which is furthermore harmful in sensitive tasks such as surveillance, as shown by the work of Ciuonzo *et al.* [59], which focused on the issue of distributed detection of a non-cooperative object in a wireless sensor network.

While centralized learning-based intrusion detection approaches have been successful, including the hybrid hierarchical and AutoEncoder techniques, as presented by Bovenzi *et al.* [60], which provided a two-tier hierarchical network-based IDS that performs anomaly detection with a multimodal deep autoencoder, and soft output classifiers. And also, the work of Mirsky *et al.* [61], which provided Kitsune, a network-based plug-and-play IDS that can efficiently classify attacks on the local network without supervision. However, data privacy, network latency, and similar centralized learning-based issues are not considered in these approaches.

To identify compromised IoT devices, Nguyen *et al.* [57] proposed an autonomous self-learning distributed scheme, named DIOT, which is based on a federated learning approach. The flask and flask socketio libraries are used during the implementation of the federated learning algorithm. The performance evaluation shows that the DIOT scheme is able to detect 95.6% of attacks in an average of 257 milliseconds. Zhao *et al.* [62] developed a federated learning-based intrusion detection system, which can be used for detecting compromised IoT devices. The proposed system proposes that the global initial long short-term memory model is distributed among all user servers. Then, the user servers form their own unique model and start uploading their model settings to the central server. Last, the central server aggregates the model settings in order to form a new aggregate global model and then sends it to the user servers. The results of simulation on the SEA dataset (i.e., produced by the AT&T Shannon Lab) demonstrate that the proposed system reaches better accuracy and coherence compared to

TABLE 3. Federated learning-based solution for cyber security in IoT applications.

Scheme	Year	Network model	Countermeasures	Threat models	Datasets	Pros (+) Cons (+)
ur Rehman *et al.* [27]	2021	Industrial Internet of Things	- Cross-Device Federated Learning - Blockchain technology	Poisoning attacks	Turbofan Engine Degradation simulation dataset	+ Less loss regardless of population size - The threat model is limited
Sun et al. [47]	2021	Industrial Internet of Things	- Digital Twin - Deep reinforcement learning	Byzantine attack	MNIST dataset	+ Efficent in terms of energy saving, convergence rate, and learning accuracy - Vulnerable to dishonest users
Yang et al. [48]	2021	Cyber physical systems	Optimized federated soft-impute algorithm	Differential attack	Two synthetic tensors	+ Low recovery error under differential privacy protection - Energy consumption
Kong et al. [24]	2021	Internet of Vehicles	- Limited Laplace mechanism - Homomorphic threshold encryption mechanism	Unregistered dishonest users	N/A	+ Robustness against dishonest users - Computation and communication cost
Thwal et al. [49]	2021	Internet of Healthcare Things	- Deep learning-based clinical decision support system	Unregistered dishonest users	Laboratory network setup	+ Guarantee the safety of patient privacy - Computation and communication cost
Fang et al. [50]	2020	Cloud Computing	- Lightweight encryption protocol	Colluding parties and an honest but curious server	MNIST and UCI Human Activity Recognition Dataset	+ Highest accuracy compared to existing works - Vulnerable to the generative adversarial network
Dong et al. [51]	2020	Ternary federated learning	- Shamir's threshold secret sharing(TSS) - Paillier homomorphic encryption(PHE)	Honest-but-curious or semi-honest adversary	MNIST and SVHN	+ Communication overheads and computational time - Vulnerable to the generative adversarial network
Yu et al. [52]	2020	5G-enabled IoT	- Blockchain technology - Deep reinforcement learning	Sniffer attacks and jamming attacks	MATLAB RL toolbox	+ Energy consumption - Differential privacy protection is not considered
Lu et al. [53]	2020	Digital Twin Edge Networks	- Blockchain technology - Deep reinforcement learning	N/A	MNIST dataset with Fashion-MNIST	+ Communication efficiency and data security - Vulnerable to blockchain-related attacks
Liu et al. [54]	2020	Mobile Crowdsensing	- Bresson's cryptosystem - Shamir's secret sharing	- Inference attack - Chosen plaintext attack	ADULT and MNIST	+ Computation and communication cost reduction - Robustness against dishonest users
Lu et al. [55]	2020	Vehicular cyber-physical systems	- Random sub-gossip updating - Distributed model aggregation	- Differential attack	20 Newsgroups dataset	+ Protecting privacy in updating - Energy consumption
Wang et al. [25]	2020	Internet of Drones	- Blockchain technology - Local differential privacy - Reinforcement learning	- Privacy leakage attack - Poor quality local model update attack	MNIST	+ Enhanced the quality of the local model update (QoLM) metric - Computation and communication cost
Lu et al. [56]	2019	Internet of Vehicles	- Neural network model	Unregistered dishonest users	The core control systems of electric vehicle	+ Privacy preserving as well as driver personalization - Vulnerable to differential attack
Nguyen et al. [57]	2019	IoT devices	- Gated recurrent units	- Adversarial machine learning - Poisoning federated learning	Laboratory network setup	+ 95.6% of attacks are detected in 257 milliseconds - Communication overheads
Hao *et al.* [58]	2019	Industrial artificial intelligence	- Augmented Learning with Error	Inference attack	MNIST dataset	+ Communication and computation costs - Threat model is limited

the conventional systems. To find the best candidate clients and solve the issue of accuracy optimization in federated learning, Mohammed *et al.* [63] introduced an online stateful heuristic based on federated learning combined with an IoT client alarm application, which can be used to notify clients of any unauthorized IoT devices in the IoT environment. The results of simulation on a real data set demonstrates that the suggested system surpasses the online randomized algorithm with up to 27% gain in terms of accuracy.

B. SECURE INDUSTRIAL INTERNET OF THINGS

With small size, small cost, and limited energy consumption, these appealing capabilities have made Internet of Things (IoT) largely endorsed in smart factories to supervise machinery, guide their automatic processes, or to help create a virtual representation of systems for advanced simulation purposes using digital twins [64]. To provide the tensor based data mining while guaranteeing the data security in industrial internet of things, Kong *et al.* [65] proposed a framework

Federated Tensor Mining, named FTM, which is based on homomorphic encryption methods. The FTM framework is claimed to achieve high accuracy due to the homomorphic attribution. Khoa *et al.* [66] presented an IDS based on collaborative learning which can be applied effectively in the Industrial IoT and Industry 4.0. The proposed system builds intelligent "filters" for deployment at IoT gateways to quickly identify and prevent cyberattacks. Specifically, each filter utilizes the data collected in a filter's network in order to train its model for cyberattack detection through a deep learning system. Afterward, the trained model is distributed to other IoT gateways to increase the accuracy of intrusion detection throughout the overall system.

Rehman *et al.* [27] proposed an idea to enable a fully decentralized cross-device federated learning system, named TrustFed, which uses Industrial IoT devices as federated learning candidates. To maintain participants' reputations, the proposed TrustFed system uses smart contract technology and the Ethereum blockchain. TrustFed can identify and eliminate outliers in the training distributions prior to combining the model updates. The results of the simulation on the Turbofan Engine Degradation simulation dataset (released by NASA) demonstrates that the proposed system performs better in terms of the lower loss irrespective of the population size. Sun *et al.* [47] introduced a new framework based on digital twin to assist federated learning in Industrial IoT. The digital twin are used for capturing the characteristics of industrial devices. Hao *et al.* [58] developed a privacy-enhanced federated learning system, named PEFL, for industrial artificial intelligence, which is based on Augmented Learning with Error (A-LWE) term embedded with the homomorphic ciphertext of private gradients. To provide differential privacy, the PEFL system adopts a distributed Gaussian mechanism. The performance evaluation on MNIST dataset demonstrates that the PEFL system in terms of accuracy as well as communication and computation costs. To reduce the communication burden on the federated learning server, a proxy server can be used which is proposed Zhao *et al.* [67] to achieve anonymity of participants.

C. SECURE EDGE COMPUTING

Newly emerging technologies such as Mobile Edge Computing (MEC) and new generation communication technologies are essential to support the fast development and deployment of the IoT networks. As IoT networks grow in scale, determining the optimal allocation of limited resources to deliver high-quality IoT services is a critical challenge. Edge computing involves the processing of data at the edge of a network compared to processing in the cloud or on a remote server. To provide privacy and data security, Taïk and Cherkaoui [68] designed a system model based on federated learning and edge computing. The edge devices are used to train models by federated learning, which can minimize security issues. Lu *et al.* [53] designed a new system, named DITEN, that integrating blockchain and federated learning in edge networks. The proposed DITEN system uses Deep Neural Networks (DNN) as a strategy scheduler to ensure data privacy of users and enhance learning security. The experimental results on two datasets, namely, the real-world MNIST dataset and the Fashion-MNIST show that the proposed DITEN system is efficient compared to the conventional federated learning in terms of learning accuracy, learning loss, and communication time cost. Qian *et al.* [69] developed a privacy-preserving data analytic system, where the federated learning at the centralized fog devices. The proposed system uses an active learning in edge devices, which can harvest the potential privacy benefits as well as reduce latency and communication overhead.

To provide joint IoT network and edge server optimization, Xiao *et al.* [70] proposed a federated edge intelligence framework, named FEI. The FEI consists of a group of edge servers that trains a shared model using the data collected and uploaded from IoT devices. Cui *et al.* [71] introduced a secure and decentralized platform, named SAPE, for securing edge computing. The SAPE platform enables users to send their assignments, which are then planned to the relevant edge nodes to reduce the time it takes to complete the tasks. To prevent attacks, the SAPE platform uses federated deep reinforcement learning (DRL). The reliability of the federated training process is improved by a blockchain-based verification scheme. The findings demonstrate that SAPE overcomes some of the shortcomings conventional schemes during the defense against adversarial attacks.

D. SECURE INTERNET OF DRONES

The combination of unmanned aerial vehicles (UAVs) and artificial intelligence (AI) technology created opportunities to facilitate existing ground-based mobile crowdsensing platforms to achieve more difficult missions. More precisely, drones enable autonomous crowdsensing at any time and any place due to their remarkable benefits of lower cost, faster operational deployment, and more flexible movement, as presented by Motlagh *et al.* [72], which provided a demonstration of the use of drones for crowd surveillance through face recognition. Federated learning can provide significant privacy protection by allowing a collection of UAVs to train a shared AI model collaboratively while preserving the training data (i.e., sensed data) on their devices at the local level. Fig 5 illustrate the federated learning-based cybersecurity for internet of drones. For secure and efficient AI model training in UAV-assisted mobile crowdsensing, Wang *et al.* [25] designed a practical federated learning framework, named SFAC, which is based on three technologies, namely, blockchain, local differential privacy, and reinforcement learning. Blockchain technology is used to preserve data training and contribution verification between drones, whereas reinforcement learning is used to achieve optimal strategies. Their performance evaluation using the MNIST dataset showed that the SFAC framework enhanced the quality of the local model update (QoLM) metric in the federated learning process learning, compared with conventional frameworks. To defend against jamming attacks,

Mowla *et al.* [73] introduced an adaptive federated reinforcement learning system, which can be applied for flying ad-hoc networks. The simulation results indicated a 39.9% improved average accuracy of the federated jamming detection scheme used in the defense mechanism.

To counteract eavesdropping in a fog-aided IoD network, Yao *et al.* [74] proposed a secure federated learning scheme. The main idea of this proposed scheme is that monitoring the energy of all the unmanned aerial vehicles (UAVs) to optimize the safety rate of the federated learning system is limited by the UAV battery capacity and the Quality of Service (QoS) constraint. The performance evaluation of the proposed scheme shows that it performs better than two existing related algorithms with a small federated learning training time. Therefore, Yazdinejadna *et al.* [75] designed an authentication system based on federated learning using drones' Radio Frequency (RF) features. The proposed authentication system uses the Deep Neural Network (DNN) and Homomorphic Encryption (HE). The DNN network is implemented locally on drones with Stochastic Gradient Descent (SGD) optimization, while the HE system is used to secure model parameters. From the experimental findings, the proposed authentication system obtains a high true positive rate when authenticating drones and improved performances in comparison to alternative machine learning-based systems.

E. SECURE INTERNET OF HEALTHCARE THINGS

The management of health has emerged as a major issue and challenge as new complex types of diseases and symptoms are introduced like COVID-19. Fig 6 present how the healthcare sector can use federated learning techniques in order to maintain patients' data privacy, while benefiting from other hospitals' knowledge. Thwal *et al.* [49] designed a deep learning-based clinical decision support solution, which is trained and managed in a federated learning model. The proposed solution focused on an approach to ensure patients' privacy and address the threat of cyberattacks by allowing for the mining of clinical data at a large scale. Based on a federated learning model, the proposed solution can exploit rich clinical data to train every local neural network with no requirement to share patient private data.

To decrease energy consumption in the federated learning process, Hao *et al.* [76] designed a new scheme, which separates the model into three sections and transfers the central section to the cloud server with a high computational cost. To perform gradients aggregation in ciphertext context, the proposed scheme applies homomorphic encryption, which can resist several existing deep learning privacy attacks. For securing wearable healthcare, Chen *et al.* [77] a federated transfer learning framework, named FedHealth. The FedHealth framework combines different organizations' data without losing information privacy and performs comparatively personalized learning of models using transfer of knowledge.

The COVID-19 pandemic triggered a global crisis that required collaborative efforts to combat it. A critical factor in evaluating and responding to COVID-19 is the effective identification of infected patients, and AI is a key part of this. However, the problem with the old centralized AI is the sharing of data among hospitals around the world, which raises many privacy issues, and that's where FL comes in. Zhang *et al.* [23] proposed a dynamic fusion-based FL system to analyze medical diagnostic images such as CT scans and X-rays, and decide dynamically which clients participate according to the performance of their local model and plan the fusion of models depending on the training time. The results demonstrated that the system is practical in terms of performance, communication and failure tolerance. Kumar *et al.* [21] proposed a blockchain-based FL system for COVID-19 detection, which was trained and evaluated on real COVID-19 patient data that was collected and publicly published from various hospitals with different types of CT scanners, as well as a data normalization strategy. Liu *et al.* [22] proposed an FL-based model for learning COVID-19 data. The authors evaluated the performance of popular models, including MobileNet, ResNet18, and COVIDNet, with and without the FL framework. The authors concluded that ResNeXt shows the highest efficiency in images with COVID-19 labels. Whereas, MoblieNet possessed the lowest number of parameters. Hence, the work suggests that ResNeXt and ResNet18 are selected to be better for COVID-19 identification among the models used.

F. SECURE CLOUD COMPUTING

While conventional machine learning training models share data centrally in the cloud, an increasing number of customers are not interested in participating in data sharing due to privacy or peer competition issues. Federated learning has been suggested as a distributed platform to overcome these limitations, where multiple customers collectively train a machine learning model without partitioning their individual datasets. Fang *et al.* [50] designed a federated learning scheme with strong privacy preservation, named HFWP, for securing cloud computing. Based on a lightweight encryption protocol, the HFWP scheme is robust against colluding parties and an honest but curious server. The experimental results on two real-world datasets, namely, MNIST and UCI Human Activity Recognition Dataset, shows the highest accuracy compared to other existing works. Zhang *et al.* [78] introduced a federated learning scheme that takes the local characteristics of AI IoT applications, which can enhance the accuracy of prediction of any individual AI IoT-enabled device.

For enhancing cloud computing-based 5G heterogeneous network, Wei *et al.* [79] designed a federated learning scheme based on end-edge-cloud cooperation. Within this scheme, the nodes that are equipped with mechanisms for attack detection are deployed in the end, edge, and cloud of the 5G heterogeneous network. To reduce the negative impacts due to heterogeneity in a cloud-edge architecture, Wu *et al.* [80] proposed a personalized federated learning

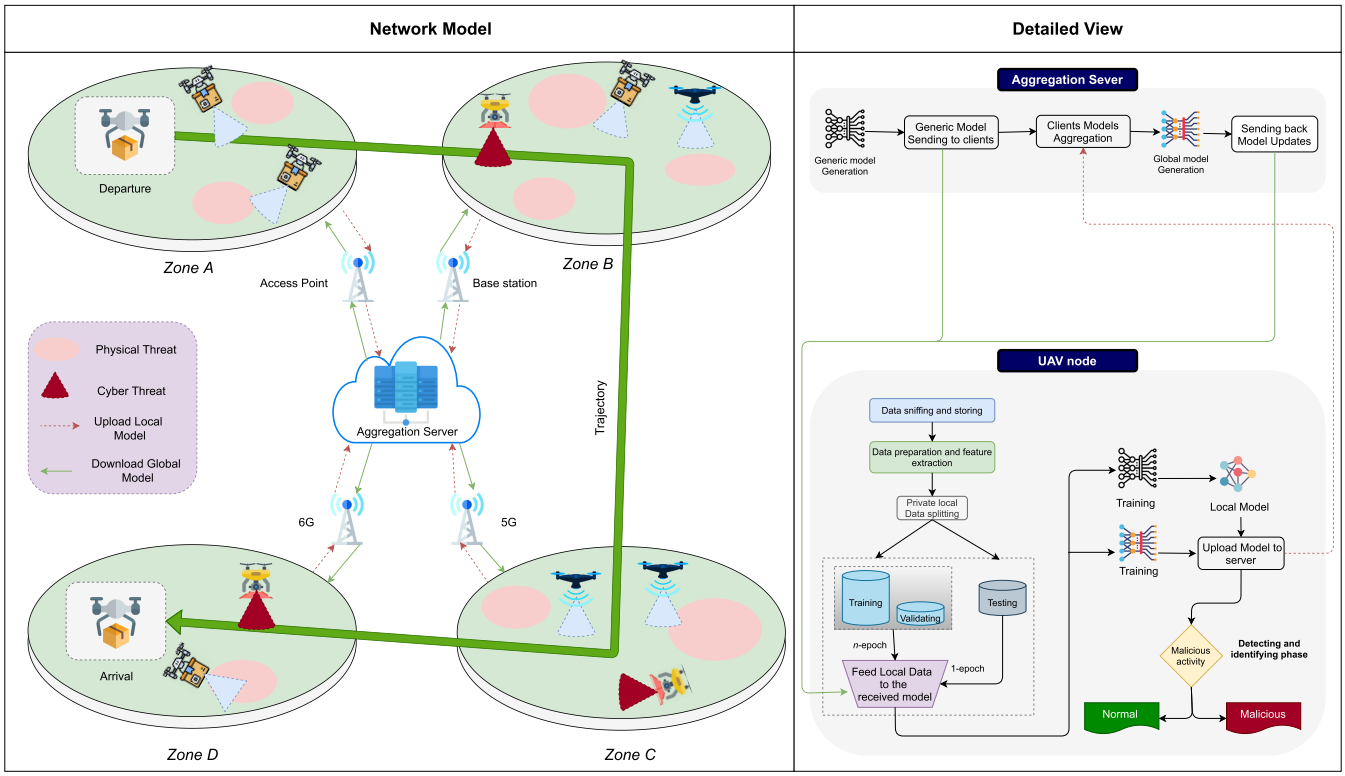


FIGURE 5. Federated learning for secure internet of drones.

scheme, which the power of edge computing is used for high throughput and low latency.

G. DATA COLLABORATIONS IN IoTs

As IoT technologies are rapidly emerging, network applications require cross-domain collaborative computational processing, which necessitates the aggregation and cooperation of a large number of network data sources. Different data owned by various stakeholders and having distinct properties will be combined into the network applications within these processes. The information that is revealed to the providers of applications, results in the inevitable risks of losing data privacy control. To enable the secure collaboration of massive data sources, Yin *et al.* [81] designed a secure data collaboration scheme, called FDC, which can be applied in an IoT environment. The FDC scheme uses three parties: a blockchain system, public data center, and a private data center. The blockchain system is used to sustain flexibility and access control, while the private data center is applied for registration, management, storage, and IoT data collection. The performance evaluation on wearable sensor data shows that the proposed FDC scheme provides efficient accuracy and loss.

H. SECURE 5G-ENABLED IoT

The IoT network environments are time-varying, and the network devices' heterogeneous resources make it difficult to provide reliable, secure, and real-time communications among the network devices and their service servers, especially in the 5G-enabled IoT. Yu *et al.* [52] proposed a federated learning-based distributed model, named UDEC, in order to address the following three challenges: *1)* Privacy and security-preserving services, *2)* Dynamic and low-cost scheduling, and *3)* Full use of system resources. The UDEC model train deep reinforcement learning to secure critical users' service request data at the edge nodes. Their performance evaluation shows the effectiveness of the UDEC model in terms of energy consumption.

I. SECURE INTERNET OF VEHICLES

Vehicular IoT provides a safer travel environment and better on-board experience, leading us to a smart and self-driving automotive future. In particular, there are a number of applications that can be found in the field of automotive IoT, including, autonomous vehicles, driver assistance, vehicle telematics, and predictive automotive maintenance. A federated learning approach is implemented in the field of data-driven navigation, which uses the data that mobile users collect and embedded processing resources. Fig 7 illustrate the use of federated leaning-based cybersecurity for Internet of Vehicles applications. To address the challenge of flexibility of participants under a federated learning-based navigation application, Kong *et al.* [24] proposed a privacy-preserving model aggregation technique,

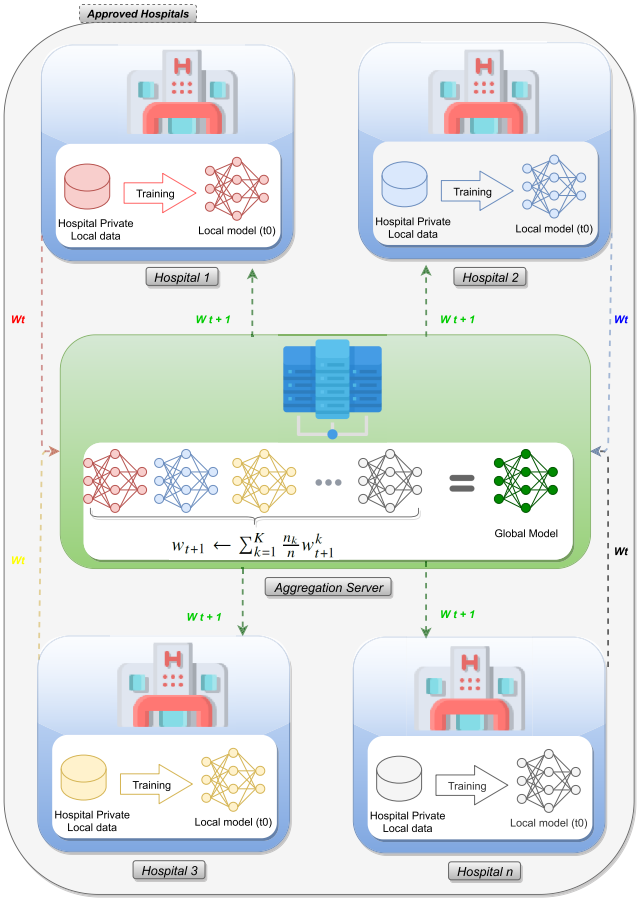


FIGURE 6. Federated learning for secure internet of Healthcare things.

named FedLoc, which can secure updates to locally trained models, providing robust support for participant fluctuation. The FedLoc scheme is robust against malicious unauthorized participants by employing the limited Laplace mechanism as well as the homomorphic threshold encryption mechanism. Lu *et al.* [56] designed a collaborative edge learning framework, named CLONE, by using real-world data set captured from a large electric vehicle (EV) manufacturing enterprise. The CLONE framework is based on long-term memory networks and a federated learning algorithm to proves latency saving, privacy enforcement, safety preservation, and the efficacy of driver personalization. The CLONE framework selects the fault of an EV battery and related hardware as a case study to demonstrate that the CLONE system can predict failures with accuracy to achieve collaborative and reliable driving. Lu *et al.* [55] proposed a scheme for federated peer-to-peer vehicle learning that uses random updating of sub-pots with no conservators, which increases both safety and reliability. The process of aggregation is performed in all vehicles in an asynchronous manner. When performing a joint learning task that includes data sharing or leak detection, all vehicles act as participants to perform federated learning. The information from vehicle data retrieval is stored on neighboring RSUs in the system in a distributed hash table form.

Lu *et al.* [55] proposed a scheme for federated peer-to-peer vehicle learning that uses random updating of sub-pots with no conservators, which increases both safety and reliability. The process of aggregation is performed in all vehicles in an asynchronous manner. When performing a joint learning task that includes data sharing or leak detection, all vehicles act as participants to perform federated learning. The information from vehicle data retrieval is stored on neighboring RSUs in the system in a distributed hash table form.

J. SECURE MOBILE CROWDSENSING

Mobile Crowdsensing is an emerging key element of IoT, which is a model that employs individuals wearing smart devices, called ''workers'', to conduct different sensing activities. To resolve two challenges for mobile crowdsensing, namely, user dropout and forced aggregation, Liu *et al.* [54] proposed a federated extreme gradient boosting framework, named FEDXGB, which is based on two kinds of parts, a central cloud server and a set of users. FEDXGB performs the following process. The central server takes an iterative invocation of a sequence of secure schemes to construct the XGBoost classification and regression tree. Within the schemes, the FEDXGB framework uses a secure aggregation protocol to aggregate user gradients. Through a combination of Bresson's cryptosystem and Shamir's secret sharing, FEDXGB allows the central server to perform constrained aggregation on the gradients and is able to recover dropout users' data. The performance evaluation under both ADULT and MNIST datasets show that the FEDXGB framework can provide a computation and communication cost reduction with negligible performance loss.

The data aggregation techniques based on homomorphic encryption for privacy-preserving have been well-studied for improving the privacy of FL systems. Zhang *et al.* [82] proposed a secure data aggregation system, named FedSky, for federated mobile crowdsensing, which is based on an effective worker selection mechanism. Instead of choosing a random cluster of users, The FedSky system chooses a cluster of users based on the size of the users' local data and the computing power of their mobile devices. Compared to the conventional FedAvg approach [83], the proposed system can reduce significantly the computation time of the users as well as the latency of the system. The performance evaluation on the MNIST dataset shows that the proposed system the maximum training time can be as high as 6 hours under the experimental setting of $sd = 15$ and $k = 100$ (sd: the standard deviation for computational power; k: the number of selected workers).

K. CYBER PHYSICAL SYSTEMS

Cyber physical systems process multi-source and large-scale data in various domains of application. These data are generally composed of private personal and incomplete information, usually distributed across various devices and locations. Federated learning is proposed as an efficient approach for ensuring the privacy of cyber physical systems. Based on a

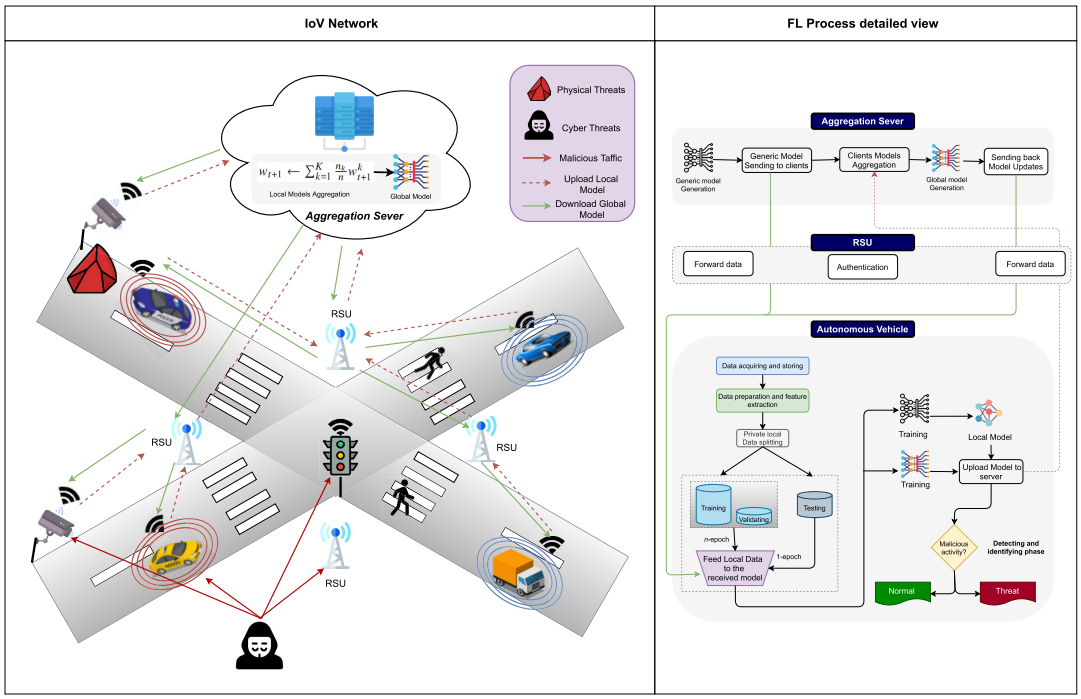


FIGURE 7. The application of federated learning approach for secure internet of vehicles.

Gaussian mechanism and an optimized federated soft-impute algorithm, Yang *et al.* [48] introduced a privacy-preserving tensor completion method. Through a formal recovery error bound, the proposed privacy-preserving tensor completion method is proven that can provide a privacy guarantee with high accuracy.

III. FEDERATED LEARNING-BASED CYBER SECURITY INTRUSION DETECTION

Tab. 4 presents the federated learning-based systems for intrusion and malware detection in IoT applications.

A. FEDERATED LEARNING-BASED ANOMALY DETECTION

Federated learning is a decentralized machine learning approach that exploits the performance computing power of edge devices with no explicit exchange of user data patterns. The local models are trained on user data on the device, and those models are forwarded to a central server. Since it is trained on sensitive user data, federated learning can suffer from machine learning attacks against the locally created models. To overcome this problem, Al-Marri *et al.* [89] proposed an IDS based on federated mimic learning. The proposed system is implemented and evaluated using Python on Google Colab with the real-world dataset (NSL-KDD), which the results show 98.11% detection accuracy with federated mimic learning compared to centralized machine learning-based IDSs. To address the need for securing traffic and maintaining privacy in heterogeneous networks, Li *et al.* [90] designed a distributed an IDS based on federated learning for satellite-terrestrial integrated networks for analyzing and blocking harmful traffic, especially distributed denial of service (DDoS) attacks. The proposed IDS uses two technologies, namely, *1)* homomorphic encryption to provide secure multi-party computing in federated learning and *2)* convolutional neural network for achieving higher recognition accuracy.

To detecting various types of cyber threats against industrial cyber physical systems, Li *et al.* [92] designed an IDS based on federated learning with a convolutional neural network and a gated recurrent unit. The proposed IDS system employs the Paillier public-key cryptosystem to ensure that the model parameters remain secure and private throughout the training process. The performance evaluation under the gas pipeline system dataset show the following results: F-score = 98.14 %, recall = 97.47 %, precision = 98.85 %, accuracy = 99.20 %, which are better compared to three related works [57], [95], and [77]. Mothukuri *et al.* [85] uses Gated Recurrent Units (GRUs) models-based anomaly detection approach to provide real-time proactive recognition of intrusions in IoT networks through the use of decentralized device data. The proposed IDS can preserve the integrity of data stored on local IoT devices by sharing only the weights learned with the federated learning's central server. Huong *et al.* [86] designed an IDS, named LocKedge, for IoT networks. The LocKedge system uses the detection task right at the edge layer with high accuracy. Therefore, the detection system is based on two modules: feature extraction and classification. The feature extraction stage focuses on minimizing features from the input samples that are fed to the detection stage. The performance evaluation under the

TABLE 4. Federated learning-based systems for intrusion and malware detection in IoT applications.

IDS model	Year	Network model	FL technique	Threat models	Validation	Performance evaluation	Comments
Li *et al.* [84]	2021	Industrial internet of things	An iterative model averaging with GRU	DDoS attacks	OPNET Modeler	The detection accuracy is approximately 98%	The energy cost is not calculated
Wang *et al.* [28]	2021	Industrial internet of things	Deep reinforcement learning algorithm	Privacy leakage attack	10 computers are deployed to simulate a local anomaly detection center	Miss detection rate= 2.5%	The proposed IDS is not validated with network intrusion detection dataset
Cvitiæ et al. [29]	2021	IoT applications	Logistic Model Trees (LMT) method	DDoS attacks	Network intrusion detection dataset	Detection accuracy= 99.21% - 99.96%	The communication and energy costs are not calculated
Mothukuri et al. [85]	2021	IoT applications	Gated Recurrent Units (GRUs) models	DDoS attacks	Modbus-based network dataset	Detection accuracy= 99.5%	The energy cost is not calculated
Huong et al. [86]	2021	IoT Edge Computing	Traditional neural network	Data exfiltration attacks, Keylogging, Server Scanning, DoS (HTTP, TCP, UDP), and DDoS (HTTP, TCP, UDP).	Network intrusion detection dataset (BoT-IoT dat)	AUC = 99 %	The energy cost is not calculated
Zhao *et al.* [62]	2020	One central server communing with users servers	Long short-term memory model	Directory traversal attacks	SEA dataset (i.e., produced by the AT&T Shannon Lab)	F1 Score= 99.21%, Precision= 99.19%, Recall= 99.23%, Accuracy= 99.21%	The dataset used in the performance evaluation does not include IoT traffic
Taheri *et al.* [87]	2020	Industrial IoT	- Generative adversarial network - Federated generative adversarial network	Poisoning attack	Contagio dataset, Drebin dataset, and Genome dataset	Accuracy ratio is around 96%	Inference attacks are not considered
Chen et al. [88]	2020	Wireless Edge Networks	Gated Recurrent Units (GRUs) models	Poisoning attack	KDD CUP 99 data set, CICIDS2017 data set, and WSN-DS wireless network data set	Detection accuracy= 99%	The dataset used in the performance evaluation does not include IoT traffic
Al-Marri et al. [89]	2020	IoT devices	Federated mimic learning	The following four types of attacks are considered : DoS, Probe, R2L, and U2R	Network intrusion detection dataset (NSL-KDD dataset)	Detection accuracy=98.11%	The dataset used in the performance evaluation does not include IoT traffic
Li et al. [90]	2020	Satellite-terrestrial integrated networks	Federated learning with convolutional neural network	Distributed denial of service (DDoS) attacks	Network intrusion detection dataset	Detection accuracy=90%	The types of DDoS attacks is limited
Rahman *et al.* [91]	2020	IoT application	- Neural network architecture	Dos, Probe, U2R, and R2L attacks	Network intrusion detection dataset (NSL-KDD dataset)	An accuracy fluctuating around 83.09 %	The dataset used in the performance evaluation does not include IoT traffic
Li et al. [92]	2020	Industrial Cyber-Physical Systems	Federated learning with convolutional neural network and a gated recurrent unit	Cyber threats against industrial CPSs	Gas pipelining system	F-score = 98.14%, recall= 97.47%, precision=98.85%, accuracy= 99.20%	RoC curve metric is not reported
Payne and Kundu [93]	2019	IoT-based cloud computing	A hierarchical approach towards deep federated defenses	Hyperjacking, Hypercall attacks, DDoS attacks...etc.	N/A	N/A	There is no experimental analysis with IoT datasets
Chen et al. [94]	2019	Traditional networks	Federated deep autoencoding gaussian mixture model	The following four types of attacks are considered : DoS, Probe, R2L, and U2R	Network intrusion detection dataset (KDD-CUP 99)	Recall = 98.03%	Detection accuracy is not reported

BoT-IoT dataset shows that federated learning results are lower than its centralized mode counterpart. Chen *et al.* [94] proposed a federated deep autoencoding Gaussian mixture model, named FDAGMM, for network anomaly detection. Through the performance evaluation under the use of the network intrusion detection dataset (KDDCUP 99), the results show that the FDAGMM model is efficient in three metrics, including, F1-Score, Precision, and Recall, compared to the deep autoencoding gaussian mixture model.

Based on the performing inference of detection models and local training, Rahman *et al.* [91] proposed a federated learning-based system for detecting IoT intrusion, which can preserve data privacy. Therefore, the IoT devices can take advantage of the knowledge of their peers by sharing only the updates to a remote server. Then, the remote server aggregates the updates and exchanges an enhanced detection framework with the collaborating devices. The performance evaluation on an NSL-KDD dataset shows that the proposed system have an accuracy fluctuating around 83.09 %. Cetin *et al.* [96] proposed an IDS, named FedAGRU, which is based on federated learning. For collaborative training, FedAGRU takes advantage of the computing resources of edge devices and local datasets for training the model and then uploads the settings to a server. Through the performance evaluation under the use of the three network intrusion detection dataset, namely, KDD CUP 99 data set, CICIDS2017 data set, and WSN-DS wireless network data set, the results show that the FedAGRU system provides less communication overhead with higher detection accuracy. McElwee *et al.* [97] proposed a federated analysis security triage tool, named FASTT, for prioritizing and responding to IDS alerts. The FASTT tool resolves the issue of the high volume of intrusion detection threats that need to be reviewed by security analysts in a manual process. Based on the TensorFlow deep neural network approach, the FASTT can categorize intrusion detection alerts and identify which types of security analysts are to review the threats.

To construct a generalized model for anomaly detection in the industrial internet of things, Wang *et al.* [28] proposed hierarchical federated learning, where every local model is trained by deep reinforcement learning algorithm. As the local datasets are not needed during federated learning, the privacy leakage risk is minimized. Moreover, through injecting a degree of privacy leakage and an interaction function into the anomaly detection concept, the proposed system can significantly increase the accuracy of detection.

Based on a boosting method of logistic model trees, Cvitic *et al.* [29] proposed a DDoS traffic detection for different IoT device classes. For collecting federated data from heterogeneous sources in IoT networks, Moustafa *et al.* [98] introduced the testbed TON IoT datasets for Windows operating systems, which is deployed in three layers: edge, fog, and cloud. The edge layer includes IoT devices, the Fog layer includes gateways and virtual machines, and the cloud layer includes cloud services, connected to the other two layers. Therefore, the TON IoT datasets employed under the following nine attack families: 1) Man-In-The-Middle (MITM) attack, 2) Password attack, 3) Cross-site Scripting (XSS) attack, 4) Injection attack, 5) Backdoor attack, 6) Ransomware attack, 7) Distributed Denial of Service (DDoS) attack, 8) Denial of Service (DoS) attack, and 9) Scanning attack. To provide wireless edge network security in IoT networks, Chen *et al.* [88] proposed a federated learning-based intrusion detection system, named FedAGRU, which employs gated recurrent units (GRUs) models. Specifically, the proposed FedAGRU system is different from the existing centralized learning approaches by providing updates to the global learning models rather than sharing the original data directly between the central server and edge devices. Based on three datasets, namely, KDD CUP 99 data set, CICIDS2017 data set, and WSN-DS wireless network data set, the results demonstrate that FedAGRU increases the accuracy of detection by around 8% compared to other centralized learning approaches. Moreover, the cost of communication of FedAGRU achieves 70%, which is lower performance than other federated learning approaches.

B. FEDERATED LEARNING-BASED MALWARE DETECTION

There are billions of IoT devices without suitable protection measures which have been developed and deployed in the last few years. The susceptibility of these devices to malware has increased the requirement for effective detection technologies to identify devices that are compromised by malware inside the network. Taheri *et al.* [87] proposed an federated learning-based system, named Fed-IIoT, for android malware detection. To impersonate the environment of a poisoned sample, the Fed-IIoT system employs a generative adversarial network. The performance evaluation on three IoT datasets (the Contagio dataset, Drebin dataset, and Genome dataset) using different features show that the Fed-IIoT system performs significantly better than other local adversarial training mechanisms. To perform malware detection in cloud computing environments, Payne and Kundu [93] proposed a hierarchical approach towards deep federated defences. Their proposed approach formalized malware detection as a graph and hypergraph learning problem.

IV. FEDERATED LEARNING WITH BLOCKCHAIN

Blockchain is a decentralized, provenance-preserving, immutable ledger technique. It provides an efficient method to remove a central server that is prone to attacks in an untrusted computing environment [110], [111]. To alleviate the security problems that involve a central server in federated learning, the blockchain model can be integrated with the federated learning as shown in Fig 8 [112]–[118]. Tab. 5 presents works on blockchain and federated learning-based solutions for cyber security in IoT applications.

A. PERMISSIONED BLOCKCHAIN-BASED SOLUTIONS

The implementation of distributed multi-party data sharing in IoT applications is challenged by several issues. Based on permissioned blockchain, Lu *et al.* [106] developed a differential private multi-party data model sharing mechanism,

TABLE 5. Blockchain and federated learning-based solutions for cyber security in IoT applications.

FL-Blockchain system	Year	Blockchain model	FL technique	Consensus	(L), (T), (C)	(S), (Com), (Scal)	IoT application	(+) Pros (-) Cons
Lu *et al.* [18]	2021	Permissioned	Federated averaging	Delegated Proof of Stake (DPoS)	(L) Medium (T) High (C) Medium	(S) High (Com) Low (Scal) High	Digital Twin empowered 6G Networks	+ Minimize the time cost - Nothing-at-stake problem
Połap *et al.* [99]	2021	Permissioned	ADAM algorithm	N/A	(L) Medium (T) Low (C) High	(S) High (Com) Low (Scal) High	Internet of Medical Things (IoMT)	+ Parallel training of classifiers - The consensus algorithm is not defined
Li *et al.* [100]	2020	Permissionless	Federated averaging	Proof-of-work (PoW)	(L) High (T) Low (C) High	(S) High (Com) Low (Scal) Low	Crowdsourcing	+ Privacy preserving in crowdsourcing - Selfish mining is not considered
Liu *et al.* [101]	2020	Permissionless	Deep learning algorithms	N/A	(L) Low (T) High (C) Low	(S) High (Com) Low (Scal) Low	5G networks	+ Resist poisoning attacks as well as membership inference attacks - Vulnerable to Reputation-based attacks
Wang *et al.* [102]	2020	Permissionless	Convolutional networks (CNN)	Proof-of-work (PoW)	(L) High (T) Low (C) High	(S) High (Com) Low (Scal) Low	Edge computing	+ Prediction accuracy under attacks - Vulnerable to mining attacks
Rahman *et al.* [103]	2020	Permissioned	Deep learning applications	N/A	(L) Medium (T) Medium (C) High	(S) Medium (Com) Medium (Scal) Medium	Internet of Health Things	+ Supports differential privacy - Threat model and consensus algorithm are not defined
Połap *et al.* [104]	2020	Permissioned	Convolutional neural network	N/A	(L) Low (T) Medium (C) Low	(S) Medium (Com) High (Scal) Low	Internet of Medical Things	+ Removing centralized trust - Threat model is not defined
Sharma *et al.* [105]	2020	Permissionless	Recursive approach of federated learning	N/A	(L) Medium (T) Medium (C) Medium	(S) High (Com) Low (Scal) Low	Internet of Battle Things	+ An accuracy rate greater than 92.7 % - Threat model is not defined
Lu *et al.* [106]	2019	Permissioned	Gradient boosting decision tree	Proof of training Quality	(L) Low (T) High (C) Low	(S) High (Com) High (Scal) High	Industrial IoT	+ Removing centralized trust - High communication cost
Majeed *et al.* [107]	2019	Permissioned	Linear regression problem	Proof-of-Work (PoW)	(L) Low (T) High (C) Low	(S) High (Com) High (Scal) Low	Multi-access edge computing	+ Removing centralized trust - Vulnerable to mining attacks
Lugan *et al.* [108]	2019	Permissioned	Convolutional Neural Network	Federated Byzantine Agreement (FBA)	(L) High (T) High (C) Low	(S) High (Com) High (Scal) High	Medical application	+ Safeguards data privacy - Trust requirements
Doku *et al.* [109]	2020	Permissioned	Deep learning applications	Proof of Common Interest (PoCI)	(L) High (T) High (C) High	(S) Medium (Com) Medium (Scal) Medium	Edge-based IoT applications	+ AI services closer to the end-user - Threat model are not defined

(Com) Communication, (S) Storage, (C) Computation, (T) Throughput, (Scal) Scalability, (L) Latency

which is combined with federated learning. The proposed mechanism can reduce the threat of data leakage, which enables data owners to have more control over the access to stored and shared data. The simulation results on two real-world data sets (i.e., Reuters dataset and 20 newsgroups dataset) show that the proposed system can guarantee the quality of shared data as well as differential privacy.

To enhance the security of federated learning, Majeed and Hong [107] developed a blockchain-based solution, named FLchain, which can be applied in multi-access edge computing. The FLchain solution uses two ideas, namely, *1)* the channels for learning multiple global models and *2)* the global model state tree. Specifically, the aggregation of local model updates is updated and stored in the blockchain network.

Połap *et al.* [104] developed a privacy-preserving federated learning scheme, which is based on blockchain technology for securing the Internet of Medical Things. The use of the blockchain technology here provides security to updates of local data, which are critical for the aggregation of federated learning, and are derived from trusted devices with authenticity. Furthermore, the local updates can be stored as transactions in the blockchain network. The simulation results on the Tuberculosis Chest X-ray Image Data Sets with a convolutional neural network as a learning classifier show that the proposed scheme achieves an effectiveness average of 73,7%. Based on a multi-agent system, Połap *et al.* [99] developed a security architecture that combines the implementation of blockchain technology and federated learning

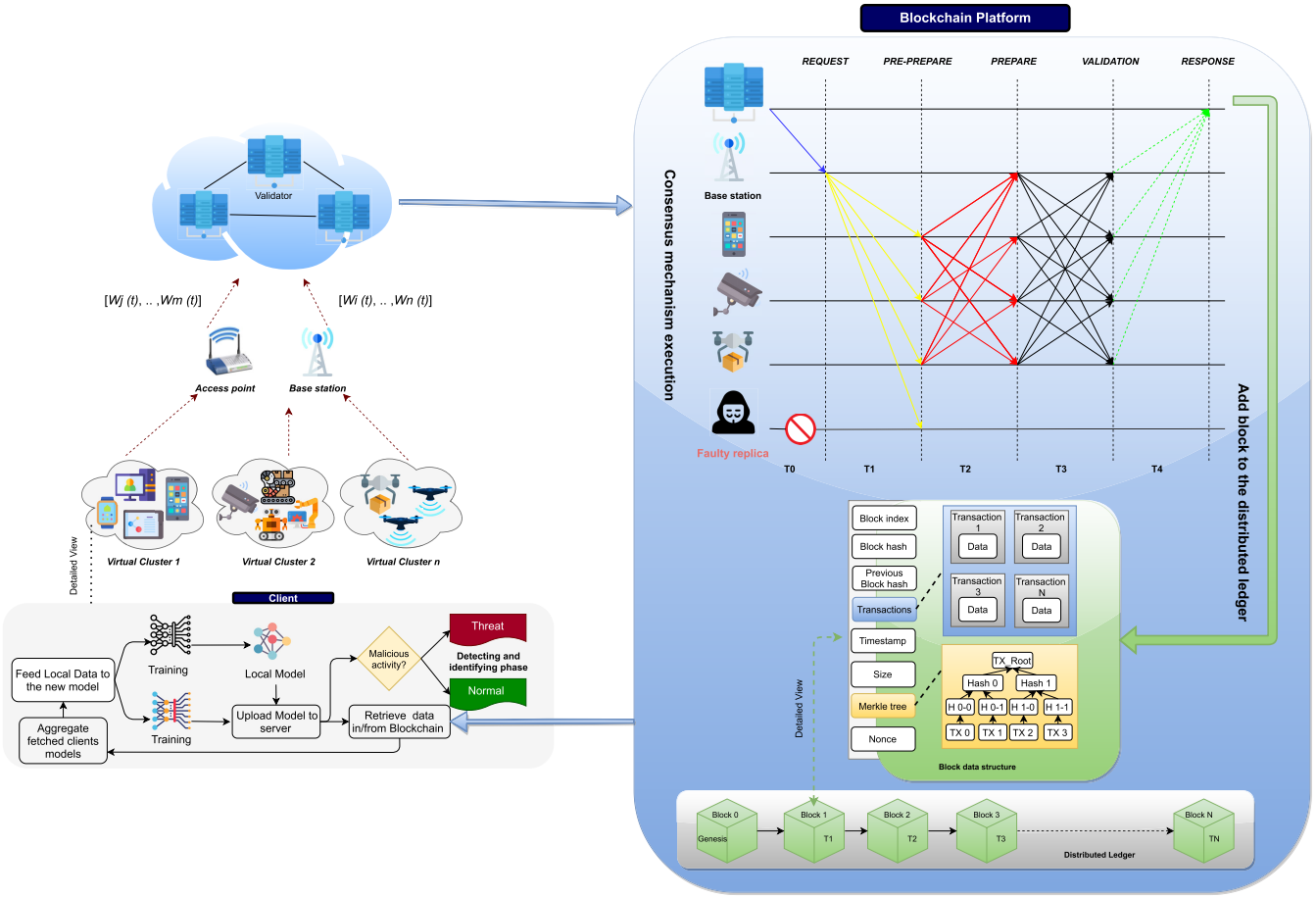


FIGURE 8. **Federated learning with Blockchain.**

for securing the Internet of Medical Things (IoMT). The proposed architecture enables separating specific tasks to agents units as well as sharing and protecting private data using blockchain technology. The performance evaluation on Skin Cancer MNIST dataset with the ratio of 70:30 between training and validating shows that the proposed architecture achieved an accuracy of 80 % for 25 iteration.

Lugan *et al.* [108] introduced a scalable security architecture by deriving a new paradigm of trusted coalitions with a high degree of trustworthiness which provides privacy-preserving of data as well as motivation for coalition participation in the absence of a central authority. The proposed architecture is based on permissioned blockchains, which enable deep learning that is distributed with rising degrees of security and privacy. Lu *et al.* [18] proposed a permissioned blockchain empowered federated learning scheme, using digital twins to support long-distance communication between edge servers and end users in edge computing. The performance evaluations on the CIFAR10 dataset show that the learning loss of the proposed scheme is improved through the optimization process.

Through a shared machine learning model, Doku *et al.* [109] proposed a federated learning scheme, named iFLBC, which is based on blockchain technology. The iFLBC scheme generates a shared model based on the aggregation of the trained models. The aggregated model is then used by IoT users to provide edge intelligence to end users. The Proof of Common Interest (PoCI) is used by the iFLBC scheme as a consensus algorithm to determine relevant data.

To perform authentication and trust management of federated nodes as well as the edge training model, Rahman *et al.* [103] introduced a hybrid lightweight federated learning platform that uses smart blockchain contracts for securing the Internet of Health Things (IoHT). Their platform is designed to enable inference process model learning, and the complete encryption of a dataset. Here a blockchain is used to aggregate the updated model parameters using multiplicative encryption, while the additive encryption operation is performed by each federated edge node.

Through a shared machine learning model, Doku *et al.* [109] proposed a federated learning scheme, named iFLBC, which is based on blockchain technology. The iFLBC scheme generates a shared model based on the aggregation of the trained models. The aggregated model is then used by IoT users for the provision of edge intelligence

to end-users. The Proof of Common Interest (PoCI) is used by the iFLBC scheme as a consensus algorithm to determine relevant data.

B. PERMISSIONLESS BLOCKCHAIN-BASED SOLUTIONS

The permissionless blockchains (aka. public blockchains) enable any person to perform operations and to join as a validator. Li *et al.* [100] introduced a crowdsourcing protocol, called CrowdSFL, which is based on federated learning and blockchain technology. The CrowdSFL protocol uses a re-encryption algorithm based on Elgamal to provide higher security with less overhead. The simulation results show that the proposed CrowdSFL protocol can resist the following malicious behaviors: Malicious miners, Malicious workers, and Malicious requesters. To resist poisoning attacks as well as membership inference attacks in 5G networks, Liu *et al.* [101] developed a blockchain-based federated learning protocol. The proposed protocol can provide privacy-preserving of data based on the local differential privacy technology. The performance evaluation using two datasets, including, MNIST dataset and CIFAR-10 dataset, show that the proposed protocol can deter poisoning attacks.

Wang *et al.* [102] proposed a secure decentralized multi-party learning scheme, named BEMA, for edge computing-based IoT applications. Specifically, each part in the BEMA scheme distributes their local model and during that time, they are processing the models received from other users about their local dataset and identify the models that require certification. According the BEMA scheme, the parties broadcasts the certification message to the corresponding parties. Based on the certification message, the system parties are not required to exchange their dataset with any other parties. The simulation results on the MNIST dataset show that the BEMA scheme is efficient in term of prediction accuracy under attacks compared to the baseline models.

Based on the features of blockchain technology and federated learning, Sharma *et al.* [105] proposed a distributed computing defence scheme for securing the Internet of Battle Things. The proposed system is composed of four different layers: data layer, edge layer, fog layer, and cloud layer. The performance evaluation shows that the proposed scheme achieved an accuracy rate of more than 92.7 %.

V. THREAT MODELS IN FEDERATED LEARNING

As federated learning is based on the collaborative action of all edge devices to build a machine learning model, a machine learning model can be faked when only a couple of edge devices are operating incorrectly [137]. Tab. 6 presents the vulnerabilities that can be exploited by adversaries in federated learning-based systems for IoT networks.

A. INFORMATION LEAKAGE

The problem of information leakage from collaborative deep learning is addressed by Hitaj *et al.* [120], where the authors proposed an attack to leverage the real-time quality of the learning operation which enables the adversary to train a generative adversary network (GAN) to create a set of targeted training patterns designed to be protected from the adversary. Based on the analysis of the privacy leakage of TernGrad [138], Dong *et al.* [51] proposed a secure and robust federated learning protocol, named EaSTFLy, which can be applied in IoT networks. The EaSTFLy protocol uses privacy-preserving technologies, namely, Paillier homomorphic encryption (PHE) and Shamir's threshold secret sharing (TSS) in order to solve arising privacy issues. The performance evaluation shows that the EaSTFLy protocol can resist against semi-honest adversaries using two datasets, including, MNIST and SVHN.

To train a deep neural network over a large dataset can consume significant time and resources. One popular approach to scaling is to fragment the training dataset, and simultaneously train different networks on each of these subsets and then share settings via a server of metrics. When training, a local model retrieves settings from the server, computes any required changes from its existing training dataset, and then sends these changes directly back to the server, which makes changes to the overall settings. Melis *et al.* [136] founded that the leakage of unintended features will expose collaborative learning to powerful inference attacks.

B. POISONING ATTACK

Poisoning attacks focus on degrading the accuracy of a machine learning model by falsifying the aggregation through the use of poisoned model updates, as shown in Fig 9. Tan *et al.* [137] categorized poisoning attacks using the sources of poisoned model updates into two types, namely, model poisoning and data poisoning. Data poisoning is performed by changing the training data in the damaged edge devices, while model poisoning uses some predefined rules to generates updates to the poisoned model. Zhao *et al.* [127] proposed a defense security system against poisoning attacks using the concept of generative adversarial networks. The proposed system removes adversaries using auditing data that is generated by generative adversarial networks. Based on microaggregation and Gaussian mixture models, Singh *et al.* [126] designed a security system, where the clients of the system self-identify as members of a minority group and advertise relevant features to their peers. Even with a low proportion of malicious edge servers, data poisoning attacks can significantly decrease recall and classification accuracy, as discussed by Tolpegin *et al.* [139]. Fang *et al.* [125] proposed a new idea to defend against the local model poisoning attacks based on two concepts, including, Reject on Negative Impact (RONI) and TRIM. The RONI consists of evaluates the influence of every training instance on the learned model's error rate and deletes the training instances that have a significant negative influence. Ma *et al.* [128] proposed a secure federated learning mechanism based on the trimmed optimization with multiple keys, which can resist a range of poisoning attacks. Taheri *et al.* [87] uses two concepts, including, Federated Generative Adversarial Network (FedGAN) and Generative

TABLE 6. The vulnerabilities that can be exploited by adversaries in federated learning-based systems for IoT networks.

Threat model	Definition	Scheme	Year	Proposed solutions
Adversarial attack	- Create additional training images to ensure that more of the space is covered - Generate adversarial attack data and attempting to classify these generated data - The generative adversary network (GAN) is composed of two components, including, 1) generator and 2) discriminator - The adversarial machine learning has two sub-fields: adversarial attack and adversarial defence [119]	Hitaj et al. [120]	2017	Differential privacy at different granularity
		Ibitoye et al. [121]	2019	The study uses two deep learning approaches, including, a typical Feed-forward Neural Network (FNN) and a Self-normalizing Neural Network (SNN)
		Hassan *et al.* [122]	2020	A robust decision boundary optimization approach
		Song et al. [123]	2020	The use of deep neural networks
		Qiu *et al.* [124]	2021	The use of saliency maps to identify the critical features
Differential attack	Privacy threat as the possibility of an individual entry being identified in a dataset	Yang et al. [48]	2021	Optimized federated soft-impute algorithm
		Lu et al. [55]	2020	Federated peer-to-peer vehicle learning that uses random updating of sub-pots with no conservators
Poisoning attack	An attacker inserts poisoned data samples within a training data set to increase the training classifier's error	Cetin et al. [96]	2019	Preventing the upload of unimportant data to the server
		Fang *et al.* [125]	2020	Based on two concepts, including, Reject on Negative Impact (RONI) and TRIM
		Singh *et al.* [126]	2020	Based on microaggregation and Gaussian mixture models
		Zhao *et al.* [127]	2020	Generate auditing data using generative adversarial networks
		Taheri *et al.* [87]	2020	Based two concepts, including, Federated Generative Adversarial Network (FedGAN) and Generative Adversarial Network (GAN)
		Ma et al. [128]	2021	Secure federated learning based on the trimmed optimization with multiple keys
		ur Rehman et al. [27]	2021	Enable decentralization using Ethereum blockchain and smart contract technology to detect the poisoning attacks
Privacy Leakage Attack	The attackers can deduce if an IoT device has been involved in some mission from their local model updates via differential attacks	Wang et al. [25]	2020	The use of three technologies, namely, blockchain, local differential privacy, and reinforcement learning
Jamming attack	The intruder's intention is to maliciously interrupt the victim network's conversation by interfering or colliding at the recipient's side	Mowla *et al.* [129]	2019	The application of dempster–Shafer theory-based client group prioritization technique
Privacy leakage Attack	The attackers can deduce if an IoT device has been involved in some mission from their local model updates via differential attacks	Wang *et al.* [25]	2021	The use of three technologies, namely, blockchain, local differential privacy, and reinforcement learning
Byzantine attack	An attacker distributes a local malicious model to other participants to modify the result of the classification of the max-model predictor	Wang *et al.* [102]	2020	Secure federated learning based on the blockchain technology
		Jebreel *et al.* [130]	2020	The concept is the analysis of a small fraction of the updates, instead of analyzing the whole updates
		Sun et al. [47]	2021	Adaptive federated learning with digital twin
Shilling attack	Shill attackers attempt to affect recommendation systems by producing many malicious profile users	iang *et al.* [131]	2020	Designing four novel features from the gradient matrices
Black-box attack	An adversary can access the deep learning networks' inputs and outputs but not the internal settings	Chen et al. [132]	2017	Ths use of zeroth order optimization
		Papernot et al. [133]	2017	To craft adversarial examples, the proposed work use the local substitute of the target model
Gray box attack	An adversary has partial information about the defensive system	Apruzzese *et al.* [134]	2020	Designing deep reinforcement learning approaches to protect botnet detectors from adversarial attacks
		Xu *et al.* [135]	2021	An improved classifier together with an attacking generator
Inference attack	Allow a malicious participant to infer membership and properties. The attacks is conducted by examining data to obtain illegitimate knowledge regarding a specific topic or database	Melis et al. [136]	2019	Learn only the features relevant to a given task
		Hao *et al.* [58]	2019	Privacy-enhanced federated learning scheme
		Liu et al. [54]	2020	Federated extreme gradient boosting (XGBoost) scheme
		Liu *et al.* [101]	2020	The local differential privacy technology

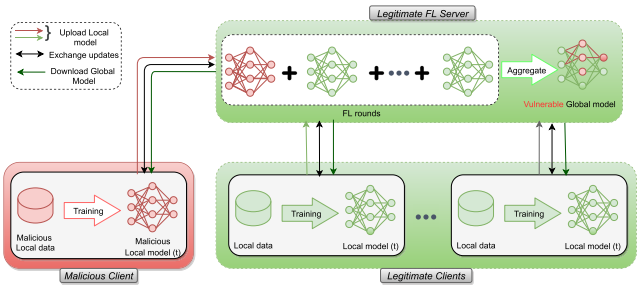


FIGURE 9. Poisoning attack in federated learning.

Adversarial Network (GAN), to create an architecture based on federated learning, named called Fed-IIoT. The proposed Fed-IIoT architecture can resist dynamic poisoning attacks in the server-side components.

C. JAMMING ATTACK

Adversaries can initiate a jamming attack against federated learning-based security and privacy systems where the intruder's intention is to maliciously interrupt the victim network's conversation by interfering or colliding at the recipient's side. Mowla *et al.* [129] proposed a security architecture using federated learning for the detection of cognitive jamming attack. Based on the Dempster–Shafer theory-based client group prioritization technique, the detection can be performed on the device while taking into account the unbalanced sensory data characteristics of the environment under training.

D. BYZANTINE ATTACK

An attacker distributes a local malicious model to other participants to modify the result of the classification of the max-model predictor. This attacker can induce errors in their local model update process. Wang *et al.* [102] designed a secure federated learning system based on blockchain technology that can defend against Byzantine attacks. Jebreel *et al.* [130] designed a novel concept against Byzantine attacks where the basic concept is the analysis of a small fraction of the updates, instead of analyzing the whole updates. Sun *et al.* [47] proposed adaptive federated learning with digital twin, which is based on the concept of interaction records and learning quality that rely on the use of malicious updates to mitigate the malicious data threat.

E. ADVERSARIAL ATTACK

When an adversary is able to compromise an IoT device without being detected, it can attempt to ''poison'' the system's training operation by falsifying packets as adversarial samples that are designed to influence the model's learning in a manner that prevents the malicious activity from being detected [140], [141]. Hitaj *et al.* [120] uses the differential privacy at different granularities against generative adversarial network. Song *et al.* [123] proposed federated defense against adversarial attacks using deep neural networks. Qiu *et al.* [124] proposed an adversarial attack against deep learning-based network intrusion detection systems to attack one state-of-the-art Kitsune [61]. The proposed attack uses saliency maps to identify the critical features. Therefore, Ibitoye *et al.* [121] showed the impact of adversarial samples on an intrusion detection system based on a deep learning approach in the environment of an IoT network. Specifically, the study uses two deep learning approaches, including, a typical Feed-forward Neural Network (FNN) and a Self-normalizing Neural Network (SNN). The performance results on the BoT-IoT dataset show that an intrusion detection system based on an FNN performs better than with SNN.

The concept of Generative Adversarial Network (GAN) was introduced by Goodfellow *et al.* [142], which is used by Hassan *et al.* [122] to generate adversarial attack data and attempting to classify these generated data. The GAN is composed of two components, including, 1) generator and 2) discriminator. Fig 10 illustrate GAN with FL-based IoT for cyber security [143]. To improve the reliability of the attack/non-attack detection system for a non-noisy as well as an adversarial setting, the authors proposed a robust decision boundary optimization approach. To train the downsampler, the proposed system uses a novel cooperative training algorithm, which provides an improved delivery for noisy examples with the real distribution. Throughout the performance evaluation on a SCADA dataset, the results show that the proposed system can classify with a binary cross-entropy loss score of 0.47 and an accuracy of 95.55 %.

Recently, Rosenberg *et al.* [144] proposed a taxonomy for the adversarial attacks in cyber security based on the following seven distinct attack characteristics:

- Attack's output: It indicates two types of attacks that aim to modify a feature's values, including, feature vector attack and end-to-end attack.
- Perturbed features: This characteristic of the attack consists of the features being added or modified.
- Attacker's goals: This characteristic of the attack consists of performing incorrectly the security goals such as authentication, confidentiality, privacy, integrity, and availability. . . etc.
- Attack's targeting: It indicates three types, including, label indiscriminate attack, label-targeted attack, and feature-targeted attack.
- Attacker's training set access: It indicates the type of the adversary's access to the training set used by the classifier.
- Attacker's knowledge: This characteristic of the attack is based on the amount of knowledge of the attacker regarding the classifier.
- Targeted phase: It indicates two phases, including, training phase attack and inference phase attack.

F. PRIVACY LEAKAGE ATTACK

In a distributed learning approach, the parameters of an updated local model on IoT devices can keep disclosing some

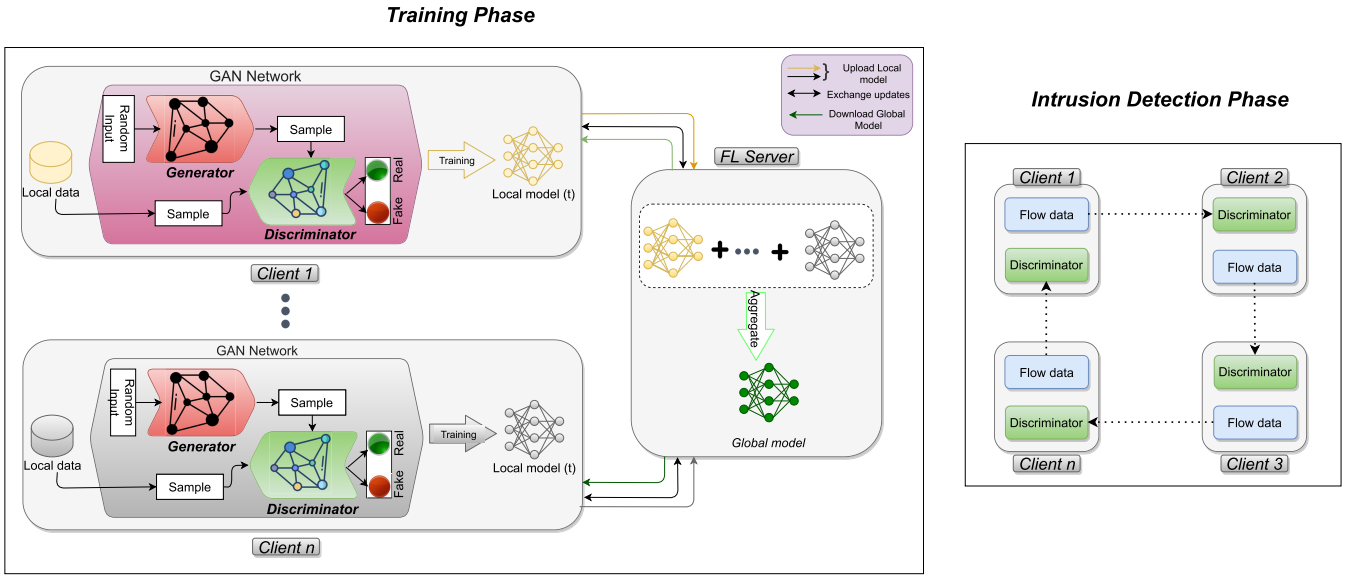


FIGURE 10. Generative Adversarial Network (GAN) with FL-based IoT for cyber security.

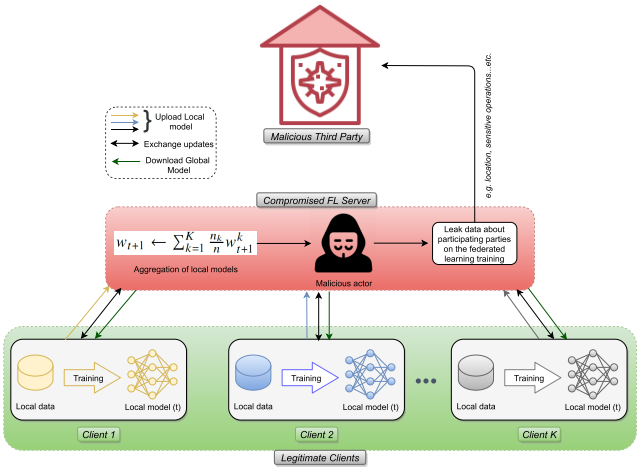


FIGURE 11. Privacy leakage attack in federated learning.

information regarding data that has been employed during training. Furthermore, the attackers can deduce if an IoT device has been involved in some mission from their local model updates via differential attacks. As each task has specified detection positions, the privacy of the location of the IoT devices involved can be leaked. To resist against such privacy leakage attack, Wang *et al.* [25] proposed a framework that uses three technologies, namely, blockchain, local differential privacy, and reinforcement learning. Fig 11 illustrates a privacy leakage attack in federated learning where a malicious actor compromises the aggregation server and leaks the data of participating entities.

G. SHILLING ATTACK

Shill attackers attempt to affect recommendation systems by producing many malicious profile users and rating target items with extreme ratings to increase or decrease their popularity. Jiang *et al.* [131] proposed a new idea about designing four features from the gradient matrices in order to detect shilling attackers. Specifically, the proposed idea train a semi-supervised Bayes classifier. The performance evaluation on two real-world datasets, namely, MovieLens and Netflix, demonstrates that the proposed idea can not only identify shilling hackers but also improve the performance of recommendations significantly.

H. INFERENCE ATTACK

An inference attack is a technique of data mining that is conducted by examining data to obtain illegitimate knowledge regarding a specific topic or database. Hao *et al.* [58] proposed a privacy-enhanced federated learning scheme that can ensure the privacy of training data during and after the training process as well as resist model inversion attacks and membership inference attacks. Liu *et al.* [54] proposed a federated extreme gradient boosting scheme that is based on differential privacy and homomorphism of the Paillier cryptosystem against the inference attack. Liu *et al.* [101] proposed secure federated learning for detection poisoning and membership inference attacks using the local differential privacy technology.

I. OTHER ATTACKS

There are other offensive strategies that can be used to attack ML models, such as white/black-box attacks, or even gray-box attacks. The black-box attacks only provide the ability to query the network's output or even have no network knowledge, while white-box attacks suppose that the attack target is available [119]. Gray box attacks train a generative model to produce adversarial examples and assume only access to the target model in the training phase [134], [135]. These three

methods are generally categorized as adversarial attacking methods.

VI. EXPERIMENTATION

We train three deep federated learning-based IDS models for cyber attack detection in IoT, namely Deep Neural Network (DNN)-based IDS model, Convolutional Neural Network (CNN)-based IDS model and Recurrent Neural Network (RNN)-based IDS model. Then, we compare the results with the classic/centralized versions of machine learning (non-federated learning).

A. EXPERIMENTAL SETUP

We performed our experiments on Google Colaboratory using well-known libraries, including NumPy, Pandas, TensorFlow, and Keras. There are different open-source federated learning frameworks that can be used for simulating and experimenting the federated learning algorithms, including, 1) Federated Learning and Differential Privacy (FL&DP) framework (developed by Sherpa.AI), 2) PySyft (developed by OpenMined), 3) Paddle Federated Learning (PFL) (developed by Baidu), 4) Federated AI Technology Enabler (FATE) (developed by Webank's AI department), and 5) TensorFlow Federated (TFF) (developed by Google Inc.). We chose the Sherpa.AI framework for its advantages compared to other frameworks [145]. The source code for the experimental evaluation of this article is available upon request.[1]

1) FEDERATED LEARNING PROCESS

In Fig 12 we illustrate the learning process applied in our deep federated learning based-IDS model. Alg. 1 shows a pseudo-algorithm for the steps taken to train the various client sets, which is adapted from [9]. At the beginning, a C fraction of K clients is picked by the aggregation server to join the FL workflow, and carry out computations for R federated learning rounds. The aggregation server produces a random generic model having a random set of initial weights w. Next, each client k retrieves the generic model from the aggregation server. Every client re-train the generic model with its private data locally and calculate a new local set of weights w^k_{t+1} for the freshly generated local model. The clients share the updated model. Then, the server aggregates the parameters of all clients ($\sum_{k=1}^{K} \frac{n_k}{n} w^k_{t+1}$). After that, the aggregation server sends the updated global model to the clients, where each client applies the updated parameters, to improve the global model. These steps are repeated until the model is converged.

B. DATASETS DESCRIPTION AND PRE-PROCESSING

Datasets are mandatory for training and evaluating IDSs in IoT networks. The selection of the appropriate datasets for a specific task is also of great importance. The datasets that can be used in the performance evaluation of FL approaches for IoT networks are reviewed in Tab. 7. There are three datasets, namely, MNIST [146], Fed. EMNIST [147], and

[1]https://github.com/Ferrag/FLCYBERSECURITYIOT

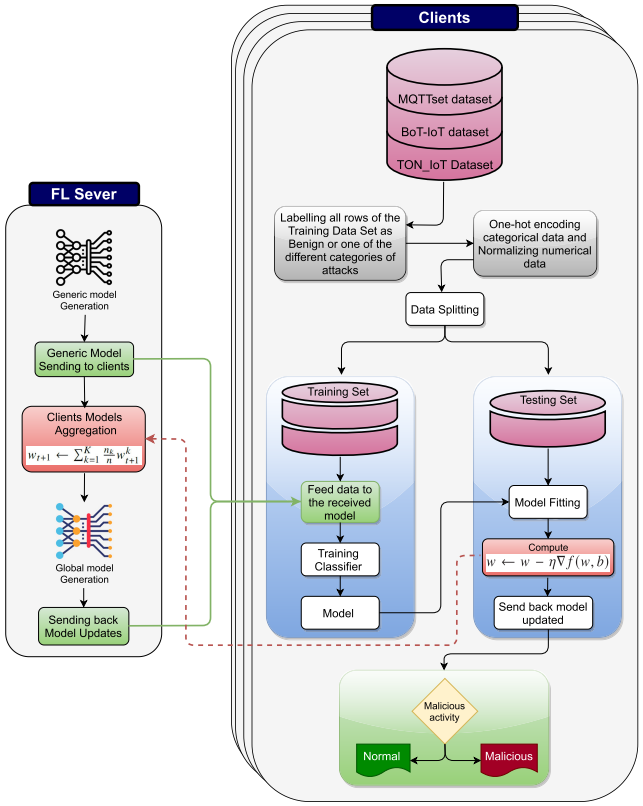


FIGURE 12. The architecture of our federated deep learning-based IoT intrusion detection system.

Algorithm 1: Federated Averaging

Server (K, C, R) :
  $w_1 \leftarrow GenericModel()$
  for $t = 1, .., R$ **do**
    $S_t \leftarrow$ Subset(max($C \cdot K$, 1), "*random*")
    Parallel.for $k \in S_t$ **do**
      $w^k_{t+1} \leftarrow Client(w_t, k)$
    end
    $w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w^k_{t+1}$
  end
Client (w, k) :
  $\mathcal{B} \leftarrow$ Split($\mathcal{P}, B$)
  for $i = 1, .., E$ **do**
    for $b \in \mathcal{B}$ **do**
      $w \leftarrow w - \eta \nabla f(w, b)$
    end
  end
  Send w to Server

CIFAR-10 [151] that can be used as real object classification tasks for evaluating adaptive FL for Industrial IoT. Therefore, these datasets are not suitable for evaluating federated learning-based IoT intrusion detection systems. Security researchers use cyber security datasets such as NSL-KDD [152] and CICIDS 2017-2018 [153] for the

TABLE 7. Datasets that can be used in the performance evaluation of FL approaches for IoT networks.

Dataset	Description	Studies	Fields	(+) Pros | (-) Cons
MNIST [146]	Constructed from the NIST Special Databases 1 and 3, featuring binary images of handwritten numbers and characters. The dataset includes huge handwritten data which are commonly used for training diverse Ai-based image processing systems.	Sun et al. [47]	IIoT cyber security	+ Can be used as real object classification tasks for evaluating adaptive FL for Industrial IoT. + It's adapted to simulate federated learning tasks on digit classification in an IoT environment. + Evaluate privacy-enhanced federated learning for IIoT. - The dataset is not appropriate for the evaluation of Blockchain empowered federated deep learning approaches for IoT and IIoT networks.
		Wang et al. [25]	Internet of Drones security	
		Hao *et al.* [58]	Industrial AI	
		Kong et al. [24]	Mobile Crowd Sensing	
Fed. EMNIST [147]	Constructed by partitioning the Extended MNIST data according to the author of the data.	Caldas *et al.* [148]	Evaluation frame-work	+ Can be used as a benchmark for federated settings. - It is not suitable for evaluating IoT security research since there are no attacks in the dataset.
TON_IoT [149]	Built from heterogeneous data sources gathered from IoT and IIoT sensor telemetry datasets.	Moustafa *et al.* [150]	Edge-based AI security	+ Determine the efficiency of federated learning-based IoT intrusion detection systems. - It's not adapted to simulate federated learning tasks on digit classification in an IoT environment.
Fed. TON_IoT [98]	Constructed from ToN_IoT with the involvement of federated data sources collected from IoT service telemetry datasets.	Moustafa *et al.* [98]	AI-Based Security	+ Suitable for evaluating federated learning-based cyber security solutions. - The main limitation of this dataset is that it does not include digit classification for simulate federated learning tasks compared to Fed. EMNIST [147].
CIFAR-10 [151]	Contains 60,000 color images divided into 10 classes, with each class having 6K images. There are 50K training images and 10K test images.	Liu *et al.* [101]	Blockchain-based FL protocol	+ Extensive use by the research community due to ease of use and support for a variety of ML and FL based frameworks. - It is not suitable for evaluating federated learning-based IoT intrusion detection systems.
		Lu *et al.* [18]	Edge Network Optimization	
NSL-KDD [152]	Proposed to address some of the issues related to the KDD'99 dataset [152]. It includes several categories of attacks, including probing, DoS and user to root.	Rahman *et al.* [91]	FL-based IoT cyber security	+ Suitable for evaluating FL-based cyber security solutions. - Does not contain IoT and IIoT traffic. In addition, it is obsolete in the age of IoT networks (i.e., Fog, Edge, Cloud, Virtualization, 6G...etc.).
		Al-Marri *et al.* [89]	FL-based IDS	
CICIDS 2017-2018 [153]	Consists of labeled real network traffic, including complete packet payloads. Used for evaluating IDSs with an emphasis on network-based anomaly detectors.	Cetin *et al.* [96]	FL-based IDS	+ Determine the efficiency of federated learning-based intrusion detection systems. + Suitable for evaluating federated learning-based cyber security solutions. - It's not adapted to simulate federated learning tasks in an IoT environment.
		Chen et al. [88]	Wireless Edge Networks Security	
Bot-IoT [154]	Was achieved by engineering a real-world network setting in the Cyber Range Lab at UNSW Canberra. It consists of real network traffic for a mixture of normal traffic and botnet traffic.	Ibitoye *et al.* [121]	IoT-based IDSs security	+ The dataset is supplied in different formats (pcap, csv), and have been partitioned, by attack category and subcategory, which further facilitates FL-based assessments. + A lightweight version of the dataset (5% of the original) is also provided to facilitate the learning and testing process. - The main limitation of this dataset is that it does not include the different types of IoT applications.
		Huong *et al.* [86]	FL-based IDS IoT	
		Popoola *et al.* [155]	Zero-Day Botnet IoT Detection	
MQTTset [156]	Consists of network traffic of MQTT protocol, for a combination of normal traffic and attack traffic.	Vaccari *et al.* [156]	IoT-based Protocol Security	+ Due to the lack of IoT protocol-specific datasets, this dataset helps researchers evaluate their FL-based IDSs in the context of IoT protocol security. - Only applicable to MQTT-based protocols.
N-BaIoT [157]	Generated by using the traffic generated by nine heterogenous commercial IoT devices, either infected with botnet and malware attacks, or clean.	Reya *et al.* [158]	FL-based IoT Malware Detection	+ Incorporate malicious traffic from two of the most popular IoT-based malwares: Mirai and BASHLITE. + Proper combination with FL-based IoT IDS due to the distributed nature of botnets. - The threat model is limited to botnets and malware attacks.
		Popoola *et al.* [155]	Zero-Day Botnet IoT Detection	

TABLE 8. Datasets description for experimental evaluation.

Dataset	Flow Type	Count	Training	Testing
Bot-IoT	Benign	477	370	107
	DDoS	+1.9M	154131	38530
	DoS	+1.6M	132014	33011
	Reconnaissance	91082	72919	18163
	Theft	79	65	14
MQTTset	Benign	165463	115824	49639
	DoS	130233	91156	39077
	Brute Force	14501	10150	4351
	Malformed	10924	7646	3278
	SlowITe	9202	6441	2761
	Flood	613	429	184
TON_IoT	Benign	35000	28000	7000
	Password	5000	4000	1000
	Backdoor	5000	4000	1000
	Injection	5000	4000	1000
	XSS	577	461	116
	Scanning	529	423	106

performance evaluation of federated learning-based intrusion detection systems [159]. These two datasets does not contain IoT and IIoT traffic. In addition, NSL-KDD [152] is obsolete in the age of IoT networks (i.e., Fog, Edge, Cloud, Virtualization, 6G…etc.). For evaluating FL-based cyber security solutions in IoT networks, the security research community uses the following three datasets: TON_IoT [149], Bot-IoT [154], and MQTTset [156]. They are chosen specifically because they are build from heterogeneous data sources as well as collected from IoT and IIoT sensor telemetry datasets.

FL-based tasks require the data distribution to be Non-Independent and Identically Distributed (Non-IID) and unbalanced, which reflects the properties of the real-world scenario. However, due to the lack of FL-specific datasets, any pre-existing public dataset with engineered partitions can be used to mimic data federations, as employed in our experiment. Based on the datasets review presented in Tab. 7, we selected and used three real traffic IoT-based datasets, namely: BoT-IoT dataset, MQTTset dataset, and TON_IoT dataset. Tab. 8 provides a list of flow types and sample counts for each dataset. Description and pre-processing of each dataset is as follows:

1) BoT-IoT DATASET

The BoT-IoT dataset was produced at the Cyber Range Lab at UNSW Canberra as a result of building a real-life network environment integrating a mix of normal and botnet traffic [154], [160]–[164]. All 69.3 GB captured PCAP files with over 72 million records. The dataset is available in a variety of file formats, including PCAP, generated argus files, as well as CSV files. We used the CSV files for our experimental evaluations. The dataset includes various types of cyber attacks including:

- *DDoS & DoS attacks:* The purpose of these attacks is to make services inaccessible to legitimate users by using a group of compromised bot-nets. Both DDoS, DoS for TCP and UDP attacks were carried out using the Hping3 tool.
- *Reconnaissance:* or probing attacks, which is a type of malicious behavior that collects user data by scanning remote systems. The dataset contains two types of such attacks, namely: port scanning using Hping3, and operating system fingerprinting using Nmap and Xprobe2 tools.
- *Theft:* The objective of these cyber attacks is to compromise sensitive data. The dataset contains two types of such attacks, namely Keylogging and Data theft attacks, both of which are carried out using the Metasploit framework.

After dropping missing values, we also dropped the *'pkSeqID'*, *'saddr'*, *'sport'*, and *'daddr'* features in order to prevent overfitting, we encoded the *'proto'* feature' with one-hot encoding. Then, we normalized other numerical features with the *Z-Score* normalization strategy as follows:

$$z = \frac{x - \mu}{\sigma} \tag{1}$$

where, x denote the value of the feature, μ denote the mean, and σ denote the standard deviation.

2) MQTTset DATASET

introduced by *Vaccari et al. [156]* to address the lack of support for specific protocols that IoT environments are currently using. It consists of Message Queue Telemetry Transport (MQTT) protocol-based traffic between various IoT devices to imitate a smart IoT environment. It comprises real-world attacks tailored to target the IoT environment, including:

- *DoS:* This attack was conducted using the MQTT-malaria tool
- *Brute Force:* The approach to this type of attack is to try to recover the user credentials used by MQTT using the MQTTSA tool.
- *Malformed data:* this type of attack is designed to trigger several malformed packets and send them to the broker, attempting to raise exceptions on the selected service.
- *SlowITe:* the Slow DoS against IoT Environments attack is a new DoS approach that targets the MQTT protocol, which generates a huge number of connections to the MQTT broker.
- *MQTT Publish Flood:* This approach seeks to overload the system by using a unique connection rather than instantiating multiple connections using the IoT-Flock tool.

3) TON_IoT DATASET

This dataset is introduced by the IoT Lab of the UNSW Canberra Cyber, the School of Engineering and Information technology (SEIT), UNSW Canberra at the Australian Defence Force Academy (ADFA) [150] for the collection and analysis of mixed data sources from IoT and Industrial IoT (IIoT). The benchmark was conducted using several virtual machines that included multiple operating systems to address the cross-layer connectivity between the three tiers: IIoT,

TABLE 9. Settings for deep learning classifiers.

Classifier	Parameter	Value	Motivation
DNN	Hidden nodes	25-60	The balance between neurons with the appropriate number of hidden layers leads to a better efficiency.
	Hidden layers	2	
CNN	Convolutional layers	2 Conv1D	Convolution layers, filters, and pooling layers apart from the neurons, significantly reduce the number of trainable parameters as compared to fully connected networks. By using several such processes, it is possible to train the model for the most complex objectives.
	Filters	18-26	
	Kernel size	3	
	Pooling layers	1 *Global Average Pooling 1D*	
	Hidden nodes	39-60	
	Hidden layers	2	
RNN	Hidden nodes	22-60	The model can handle inputs of any given length, as the model size doesn't increase with the input size.
	Hidden LSTM layers	2	
*	Batch size	1000	For each model, the activation function is *ReLu*, the output layer is SoftMax since there is a multi-class classification, the loss function is *categorical_crossentropy*, and the optimization process is *Adam*. To prevent overfitting, we used two methods: dropout and L_2 regularization. In order to ensure that each device gains knowledge before sharing it with its peers, we used one FL global epoch and 50 local epochs.
	Local epochs	1	
	Global epochs	50	
	Dropout	0.1	
	Learning rate	0.01-0.5	
	Regularization	L_2	
	Loss function	*categorical_crossentropy*	
	Activation function	*ReLu*	
	Classification function	*SoftMax*	
	Optimizer	*Adam*	

Cloud, and Edge/Fog systems. Parallel processing was used to assemble the datasets to gather diverse benign and attack traffic, for IoT telemetry data service. It includes different attacking techniques, such as:

- *Password Cracking:* This type of attack is intended to allow the attacker to overcome authentication schemes in order to compromise the IIoT devices. It was conducted using CeWL and Hydra toolkits.
- *Backdoor:* With this kind of attack, it is possible for attackers to obtain non-authorized remote access to IIoT devices affected by a backdoor malware. The framework used for these attacks is the Metasploitable3 framework.
- *Injection:* With this attack, the adversary aims to inject malicious data into the IIoT applications.
- *XSS:* the adversary frequently tries to run malicious commands in IIoT applications through a web server.
- *Scanning:* scanning tools, such as Nmap and Nessus tools, allow the attacker to perform scanning attacks against the IoT/IIoT devices and MQTT broker in a public network.

To prevent overfitting, we dropped the *'date'* and *'saddr'* features. Then, we used the *Z-Score* normalization strategy for numerical features.

C. USE CASES AND PERFORMANCE METRICS

For the purpose of evaluating our experiment, we employed two use cases, namely:

- *Centralized learning approach:* The data is located at a single location with three well-known deep learning classifiers, i.e., DNN, CNN, and RNN.
- *Federated learning approach:* The data is located across different clients, and an aggregation server is used to aggregate the models of the clients. We used also the same classifiers as in the previous approach.

We used three sets of client distributions: $K = 5$, $K = 10$, and $K = 15$, with two data distribution methods: 1) independent and identically distributed (IID) and 2) non-independent and identically distributed (Non-IID), over 50 federated learning rounds. Tab. 9 shows the different parameters used in the three deep learning models for the centralized and federated learning approaches.

When conducting intrusion detection performance analysis, the most common metrics used are:

- *True Positive (TP)*: is used to determine the number of attack patterns that are properly classified as attacks.
- *False Positive (FP)*: is used to determine the number of normal patterns that are wrongly classified as attacks.
- *True Negative (TN)*: is used to determine the number of normal patterns that are proportion classified as normal.
- *False Negative (FN)*: is used to determine the number of attack patterns that are wrongly classified as normal.
- *Accuracy*: is used to determine the proportion of correct classifications to the total number of entries, which is given by:

$$\frac{TP + TN}{TP + TN + FP + FN} \tag{2}$$

- *Precision*: denotes the proportion of correct intrusion classes to the total amount of predicted intrusion results, which can be given by:

$$\frac{TP}{TP + FP} \tag{3}$$

- *Recall*: denotes the proportion of proper attack classifications relative to the overall count of all samples that ought to have been identified as attacks, it is given by:

$$\frac{TP}{TP + FN} \tag{4}$$

TABLE 10. The evaluation results of centralized learning approaches.

		Precision			Recall			F_1-Score		
Dataset	**Class**	**DNN**	**CNN**	**RNN**	**DNN**	**CNN**	**RNN**	**DNN**	**CNN**	**RNN**
Bot-IoT	Benign	100%	100%	100%	100%	100%	100%	100%	100%	100%
	DDoS	97%	95%	97%	94%	97%	95%	96%	96%	96%
	DoS	94%	97%	95%	96%	93%	97%	95%	95%	96%
	Reconnaissance	96%	97%	99%	99%	99%	99%	97%	98%	99%
	Theft	00%	00%	100%	00%	00%	36%	00%	00%	53%
MQTTset	Benign	92%	91%	91%	94%	94%	94%	93%	93%	93%
	DoS	91%	90%	90%	89%	89%	89%	90%	90%	90%
	Brute Force	69%	69%	66%	84%	86%	86%	76%	76%	75%
	Malformed	80%	86%	80%	39%	30%	20%	52%	45%	32%
	SlowITe	98%	97%	100%	100%	96%	93%	99%	96%	96%
	Flood	82%	89%	100%	35%	48%	03%	61%	50%	05%
TON_IoT	Benign	100%	100%	100%	100%	100%	100%	100%	100%	100%
	Injection	100%	100%	100%	100%	100%	100%	100%	100%	100%
	Backdoor	100%	100%	100%	100%	100%	100%	100%	100%	100%
	Password	97%	90%	100%	100%	100%	100%	98%	95%	100%
	XSS	100%	00%	100%	72%	00%	100%	83%	00%	100%
	Scanning	100%	100%	100%	100%	100%	100%	100%	100%	100%

- F_1-Score: reports the Harmonic Mean between Precision and Recall, which is given by:

$$2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \tag{5}$$

D. EXPERIMENTAL RESULTS

The outcomes achieved from both experimental use cases are as follows:

1) CENTRALIZED LEARNING MODELS

Fig 13 presents the accuracy of deep learning techniques (DNN, CNN, and RNN) in multiclass classification for the three datasets (Bot-IoT, MQTTset, and TON_IoT). The highest accuracy for the Bot-IoT dataset was obtained using the RNN classifier which achieved 96.76%, while the lowest accuracy was obtained using the DNN classifier with 95.76%. For the MQTTset dataset, the highest accuracy was obtained using the DNN classifier which achieved 90.06%, while the lowest accuracy was obtained using the RNN classifier with 89.29%. The highest accuracy for the TON_IoT dataset was obtained using the RNN classifier which achieved 99.98%, while the lowest accuracy was obtained using the CNN classifier with 98.87%.

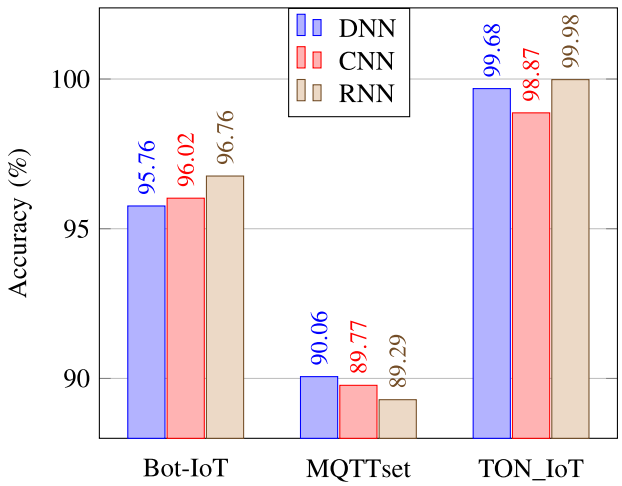


FIGURE 13. Centralized model performance.

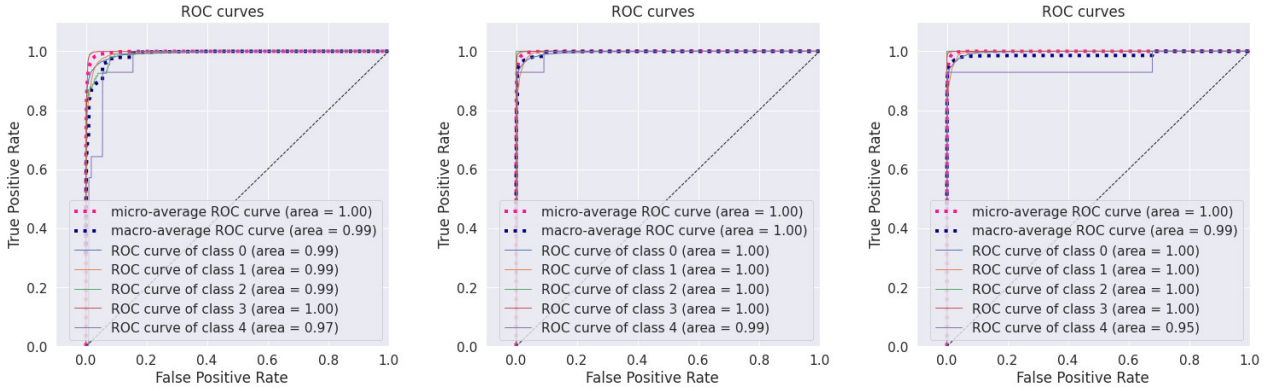
Tab. 10 provides the obtained centralized model results of deep learning techniques in terms of Precision, Recall, and F_1-score under multi-class classification, which reports the performance of the different models against the different benign and attack classes in the three datasets.

Fig 14 presents the Receiver Operating Characteristic (ROC) curves for five classes in the BoT-IoT dataset, namely: class DDoS, class DoS, class Benign, class Reconnaissance, and class Theft. All values are between 0.99 and 1.00. Fig 15 presents the ROC curves for five classes in the MQTTset dataset, namely: class Bruteforce, class DoS, class Flood, class Benign, and class Slowite. All values are between 0.94 and 0.98. Fig 16 presents the ROC curves for five classes in the TON_IoT dataset, namely: class Backdoor, class Injection, class Benign, class Password, and class Scanning.

2) FEDERATED LEARNING MODELS

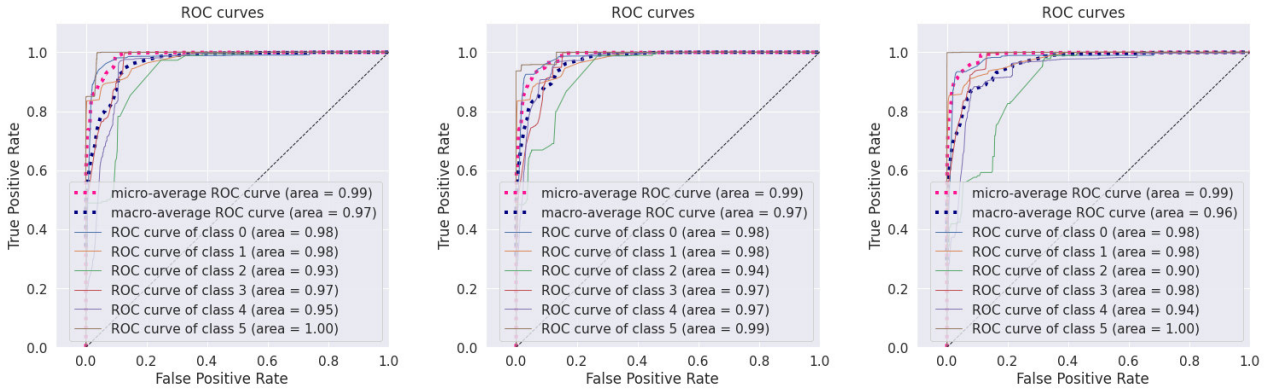
In this experimental setup rather than locating all data in one location and conducting the learning from there, a federated deep learning approach is used, where the data never leaves the client side along with the shared knowledge that goes back and forth between the aggregation server and the participating clients.

Fig 17 report the validation accuracy for each global model against the centralized model across all datasets and all classifiers. Fig 17 (a) plots the validation accuracy achieved by the federated deep learning classifiers (DNN, CNN, RNN) with both the IID and Non-IID data distribution strategies for the Bot-IoT dataset. For the IID data distribution strategy, the federated deep learning global models were able to approximate the performance of the centralized learning models. For the non-IDI data distribution strategy, the global



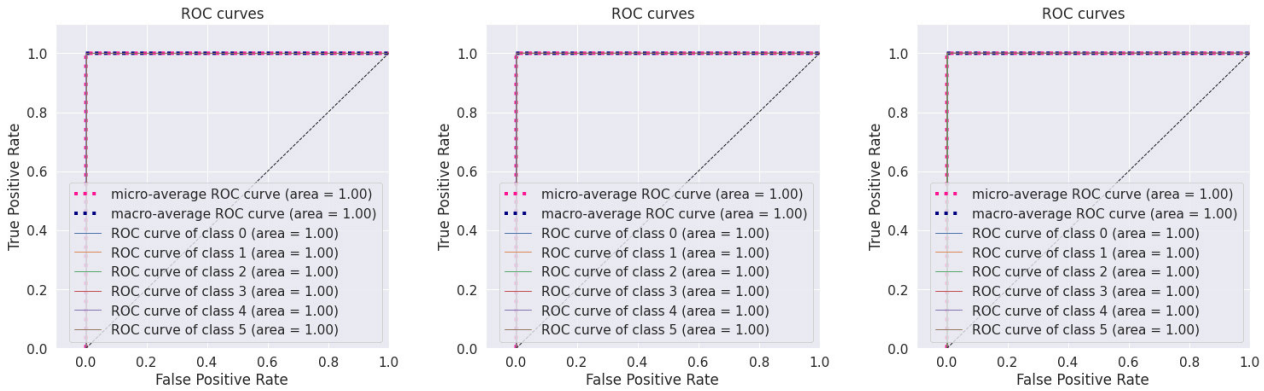
(a) DNN (b) CNN (c) RNN

FIGURE 14. The Receiver Operating Characteristic (ROC) curves for BoT-IoT dataset. (class 0: DDoS, class 1: DoS, class 2: Benign, class 3: Reconnaissance, class 4: Theft.)



(a) DNN (b) CNN (c) RNN

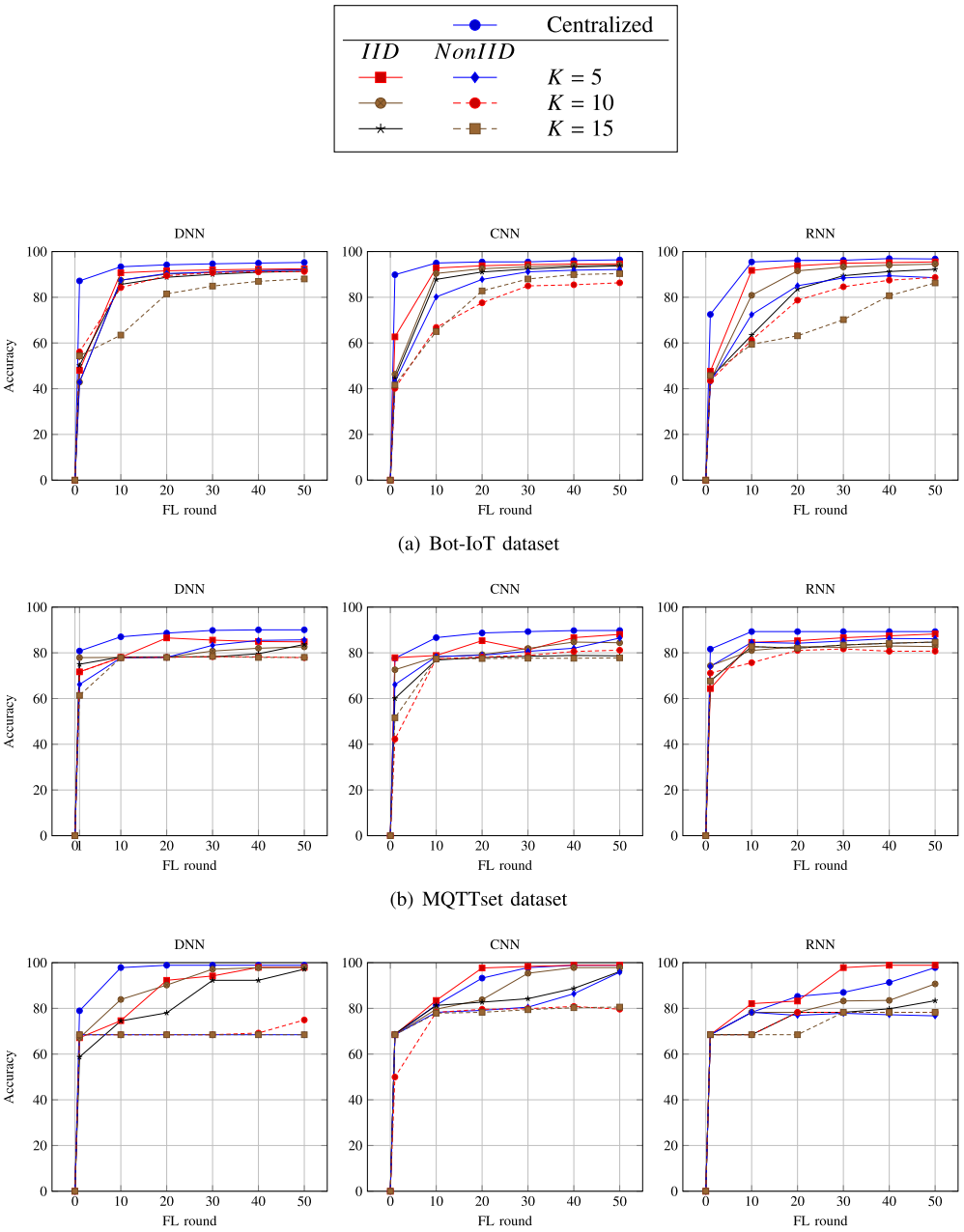
FIGURE 15. The Receiver Operating Characteristic (ROC) curves for MQTTset datasets. (class 0: Bruteforce, class 1: DoS, class 2: Flood, class 3: Benign, class 4: Slowite, class 5: Malformed.)



(a) DNN (b) CNN (c) RNN

FIGURE 16. The Receiver Operating Characteristic (ROC) curves for TON_IOT dataset. (class 0: Backdoor, class 1: Injection, class 2: Benign, class 3: Password, class 4: Scanning, class 5: XSS.)

models struggled a bit to perform the same as in IID, which is quite normal since the data samples were randomly distributed for all clients, however after 50 FL runs, the overall performance was pretty good. Fig 17 (b) and Fig 17 (c) illustrate the validation accuracy obtained by the federated deep learning classifiers with the IID and Non-IID data distribution



(a) Bot-IoT dataset

(b) MQTTset dataset

(c) TON_IoT dataset

FIGURE 17. **Learning performances.**

strategies for the MQTTset and TON_IoT datasets, respectively. Similar to the first data set, the same observations apply to these two experiments.

Tab. 11 present a detailed side-by-side comparison of all accuracies obtained by all global models and the highest/lowest accuracy of the best/worst clients couple in every set, across the first and the 50^{th} round of federated deep learning. The first observation is that in the IID data distribution strategy, the **B**est, **W**orst, and **G**lobal models are closely related to each other consistently across all settings and datasets, even though the clients are trained from different class samples. The reason being that all clients can learn from all classes. The second observation is that at the 50^{th} rounds of federated deep learning, the performance of all global models managed to approach the performance of the centralized model.

In the Non-IID case, at the first FL round, the **B**est, **W**orst, and **G**lobal models are nowhere near one another, and this is quite expected since not all clients were trained from all classes. A good example is a Bot-IoT dataset, with the CNN classifier, where K=15, the worst accuracy of the client was 01.00%, but with 50^{e} of federated deep learning rounds, this

TABLE 11. The evaluation results of federated deep learning approaches.

		1^{st} round							50^{th} round					
			IID			Non IID			IID			Non IID		
Dataset	Classifier	Clients	B	W	G	B	W	G	B	W	G	B	W	G
Bot-IoT	DNN	$K = 5$	48.12%	45.71%	48.04%	54.17%	42.89%	42.89%	92.80%	92.24%	92.49%	91.76%	61.29%	91.98%
		$K = 10$	42.89%	42.89%	42.89%	56.59%	20.22%	56.12%	92.20%	91.83%	92.03%	90.99%	56.18%	91.28%
		$K = 15$	51.33%	48.80%	50.21%	60.31%	20.32%	54.37%	91.55%	90.92%	91.39%	87.65%	63.48%	88.03%
	CNN	$K = 5$	63.22%	62.21%	62.69%	64.23%	36.75%	42.89%	94.75%	94.36%	94.61%	93.19%	48.13%	89.91%
		$K = 10$	47.42%	45.83%	46.34%	42.89%	20.22%	40.17%	94.08%	93.70%	94.06%	89.88%	48.54%	86.34%
		$K = 15$	53.74%	42.89%	44.54%	64.85%	01.00%	41.61%	93.89%	93.08%	93.74%	90.59%	52.98%	90.35%
	RNN	$K = 5$	47.81%	47.51%	47.68%	60.90%	42.89%	42.92%	95.38%	95.29%	95.47%	92.96%	65.64%	88.56%
		$K = 10$	44.10%	42.92%	43.44%	51.06%	40.08%	43.48%	94.51%	94.39%	94.50%	89.58%	63.96%	88.67%
		$K = 15$	47.24%	42.92%	44.70%	44.74%	20.24%	45.76%	92.59%	91.74%	92.24%	85.92%	64.68%	86.28%
MQTTset	DNN	$K = 5$	76.02%	69.36%	71.68%	71.87%	38.75%	66.17%	85.71%	80.23%	84.81%	83.03%	41.36%	85.68%
		$K = 10$	77.85%	68.65%	77.91%	77.60%	04.20%	71.64%	82.86%	82.27%	82.60%	78.30%	25.99%	77.88%
		$K = 15$	77.98%	71.57%	75.01%	68.35%	20.46%	61.37%	83.94%	80.58%	83.68%	78.42%	45.06%	78.03%
	CNN	$K = 5$	77.89%	71.79%	77.87%	73.52%	39.35%	66.09%	88.01%	83.09%	88.06%	86.08%	39.41%	86.45%
		$K = 10$	76.23%	67.19%	72.60%	63.55%	17.54%	42.25%	84.91%	84.00%	84.40%	80.91%	46.11%	81.16%
		$K = 15$	60.67%	57.01%	60.05%	68.81%	04.13%	51.59%	79.01%	78.63%	78.68%	78.01%	57.48%	77.80%
	RNN	$K = 5$	64.56%	63.65%	64.36%	76.11%	49.99%	74.10%	88.47%	87.45%	88.23%	86.04%	83.91%	86.16%
		$K = 10$	75.33%	73.33%	74.34%	77.24%	03.96%	71.13%	83.81%	81.60%	82.73%	84.59%	42.46%	80.73%
		$K = 15$	71.51%	66.47%	67.69%	70.98%	03.69%	39.01%	85.23%	83.24%	84.69%	83.82%	44.56%	70.47%
TON_IoT	DNN	$K = 5$	67.15%	67.11%	67.15%	68.47%	09.78%	68.47%	97.96%	96.64%	97.95%	68.47%	68.47%	68.47%
		$K = 10$	67.11%	67.11%	67.11%	68.47%	09.78%	68.47%	98.03%	94.48%	97.95%	75.39%	74.88%	74.93%
		$K = 15$	58.72%	58.72%	58.72%	68.47%	09.78%	68.47%	96.59%	86.74%	97.16%	68.47%	68.47%	68.47%
	CNN	$K = 5$	68.47%	68.47%	68.47%	68.47%	68.47%	68.47%	98.86%	98.86%	98.86%	96.46%	70.65%	95.82%
		$K = 10$	68.47%	68.47%	68.47%	68.47%	08.45%	49.96%	98.62%	97.77%	97.86%	80.13%	78.26%	79.63%
		$K = 15$	69.50%	68.63%	68.90%	68.47%	10.13%	68.47%	96.83%	93.05%	96.10%	80.63%	78.26%	80.57%
	RNN	$K = 5$	68.47%	68.47%	68.47%	68.47%	09.78%	68.47%	98.86%	98.86%	98.86%	82.08%	78.26%	76.72%
		$K = 10$	68.47%	68.47%	68.47%	68.47%	03.53%	68.47%	92.90%	88.04%	90.70%	78.26%	78.26%	78.26%
		$K = 15$	68.47%	68.47%	68.47%	68.47%	09.78%	68.47%	84.85%	79.90%	83.35%	78.26%	78.26%	78.26%

(**B**): **B**est client accuracy; (**W**): **W**orst client accuracy; (**G**): **G**lobal model accuracy;

same client has an accuracy of 52.98% and the global model achieved 90.35%. This means that this client was able to benefit from the federated learning approach even though it has very limited knowledge of the attack classes in its local private data.

3) COMPARISON

The centralized intrusion detection approaches are capable of detecting intrusions with high accuracy. However, there are problems with these practices. First, and most importantly, privacy issues, since it requires data to be collected at a single entity, thus making it easier for an attacker to target a single location for all data, if that single entity is compromised, all sensitive data will be breached. Second, given the huge flow of data coming from the end devices to that single entity, latency, and processing is major concerns that must be addressed.

Federated learning-based intrusion detection systems, on the other hand, significantly decrease the previous issues with decent detection accuracy, and in many cases, it approached the performance of a centralized approach as we showed with our federated deep learning models. Furthermore, by taking into account that the field of federated learning is in its developmental stage, we expect that in the future, federated learning will replace centralized and traditional learning approaches in many machine learning-based domains, especially in areas where data privacy is a real concern.

VII. IMPORTANCE OF THE STUDY AND OPEN CHALLENGES

Federated learning is an emerging research area that is still in its developmental stage. Although it has a lot of potential in different IoT-based application areas, the practical implementation of federated learning presents several open challenges, as discussed below.

A. IMPORTANCE OF THE STUDY

1) IoT APPLICATIONS

The study shows that the federated deep learning-based security and privacy systems can be applied for several types of IoT applications, including, Industrial Internet of Things, Edge Computing, Internet of Drones, Internet of Healthcare Things, Cloud Computing, 5G-enabled IoT, Internet of Vehicles, Mobile Crowdsensing, etc.

2) INTRUSION AND MALWARE DETECTION

The study presents the importance of using federated deep learning by intrusion detection systems and malware detection systems as a decentralized machine learning approach for detecting cyber security attacks in IoT networks.

3) WHEN FEDERATED LEARNING MEETS BLOCKCHAIN

The study shows that blockchain technology can be integrated with federated deep learning for cyber security in IoT networks. This combination reduces the threat of data leakage and enables data owners to have more control over the access to stored and shared data.

4) VULNERABILITIES OF FEDERATED DEEP LEARNING

The study presents the importance of defending against the vulnerabilities that can be exploited by adversaries in federated deep learning-based systems for IoT networks. These adversaries can use cyber security attacks such as adversarial attacks or poisoning attacks to degrading the accuracy of a

machine learning model or deduce if an IoT device has been involved in some mission from their local model updates.

5) FEDERATED DEEP LEARNING VERSUS CLASSICAL MACHINE LEARNING

The primary motivation for conducting this study was to investigate the effectiveness of federated deep learning versus conventional machine learning for cybersecurity in IoT networks. Based on the performance evaluation under three new real IoT traffic datasets, namely, the Bot-IoT dataset, the MQTTset dataset, and the TON_IoT dataset, the study demonstrates that federated deep learning approaches (i.e., CNN, RNN, and DNN) outperform the classic/centralized versions of machine learning (non-federated learning) in assuring the privacy of IoT device data and provide the higher accuracy in detecting attacks.

B. OPEN CHALLENGES AND CONSIDERATIONS

1) SECURITY AND PRIVACY CHALLENGES

Federated learning promises to protect the privacy of local user data, however, recent studies have shown that the involvement of specific participants can still be revealed by analyzing the global model [165]. Although some techniques have been used to overcome this problem, including differential privacy [166], these approaches degrade model performance or require additional conditions that are not suitable for IoT networks, especially high computing power [167]. Therefore, efficiently implemented federated approaches that provide high performance and preserve privacy without additional computational overhead are strongly required for IoT networks and applications.

2) IoT NETWORK SETTINGS CHALLENGES

The robustness of the federated deep learning system should be considered since users and aggregators are required to exchange parameters over the IoT network. In addition, communication channels and computational power are constrained in terms of capacity, as well as the presence of various network issues such as bandwidth, interference, and noise [167]. Hence, client access and limited network reliability are significant research challenges in developing a federated deep learning system for cyber security in IoT applications.

3) DATA-RELATED CHALLENGES

The issue of identifying and eliminating bias of all kinds (cognitive, sampling, reporting, and confirmation) in the data generation process is a serious concern for ML research in general. However, it is more complicated in FL due to the fact that data is distributed over multiple parties. For example, if IoT devices have varying data sizes, the FL-based system may give more importance to the contributions of the populations. In addition, If the global model update depends on the latency of the IoT network, then networks with slower devices or networks may be under-represented [168]. The most important question that may arise is how to develop a new FL-based strategy that can resist the vulnerabilities (Poisoning attack, Jamming attack, Adversarial attack, ...etc.) while considering the practicability of deploying the solution, particularly in the context of low-resource IoT devices.

4) FL PLATFORMS CHALLENGES

Many IoT-based applications can benefit from FL due to the amazing performance of collaborative learning in the appropriate domains. Although there are various emerging frameworks for FL in general, designing a specific IoT framework based on FL is still an important research topic that needs to take into account the underlying IoT infrastructure.

VIII. CONCLUSION

In this article, we conducted a comparative study with an experimental analysis of federated deep learning approaches for cybersecurity in IoT applications. Specifically, we analyzed the federated learning-based security and privacy systems for several types of IoT applications, including, Industrial IoT, Edge Computing, Internet of Drones, Internet of Healthcare Things, Internet of Vehicles, etc. Then, we reviewed the federated learning systems with blockchain and malware/intrusion detection systems for IoT applications. We reviewed the vulnerabilities that can be exploited by adversaries in the federated learning-based security and privacy systems. We provided an experimental analysis of federated deep learning with three deep learning approaches, namely, RNN, CNN, and DNN. For each deep learning model, we studied the performance of centralized and federated learning under three IoT traffic datasets, namely, the Bot-IoT dataset, the MQTTset dataset, and the TON_IoT dataset. The results demonstrate that federated deep learning approaches can outperform the classic/centralized versions of machine learning (non-federated learning) in assuring the privacy of IoT device data and provides the highest accuracy in detecting attacks.

REFERENCES

[1] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2019.

[2] X. Hei, X. Yin, Y. Wang, J. Ren, and L. Zhu, "A trusted feature aggregator federated learning for distributed malicious attack detection," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102033.

[3] H. Wen, Y. Wu, C. Yang, H. Duan, and S. Yu, "A unified federated learning framework for wireless communications: Towards privacy, efficiency, and security," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 653–658.

[4] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.

[5] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, Jan. 2018.

[6] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks," *Future Internet*, vol. 12, no. 3, p. 44, Mar. 2020.

[7] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.
[8] Y. Zhang, Q. Wu, and M. Shikh-Bahaei, "Vertical federated learning based privacy-preserving cooperative sensing in cognitive radio networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2020, pp. 1–6.
[9] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial Intelligence and Statistics*. 2017, pp. 1273–1282. [Online]. Available: http://proceedings.mlr.press/v54/mcmahan17a.html
[10] L. Feng, Y. Zhao, S. Guo, X. Qiu, W. Li, and P. Yu, "Blockchain-based asynchronous federated learning for Internet of Things," *IEEE Trans. Comput.*, early access, Apr. 9, 2021, doi: 10.1109/TC.2021.3072033.
[11] N. Bouacida and P. Mohapatra, "Vulnerabilities in federated learning," *IEEE Access*, vol. 9, pp. 63229–63249, 2021.
[12] M. S. Jere, T. Farnan, and F. Koushanfar, "A taxonomy of attacks on federated learning," *IEEE Secur. Privacy*, vol. 19, no. 2, pp. 20–28, Dec. 2021.
[13] Y. Qi, M. S. Hossain, J. Nie, and X. Li, "Privacy-preserving blockchain-based federated learning for traffic flow prediction," *Future Gener. Comput. Syst.*, vol. 117, pp. 328–337, Apr. 2021.
[14] G. Han, T. Zhang, Y. Zhang, G. Xu, J. Sun, and J. Cao, "Verifiable and privacy preserving federated learning without fully trusted centers," *J. Ambient Intell. Humanized Comput.*, pp. 1–11, Jan. 2021. [Online]. Available: https://link.springer.com/article/10.1007/s12652-020-02664-x
[15] F. O. Olowononi, D. B. Rawat, and C. Liu, "Federated learning with differential privacy for resilient vehicular cyber physical systems," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–5.
[16] Z. Xiong, Z. Cai, D. Takabi, and W. Li, "Privacy threat and defense for federated learning with non-i.i.d. Data in AIoT," *IEEE Trans. Ind. Informat.*, early access, Apr. 19, 2021, doi: 10.1109/TII.2021.3073925.
[17] Z. Yang, M. Chen, W. Saad, C. S. Hong, and M. Shikh-Bahaei, "Energy efficient federated learning over wireless communication networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1935–1949, Mar. 2020.
[18] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5098–5107, Jul. 2021.
[19] *Federated Learning: Collaborative Machine Learning Without Centralized Training Data*. Accessed: Sep. 18, 2021. [Online]. Available: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html
[20] A. Hard, K. Rao, R. Mathews, S. Ramaswamy, F. Beaufays, S. Augenstein, H. Eichner, C. Kiddon, and D. Ramage, "Federated learning for mobile keyboard prediction," 2018, *arXiv:1811.03604*. [Online]. Available: http://arxiv.org/abs/1811.03604
[21] R. Kumar, A. A. Khan, J. Kumar, N. A. Golilarz, S. Zhang, Y. Ting, C. Zheng, and W. Wang, "Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging," *IEEE Sensors J.*, vol. 21, no. 14, pp. 16301–16314, Jul. 2021.
[22] B. Liu, B. Yan, Y. Zhou, Y. Yang, and Y. Zhang, "Experiments of federated learning for COVID-19 chest X-ray images," 2020, *arXiv:2007.05592*. [Online]. Available: http://arxiv.org/abs/2007.05592
[23] W. Zhang, T. Zhou, Q. Lu, X. Wang, C. Zhu, H. Sun, Z. Wang, S. K. Lo, and F.-Y. Wang, "Dynamic fusion-based federated learning for COVID-19 detection," *IEEE Internet Things J.*, early access, Feb. 4, 2021, doi: 10.1109/JIOT.2021.3056185.
[24] Q. Kong, F. Yin, R. Lu, B. Li, X. Wang, S. Cui, and P. Zhang, "Privacy-preserving aggregation for federated learning-based navigation in vehicular fog," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8453–8463, Dec. 2021.
[25] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for UAV-assisted crowdsensing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1055–1069, Apr. 2021.
[26] D. Chen, L. J. Xie, B. Kim, L. Wang, C. S. Hong, L.-C. Wang, and Z. Han, "Federated learning based mobile edge computing for augmented reality applications," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2020, pp. 767–773.
[27] M. H. U. Rehman, A. M. Dirir, K. Salah, E. Damiani, and D. Svetinovic, "TrustFed: A framework for fair and trustworthy cross-device federated learning in IIoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8485–8494, Dec. 2021.
[28] X. Wang, S. Garg, H. Lin, J. Hu, G. Kaddoum, M. J. Piran, and M. S. Hossain, "Towards accurate anomaly detection in industrial Internet-of-Things using hierarchical federated learning," *IEEE Internet Things J.*, early access, Apr. 20, 2021, doi: 10.1109/JIOT.2021.3074382.
[29] I. Cvitic, D. Perakovic, B. Gupta, and K.-K.-R. Choo, "Boosting-based DDoS detection in Internet of Things systems," *IEEE Internet Things J.*, early access, Jun. 21, 2021, doi: 10.1109/JIOT.2021.3090909.
[30] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.
[31] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2031–2063, 3rd Quart., 2020.
[32] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," *IEEE Access*, vol. 8, pp. 140699–140725, 2020.
[33] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," *China Commun.*, vol. 17, no. 9, pp. 105–118, Sep. 2020.
[34] J. C. Jiang, B. Kantarci, S. Oktug, and T. Soyata, "Federated learning in smart city sensing: Challenges and opportunities," *Sensors*, vol. 20, no. 21, p. 6230, Oct. 2020.
[35] L. Lyu, H. Yu, J. Zhao, and Q. Yang, "Threats to federated learning," in *Federated Learning*. Cham, Switzerland: Springer, 2020, pp. 3–16.
[36] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Gener. Comput. Syst.*, vol. 115, pp. 619–640, Feb. 2021.
[37] I. Kholod, E. Yanaki, D. Fomichev, E. Shalugin, E. Novikova, E. Filippov, and M. Nordlund, "Open-source federated learning frameworks for IoT: A comparative review and analysis," *Sensors*, vol. 21, no. 1, p. 167, Dec. 2021.
[38] S. A. Rahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, "A survey on federated learning: The journey from centralized to distributed on-site learning and beyond," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5476–5497, Apr. 2021.
[39] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1622–1658, 3rd Quart., 2021.
[40] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12806–12825, Aug. 2021.
[41] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1342–1397, 2nd Quart., 2021.
[42] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102355.
[43] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet Things J.*, early access, Jul. 6, 2021, doi: 10.1109/JIOT.2021.3095077.
[44] A. N. Bhagoji, S. Chakraborty, P. Mittal, and S. Calo, "Analyzing federated learning through an adversarial lens," in *Proc. Int. Conf. Mach. Learn.*, 2019, pp. 634–643.
[45] G. Xu, H. Li, S. Liu, K. Yang, and X. Lin, "VerifyNet: Secure and verifiable federated learning," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 911–926, 2019.
[46] Y. Gao, M. Kim, S. Abuadbba, Y. Kim, C. Thapa, K. Kim, S. A. Çamtepe, H. Kim, and S. Nepal, "End-to-end evaluation of federated learning and split learning for Internet of Things," *CoRR*, vol. abs/2003.13376, pp. 1–10, Mar. 2020. [Online]. Available: https://arxiv.org/abs/2003.13376
[47] W. Sun, S. Lei, L. Wang, Z. Liu, and Y. Zhang, "Adaptive federated learning and digital twin for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5605–5614, Aug. 2021.
[48] J. Yang, C. Fu, and H. Lu, "Optimized and federated soft-impute for privacy-preserving tensor completion in cyber-physical-social systems," *Inf. Sci.*, vol. 564, pp. 103–123, Jul. 2021.

[49] C. M. Thwal, K. Thar, Y. L. Tun, and C. S. Hong, "Attention on personalized clinical decision support system: Federated learning approach," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Jan. 2021, pp. 141–147.

[50] C. Fang, Y. Guo, N. Wang, and A. Ju, "Highly efficient federated learning with strong privacy preservation in cloud computing," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101889.

[51] Y. Dong, X. Chen, L. Shen, and D. Wang, "EaSTFLy: Efficient and secure ternary federated learning," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101824.

[52] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2238–2251, Feb. 2021.

[53] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning and permissioned blockchain for digital twin edge networks," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2276–2288, Feb. 2021.

[54] Y. Liu, Z. Ma, X. Liu, S. Ma, S. Nepal, R. H. Deng, and K. Ren, "Boosting privately: Federated extreme gradient boosting for mobile crowdsensing," in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Nov. 2020, pp. 1–11.

[55] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated learning for data privacy preservation in vehicular cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 50–56, May 2020.

[56] S. Lu, Y. Yao, and W. Shi, "Collaborative learning on the edges: A case study on connected vehicles," in *Proc. 2nd USENIX Workshop Hot Topics Edge Comput. (HotEdge)*, 2019, pp. 1–8.

[57] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 756–767.

[58] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6532–6542, Oct. 2019.

[59] D. Ciuonzo, P. S. Rossi, and P. K. Varshney, "Distributed detection in wireless sensor networks under multiplicative fading via generalized score tests," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9059–9071, Jun. 2021.

[60] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–7.

[61] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," 2018, *arXiv:1802.09089*. [Online]. Available: http://arxiv.org/abs/1802.09089

[62] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Phys. Commun.*, vol. 42, Oct. 2020, Art. no. 101157.

[63] I. Mohammed, S. Tabatabai, A. Al-Fuqaha, F. E. Bouanani, J. Qadir, B. Qolomany, and M. Guizani, "Budgeted online selection of candidate IoT clients to participate in federated learning," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5938–5952, Apr. 2020.

[64] H. Darvishi, D. Ciuonzo, E. R. Eide, and P. S. Rossi, "Sensor-fault detection, isolation and accommodation for digital twins via modular data-driven architecture," *IEEE Sensors J.*, vol. 21, no. 4, pp. 4827–4838, Feb. 2020.

[65] L. Kong, X.-Y. Liu, H. Sheng, P. Zeng, and G. Chen, "Federated tensor mining for secure industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2144–2153, Mar. 2019.

[66] T. V. Khoa, Y. M. Saputra, D. T. Hoang, N. L. Trung, D. Nguyen, N. V. Ha, and E. Dutkiewicz, "Collaborative learning model for cyberattack detection systems in IoT industry 4.0," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.

[67] B. Zhao, K. Fan, K. Yang, Z. Wang, H. Li, and Y. Yang, "Anonymous and privacy-preserving federated learning with industrial big data," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 6314–6323, Sep. 2021.

[68] A. Taïk and S. Cherkaoui, "Electrical load forecasting using edge computing and federated learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[69] J. Qian, S. P. Gochhayat, and L. K. Hansen, "Distributed active learning strategies on edge computing," in *Proc. 6th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud), 5th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Jun. 2019, pp. 221–226.

[70] Y. Xiao, Y. Li, G. Shi, and H. V. Poor, "Optimizing resource-efficiency for federated edge intelligence in IoT networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2020, pp. 86–92.

[71] L. Cui, Z. Chen, S. Yang, R. Chen, and Z. Ming, "A secure and decentralized DLaaS platform for edge resource scheduling against adversarial attacks," *IEEE Trans. Comput.*, early access, Apr. 21, 2021, doi: 10.1109/TC.2021.3074806.

[72] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.

[73] N. I. Mowla, N. H. Tran, I. Doh, and K. Chae, "AFRL: Adaptive federated reinforcement learning for intelligent jamming defense in FANET," *J. Commun. Netw.*, vol. 22, no. 3, pp. 244–258, Jun. 2020.

[74] J. Yao and N. Ansari, "Secure federated learning by power control for Internet of Drones," *IEEE Trans. Cognit. Commun. Netw.*, early access, Apr. 28, 2021, doi: 10.1109/TCCN.2021.3076167.

[75] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Netw.*, vol. 120, Sep. 2021, Art. no. 102574.

[76] M. Hao, H. Li, G. Xu, Z. Liu, and Z. Chen, "Privacy-aware and resource-saving collaborative learning for healthcare in cloud computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[77] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "FedHealth: A federated transfer learning framework for wearable healthcare," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, Jul. 2020.

[78] X. Zhang, M. Hu, J. Xia, T. Wei, M. Chen, and S. Hu, "Efficient federated learning for cloud-based AIoT applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, Dec. 22, 2020, doi: 10.1109/TCAD.2020.3046665.

[79] Y. Wei, S. Zhou, S. Leng, S. Maharjan, and Y. Zhang, "Federated learning empowered end-edge-cloud cooperation for 5G HetNet security," *IEEE Netw.*, vol. 35, no. 2, pp. 88–94, Mar. 2021.

[80] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 35–44, 2020.

[81] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "FDC: A secure federated deep learning mechanism for data collaborations in the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6348–6359, Jul. 2020.

[82] X. Zhang, R. Lu, J. Shao, F. Wang, H. Zhu, and A. A. Ghorbani, "FedSky: An efficient and privacy-preserving scheme for federated mobile crowdsensing," *IEEE Internet Things J.*, early access, Aug. 31, 2021, doi: 10.1109/JIOT.2021.3109058.

[83] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," 2016, *arXiv:1602.05629*. [Online]. Available: http://arxiv.org/abs/1602.05629

[84] J. Li, L. Lyu, X. Liu, X. Zhang, and X. Lv, "FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT," *IEEE Trans. Ind. Informat.*, early access, Jun. 14, 2021, doi: 10.1109/TII.2021.3088938.

[85] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated learning-based anomaly detection for IoT security attacks," *IEEE Internet Things J.*, early access, May 5, 2021, doi: 10.1109/JIOT.2021.3077803.

[86] T. T. Huong, T. P. Bac, D. M. Long, B. D. Thang, N. T. Binh, T. D. Luong, and T. K. Phuc, "LocKedge: Low-complexity cyberattack detection in IoT edge computing," *IEEE Access*, vol. 9, pp. 29696–29710, 2021.

[87] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "Fed-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8442–8452, Dec. 2021.

[88] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020.

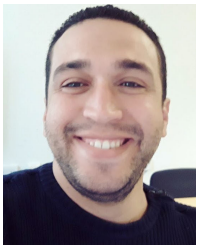
[89] N. A. A.-A. Al-Marri, B. S. Ciftler, and M. M. Abdallah, "Federated mimic learning for privacy preserving intrusion detection," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, May 2020, pp. 1–6.

[90] K. Li, H. Zhou, Z. Tu, W. Wang, and H. Zhang, "Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning," *IEEE Access*, vol. 8, pp. 214852–214865, 2020.

[91] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of Things intrusion detection: Centralized, on-device, or federated learning?" *IEEE Netw.*, vol. 34, no. 6, pp. 310–317, Nov. 2020.

[92] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.
[93] J. Payne and A. Kundu, "Towards deep federated defenses against malware in cloud ecosystems," in *Proc. 1st IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA)*, Dec. 2019, pp. 92–100.
[94] Y. Chen, J. Zhang, and C. K. Yeo, "Network anomaly detection using federated deep autoencoding Gaussian mixture model," in *Proc. Int. Conf. Mach. Learn. Netw.* Cham, Switzerland: Springer, 2019, pp. 1–14.
[95] W. Schneble and G. Thamilarasu, "Attack detection using federated learning in medical cyber-physical systems," in *Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2019, pp. 1–8.
[96] B. Cetin, A. Lazar, J. Kim, A. Sim, and K. Wu, "Federated wireless network intrusion detection," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 6004–6006.
[97] S. McElwee, J. Heaton, J. Fraley, and J. Cannady, "Deep learning for prioritizing and responding to intrusion detection alerts," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 1–5.
[98] N. Moustafa, M. Keshky, E. Debiez, and H. Janicke, "Federated TON_IoT Windows datasets for evaluating AI-based security applications," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*. Los Alamitos, CA, USA: IEEE Computer Society, Dec. 2020, pp. 848–855.
[99] D. Połap, G. Srivastava, and K. Yu, "Agent architecture of an intelligent medical system based on federated learning and blockchain technology," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102748.
[100] Z. Li, J. Liu, J. Hao, H. Wang, and M. Xian, "CrowdSFL: A secure crowd computing framework based on blockchain and federated learning," *Electronics*, vol. 9, no. 5, p. 773, May 2020.
[101] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, "A secure federated learning framework for 5G networks," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 24–31, Aug. 2020.
[102] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, and P. Li, "AI at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9600–9610, Oct. 2020.
[103] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of Health Things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.
[104] D. Połap, G. Srivastava, A. Jolfaei, and R. M. Parizi, "Blockchain technology and neural networks for the Internet of Medical Things," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 508–513.
[105] P. K. Sharma, J. H. Park, and K. Cho, "Blockchain and federated learning-based distributed computing defence framework for sustainable society," *Sustain. Cities Soc.*, vol. 59, Aug. 2020, Art. no. 102220.
[106] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4177–4186, Jun. 2019.
[107] U. Majeed and C. S. Hong, "FLchain: Federated learning via MEC-enabled blockchain network," in *Proc. 20th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Sep. 2019, pp. 1–4.
[108] S. Lugan, P. Desbordes, E. Brion, L. X. Ramos Tormo, A. Legay, and B. Macq, "Secure architectures implementing trusted coalitions for blockchained distributed learning (TCLearn)," *IEEE Access*, vol. 7, pp. 181789–181799, 2019.
[109] R. Doku and D. B. Rawat, "IFLBC: On the edge intelligence using federated learning blockchain network," in *Proc. IEEE IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2020, pp. 221–226.
[110] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
[111] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial," *IEEE Internet Things J.*, early access, May 6, 2021, doi: 10.1109/JIOT.2021.3078072.
[112] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for 5G beyond," *IEEE Netw.*, vol. 35, no. 1, pp. 219–225, Jan. 2020.
[113] S. Otoum, I. A. Ridhawi, and H. T. Mouftah, "Blockchain-supported federated learning for trustworthy vehicular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.
[114] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Netw.*, vol. 35, no. 1, pp. 234–241, Jan. 2021.
[115] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, "VFChain: Enabling verifiable and auditable federated learning via blockchain systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Jan. 12, 2021, doi: 10.1109/TNSE.2021.3050781.
[116] Y. Chen, Q. Chen, and Y. Xie, "A methodology for high-efficient federated-learning with consortium blockchain," in *Proc. IEEE 4th Conf. Energy Internet Energy Syst. Integr. (EI)*, Oct. 2020, pp. 3090–3095.
[117] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Trans. Ind. Informat.*, early access, Jun. 8, 2021, doi: 10.1109/TII.2021.3085960.
[118] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2964–2973, Apr. 2020.
[119] Y. Zhang, Y. Song, J. Liang, K. Bai, and Q. Yang, "Two sides of the same coin: White-box and black-box attacks for transfer learning," in *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2020, pp. 2989–2997.
[120] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep models under the GAN: Information leakage from collaborative deep learning," in *Proc. Conf. Comput. Commun. Secur. (ACM SIGSAC)*, Oct. 2017, pp. 603–618.
[121] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[122] M. M. Hassan, M. R. Hassan, S. Huda, and V. H. C. de Albuquerque, "A robust deep-learning-enabled trust-boundary protection for adversarial industrial IoT environment," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9611–9621, Jun. 2020.
[123] Y. Song, T. Liu, T. Wei, X. Wang, Z. Tao, and M. Chen, "FDA^3: Federated defense against adversarial attacks for cloud-based IIoT applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7830–7838, Nov. 2021.
[124] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial attacks against network intrusion detection in IoT systems," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10327–10335, Jul. 2021.
[125] M. Fang, X. Cao, J. Jia, and N. Gong, "Local model poisoning attacks to Byzantine-robust federated learning," in *Proc. 29th Secur. Symp. (USENIX Secur.)*, 2020, pp. 1605–1622.
[126] A. K. Singh, A. Blanco-Justicia, J. Domingo-Ferrer, D. Sánchez, and D. Rebollo-Monedero, "Fair detection of poisoning attacks in federated learning," in *Proc. IEEE 32nd Int. Conf. Tools Artif. Intell. (ICTAI)*, Nov. 2020, pp. 224–229.
[127] Y. Zhao, J. Chen, J. Zhang, D. Wu, M. Blumenstein, and S. Yu, "Detecting and mitigating poisoning attacks in federated learning using generative adversarial networks," *Concurrency Comput., Pract. Exper.*, p. e5906, Jun. 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5906
[128] Z. Ma, J. Ma, Y. Miao, X. Liu, K.-K.-R. Choo, and R. Deng, "Pocket diagnosis: Secure federated learning against poisoning attack in the cloud," *IEEE Trans. Services Comput.*, early access, Jun. 22, 2021, doi: 10.1109/TSC.2021.3090771.
[129] N. Mowla, N. H. Tran, I. Doh, and K. Chae, "Federated learning-based cognitive detection of jamming attack in flying ad-hoc network," *IEEE Access*, vol. 8, pp. 4338–4350, 2019.
[130] N. Jebreel, A. Blanco-Justicia, D. Sánchez, and J. Domingo-Ferrer, "Efficient detection of Byzantine attacks in federated learning using last layer biases," in *Proc. Int. Conf. Modeling Decisions Artif. Intell.* Cham, Switzerland: Springer, 2020, pp. 154–165.
[131] Y. Jiang, Y. Zhou, D. Wu, C. Li, and Y. Wang, "On the detection of shilling attacks in federated collaborative filtering," in *Proc. Int. Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2020, pp. 185–194.
[132] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, and C.-J. Hsieh, "ZOO: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models," in *Proc. 10th ACM Workshop Artif. Intell. Secur.*, Nov. 2017, pp. 15–26.
[133] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical black-box attacks against machine learning," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Apr. 2017, pp. 506–519.

[134] G. Apruzzese, M. Andreolini, M. Marchetti, A. Venturi, and M. Colajanni, "Deep reinforcement adversarial learning against botnet evasion attacks," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 4, pp. 1975–1987, Dec. 2020.
[135] Y. Xu, X. Zhong, A. J. Yepes, and J. H. Lau, "Grey-box adversarial attack and defence for sentiment classification," 2021, *arXiv:2103.11576*. [Online]. Available: http://arxiv.org/abs/2103.11576
[136] L. Melis, C. Song, E. D. Cristofaro, and V. Shmatikov, "Exploiting unintended feature leakage in collaborative learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 691–706.
[137] J. Tan, Y.-C. Liang, N. C. Luong, and D. Niyato, "Toward smart security enhancement of federated learning networks," *IEEE Netw.*, vol. 35, no. 1, pp. 340–347, Jan. 2021.
[138] W. Wen, C. Xu, F. Yan, C. Wu, Y. Wang, Y. Chen, and H. Li, "TernGrad: Ternary gradients to reduce communication in distributed deep learning," in *Proc. 31st Int. Conf. Neural Inf. Process. Syst. (NIPS)*. Red Hook, NY, USA: Curran Associates, 2017, pp. 1508–1518.
[139] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2020, pp. 480–501.
[140] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognit.*, vol. 84, pp. 317–331, Dec. 2018.
[141] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, "SoK: Security and privacy in machine learning," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS P)*, Apr. 2018, pp. 399–414.
[142] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 27, 2014, pp. 1–9.
[143] A. Ferdowsi and W. Saad, "Generative adversarial networks for distributed intrusion detection in the Internet of Things," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[144] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Adversarial machine learning attacks and defense methods in the cyber security domain," *ACM Comput. Surveys*, vol. 54, no. 5, pp. 1–36, Jun. 2021.
[145] N. Rodríguez-Barroso, G. Stipcich, D. Jiménez-López, J. A. Ruiz-Millán, E. Martínez-Cámara, G. González-Seco, M. V. Luzón, M. A. Veganzones, and F. Herrera, "Federated learning and differential privacy: Software tools analysis, the Sherpa.ai FL framework and methodological guidelines for preserving data privacy," *Inf. Fusion*, vol. 64, pp. 270–292, Dec. 2020.
[146] *The MNIST Database of Handwritten Digits*. Accessed: Sep. 18, 2021. [Online]. Available: http://www.yann.lecun.com/exdb/mnist/
[147] G. Cohen, S. Afshar, J. Tapson, and A. van Schaik, "EMNIST: Extending MNIST to handwritten letters," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, May 2017, pp. 2921–2926.
[148] S. Caldas, S. M. K. Duddu, P. Wu, T. Li, J. Konečnỳ, H. B. McMahan, V. Smith, and A. Talwalkar, "LEAF: A benchmark for federated settings," 2018, *arXiv:1812.01097*. [Online]. Available: http://arxiv.org/abs/1812.01097
[149] N. Moustafa, "New generations of Internet of Things datasets for cybersecurity applications based machine learning: TON_IoT datasets," in *Proc. eResearch Australasia Conf.*, Brisbane, QLD, Australia, 2019, pp. 21–25.
[150] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 102994.
[151] A. Krizhevsky and G. Hinton, "Learning multiple layers of features from tiny images," Univ. Toronto, Toronto, ON, Canada, Tech. Rep., 2009.
[152] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.
[153] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, 2018, pp. 108–116.
[154] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019.
[155] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT edge devices," *IEEE Internet Things J.*, early access, Jul. 28, 2021, doi: 10.1109/JIOT.2021.3100755.
[156] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, "MQTTset, a new dataset for machine learning techniques on MQTT," *Sensors*, vol. 20, no. 22, p. 6578, Nov. 2020.
[157] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervas. Comput.*, vol. 17, no. 3, pp. 12–22, Oct. 2018.
[158] V. Rey, P. M. S. Sánchez, A. H. Celdrán, G. Bovet, and M. Jaggi, "Federated learning for malware detection in IoT devices," 2021, *arXiv:2104.09994*. [Online]. Available: http://arxiv.org/abs/2104.09994
[159] M. A. Ferrag, L. Shu, O. Friha, and X. Yang, "Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions," *IEEE CAA J. Autom. Sinica*, early access, Sep. 16, 2021, doi: 10.1109/JAS.2017.7510889.
[160] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques," in *Proc. Int. Conf. Mobile Netw. Manage.* Cham, Switzerland: Springer, 2017, pp. 30–44.
[161] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Gener. Comput. Syst.*, vol. 110, pp. 91–106, Sep. 2020.
[162] N. Koroniotis and N. Moustafa, "Enhancing network forensics with particle swarm and deep learning: The particle deep framework," 2020, *arXiv:2005.00722*. [Online]. Available: http://arxiv.org/abs/2005.00722
[163] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A holistic review of cybersecurity and reliability perspectives in smart airports," *IEEE Access*, vol. 8, pp. 209802–209834, 2020.
[164] N. Koroniotis, "Designing an effective network forensic framework for the investigation of botnets in the Internet of Things," Ph.D. dissertation, School Eng. Inf. Technol., Univ. New South Wales, Sydney, NSW, Australia, 2020.
[165] Z. Wang, M. Song, Z. Zhang, Y. Song, Q. Wang, and H. Qi, "Beyond inferring class representatives: User-level privacy leakage from federated learning," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2019, pp. 2512–2520.
[166] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, Q. S. T. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3454–3469, 2020.
[167] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 46–51, Jun. 2020.
[168] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, and R. G. D'Oliveira, "Advances and open problems in federated learning," 2019, *arXiv:1912.04977*. [Online]. Available: http://arxiv.org/abs/1912.04977



MOHAMED AMINE FERRAG received the bachelor's, master's, Ph.D., and Habilitation degrees in computer science from Badji Mokhtar-Annaba University, Annaba, Algeria, in June 2008, June 2010, June 2014, and April 2019, respectively.

Since October 2014, he has been a Senior Lecturer with the Department of Computer Science, Guelma University, Guelma, Algeria. Since July 2019, he has been a Visiting Senior Researcher with the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, Nanjing, China. His research interests include wireless network security, network coding security, and applied cryptography. He has published over 80 papers in international journals and conferences in the above areas. He has been conducting several research projects with international collaborations on these topics. He was a recipient of the 2021 IEEE TEM Best Paper Award. His current H-index is 22, i10-index is 36, and 2402 citations in Google Scholar Citation. He is

featured in Stanford University's list of the world's Top 2 % scientists for the year 2019. Some of his research findings are published in top-cited journals, such as the IEEE Communications Surveys & Tutorials, IEEE Internet of Things Journal, IEEE Transactions on Engineering Management, IEEE Access, IEEE/CAA Journal of Automatica Sinica, *Sensors* (MDPI), *Journal of Information Security and Applications* (Elsevier), *Transactions on Emerging Telecommunications Technologies* (Wiley), *Telecommunication Systems* (Springer), *International Journal of Communication Systems* (Wiley), *Sustainable Cities and Society* (Elsevier), and *Journal of Network and Computer Applications* (Elsevier). He is currently serving on various editorial positions, such as an editorial board member of journals (Indexed SCI and Scopus), such as *ICT Express* (JCR IF 4.317), *IET Networks* (Citescore 4.1), *International Journal of Internet Technology and Secured Transactions* (Citescore 1.0), *Security and Communication Networks* (JCR IF 1.791), and *Journal of Sensor and Actuator Networks* (Citescore 6.2). He reviewed more than 580 articles for top-cited journals, including *Nature*, IEEE transactions, Elsevier, Springer, and Wiley journals.

OTHMANE FRIHA received the master's degree in computer science from Badji Mokhtar-Annaba University, Algeria, in 2018, where he is currently pursuing the Ph.D. degree. His current research interests include network and computer security, the Internet of Things, and applied cryptography.

LEANDROS MAGLARAS (Senior Member, IEEE) received the B.Sc. degree from Aristotle University of Thessaloniki, Greece, in 1998, the M.Sc. degree in industrial production and management from University of Thessaly, in 2004, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Volos, in 2008 and 2014, respectively. He is currently the Head of the National Cyber Security Authority, Greece, and a Visiting Lecturer with the School of Computer Science and Informatics, De Montfort University, U.K. He serves on the Editorial Board of several international peer-reviewed journals, such as IEEE Access, *Security and Communication Networks* (Wiley), *EAI Endorsed Transactions on e-Learning*, and *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*. He is an author of more than 80 papers in scientific magazines and conferences. His research interests include wireless sensor networks and vehicular ad hoc networks.

HELGE JANICKE (Member, IEEE) is currently the Research Director of the Cyber Security Cooperative Research Centre, Australia. He is affiliated with Edith Cowan University and is also a Visiting Professor in cyber security at De Montfort University, U.K. His research interests include the area of cyber security, in particular with applications in critical infrastructures using cyber-physical systems, SCADA, and industrial control systems. He established DMU's Cyber Technology Institute and its Airbus Centre of Excellence in SCADA Cyber Security and Forensics Research. He has been the Head of the School of Computer Science, De Montfort University, before taking up his current position as the Research Director of the Cyber Security Cooperative Research Centre. He founded the International Symposium on Industrial Control System Cyber Security Research (ICS-CSR) and contributed over 150 peer-reviewed articles and conference papers to the field that resulted from his collaborative research with industry partners, such as Airbus, BT, Deloitte, Rolls-Royce, QinetiQ, and General-Dynamics. His current research investigates the application of Agile techniques to cyber incident response in critical infrastructure, managing human errors that lead to cyber incidents, and research on cyber warfare and cyber peacekeeping.

LEI SHU (Senior Member, IEEE) received the B.S. degree in computer science from South Central University for Nationalities, China, in 2002, the M.S. degree in computer engineering from Kyung Hee University, South Korea, in 2005, and the Ph.D. degree from the Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010. Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, China, and a Lincoln Professor with the University of Lincoln, U.K., where he is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering. He has published over 400 papers in related conferences, journals, and books in the areas of sensor networks and the Internet of Things. His current H-index is 63 and i10-index is 253 in Google Scholar Citation. His current research interests include wireless sensor networks and the Internet of Things. He has also served as a TPC member for more than 150 conferences, such as ICDCS, DCOSS, MASS, ICC, GLOBECOM, ICCCN, WCNC, and ISCC. He was a recipient of the 2014 Top Level Talents in Sailing Plan of Guangdong Province, China, the 2015 Outstanding Young Professor of Guangdong Province, and the GLOBECOM 2010, ICC 2013, ComManTel 2014, WICON 2016, SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal best paper awards, the 2017 *Journal of Network and Computer Applications* Best Research Paper Award, the Outstanding Associate Editor Award of 2017, and the 2018 IEEE Access. He has also served as the Co-Chair for over 50 various international conferences/workshops, such as IWCMC, ICC, ISCC, ICNC, and Chinacom; especially the Symposium Co-Chair for IWCMC 2012 and ICC 2012; the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019; and the TPC Chair for InisCom 2015, NCCA 2015, WICON 2016, NCCA 2016, Chinacom 2017, InisCom 2017, WMNC 2017, and NCCA 2018.