FEDERATED LEARNING FOR INTRUSION DETECTION SYSTEM: CONCEPT, CHALLENGES AND FUTURE DIRECTION

A. Shubha[1], Dr A. Kanagaraj[2], S. Sathiyapriya[3], N. Balakumar[4], P. Karthiga[5]

[1,3,4,5] Ph.D Research Scholar, Department of Computer Science, Nallamuthu Gounder Mahalingam College
Pollachi, Tamil Nadu - 642001, India.

[2] Assistant Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College
Pollachi, Tamil Nadu - 642001, India.

as.shuba68@gmail.com, a.kanagaraj@gmail.com

ABSTRACT

The Internet of Things (IoT) is a network of electrical devices that are connected to the Internet wirelessly. This group of devices generates a large amount of data with information about users, which makes the whole system sensitive and prone to malicious attacks. The rapid development in manufacturing industries due to the introduction of IIoT devices has led to the emergence of Industry 4.0 which results in an industry with intelligence, increased efficiency and reduction in the cost of manufacturing. However, the introduction of IIoT devices opens up the door for a variety of cyber threats in smart industries. The detection of cyber threats against such extensive, complex, and heterogeneous smart manufacturing industries is very challenging due to the lack of sufficient attack traces. Machine Learning (ML) and Deep Learning (DL) with Intrusion Detection Systems have gained great momentum due to their achievement of high classification accuracy. Owing to the growing distribution of data over numerous networks of connected devices decentralized ML solutions are needed. The present paper aims to present an extensive and exhaustive review on the use of FL in intrusion detection system. In order to establish the need for FL, various types of IDS, relevant ML approaches and its associated issues are discussed. The allied challenges of FL implementations are also identified which provides idea on the scope of future direction of research. The paper finally presents the plausible solutions associated with the identified challenges in FL based intrusion detection system implementation acting as a baseline for prospective research.

Keywords: Federated Learning, Internet of Things, Intrusion Detection, Machine Learning, Deep Learning, privacy, security, Industrial Internet of Things (IIoT).

1. INTRODUCTION

1.1 Internet of Things (IoT)

The Internet of Things (IoT) is penetrating many facets of our daily life with the popularity of intelligent services and applications empowered by artificial intelligence (AI). In recent years, IDS mechanisms are usually based on artificial intelligence (AI) techniques, so that the system is trained with devices' network traffic to accurately detect any anomalous behavior, which could represent a certain type of attack [2]. IDS uses different techniques for detecting anomalies. However, traditional methods such as signature-based detection is becoming less efficient since this technique uses a signature database to recognize known attacks, and hence new attacks cannot be identified [3]. The Internet of Things paradigm has been revealed to be effective in managing such challenges since it makes it easier to connect several nodes and attain automation of networking operations. It is estimated that nowadays, 30 billion devices are connected over the Internet, and this number will reach 75 billion worldwide by 2025 [4], [5]. IoT technology can be used in sectors like Manufacturing, Agriculture, Healthcare, Transportation, Media/Advertising, Retail, Water and Waste Management, Power Distribution, etc. IoT is used in various applications like smart home, smart parking, smart water level monitoring, smart healthcare, smart traffic lighting, smart waste management, smart solar panels, etc. It is essential for achieving high productivity, efficiency, a safe working environment, and low carbon emissions in the industry and other contexts. Healthcare and manufacturing are the sectors where several startups are working extensively on smart solutions.[6]. This increase of devices is creating a massive number of issues such as attacks against the networking systems, data theft, addressing issues, battery loss, huge energy consumption, etc. However, before the revolution of Industry 3.0 and 4.0 [7]

1.2 Industrial Internet of Things (IIoT)

Recent advances in communication and smart device technologies along with the rapid development of industrial informatization have promoted the proliferation of the Industrial Internet of Things (IIoT), with its capability to increase productivity and efficiency in industries [8].The Industrial Internet of Things (IIoT) refers to the extension and use of the Internet of Things (IoT) in industrial sectors and applications. With a strong focus on machine-to-machine (M2M) communication, big data, and machine learning, the IIoT enables industries and enterprises to have better efficiency and reliability in their operations. The Industrial Internet of Things (IIoT) is a technical development that increases the manufacturing and economic effect of the manufacturing sector [9], [10]. IoT features, such as sensing, actuating, interconnecting, and processing data at various stages have resulted in the technological advancements listed. Data collection, processing, and intelligent decision-making with minimal human involvement are skills and advantages that IIoT systems offer to manufacture environments. IIoT is a division of the Internet of Things that focuses on the manufacturing industry [10]. IIoT focuses on enhancing manufacturing enterprises' accessibility, performance, scalability, time savings, and cost savings and is often correlated with Industry 4.0 [11]. The IIoT encompasses industrial applications, including robotics, medical devices, and software-defined production processes. The principal driver of IIoT is smart machines, for two reasons. The first is that smart machines capture and analyze data in real-time, which humans cannot. The second is that smart machines communicate their findings in a manner that is simple and fast, enabling faster and more accurate business decisions. IIoT is used across a range of industries from manufacturing, logistics, oil and gas, transportation, mining, aviation, energy, and more. Its focus is to optimize operations--particularly the automation of processes and maintenance. IIoT capabilities enhance asset performance and better manage maintenance. In the long run, it moves the industry toward a demand service model, increases customer intimacy, and creates new revenue streams--which all contributes to the digital transformation of industries.

1.3 Federated Learning

As an alternative to typical centralized learning approaches, federated learning (FL) was proposed in 2016 [12] as a collaborative learning approach, in which an AI algorithm is trained locally across multiple decentralized edge devices, called clients or parties, and the information is continuously updated onto a global model through several training rounds. Instead of sharing their data, parties share their models with an aggregator, which computes a global model. Nonetheless, FL suffers from privacy issues, as the global model's updates provided by parties could be used to launch several attacks to infer the private information of the training data [13]. To mitigate such privacy concerns, differential privacy (DP) [14] can be employed to obfuscate either the training data or model updates, giving statistical privacy guarantees over the data against an adversary. DP is usually considered in the scope of FL settings due to the stringent communication requirements of other privacy-preserving approaches, such as secure multiparty computation (SMC) [15]. Google proposed the concept of Federated Learning (FL) for on-device learning and data privacy preservation [10]. FL enables the devices to learn in a collaborative way without the need of data sharing with a centralized server. In other words, thanks to its features, ML/DL can be trained across multiple devices and servers with decentralized data over multiple iterations [16], [17]. FL can be divided into Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (TFL). In more details, HFL is an FL approach where datasets on the clients (i.e., devices) have the same features space with different observation. VFL (known as features-based FL) is an FL approach where the data between different domains is used to train the global model [18]. Here, dataset on the clients can have the same observations with different features. In addition to HFL and VFL, there is TFL architecture proposed in [19], which can be used when the dataset on the devices differ not only in instances but also in features.

1.4 Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a hardware or software system that tracks a network for unauthorized behavior or policy breaches. The IDS logs the details related to the intrusion, initiates warnings and takes necessary mitigation or corrective measures in case an intrusion is detected [22]. Intrusion detection is a strong active defense mechanism, and there are many intrusion detection methods [23]. Depending on the data source, intrusion detection techniques can generally be divided into two categories: network-based intrusion detection and host-based intrusion detection [24]. The network-based intrusion detection system is one of the solutions for the early detection of network attacks [25]. According to the different detection mechanisms, intrusion detection technology can be divided into two categories: misuse-based intrusion detection and anomaly-based intrusion detection. Misuse-based intrusion detection uses a set of predefined rules and patterns to detect attacks. Anomaly-based intrusion detection uses a recollected dataset with normal or malicious behavior labels and uses this dataset to train and test a detection model; any network flow that deviates from the model threshold is flagged as an anomalous entry and reported as an attacker. Due to the excellent classification performance of machine learning, researchers have widely used machine learning methods in anomaly-based intrusion detection, such as the Bayesian model, support vector machine, genetic algorithm, and other machine learning models [23].

Types Of Intrusion Detection Systems

1. Network Intrusion Detection System (NIDS):
2. Host Intrusion Detection System (HIDS):
3. Protocol-based Intrusion Detection System (PIDS)
4. Application Protocol-based Intrusion Detection System (APIDS):
5. Hybrid Intrusion Detection System

1.4.1 Characteristics of IDS

[26] established a series of basic aspects concerning the establishment and evaluation of IDS:

1) **Input data type** handled, e.g., Raw traffic, data flows and encrypted payloads for NIDS, or application data, memory accesses and kernel operations for HIDS.
2) **Location of the IDS**. Either position in the network of a NIDS or the level of the system stack where a HIDS is implemented.
3) **Performance** in terms of accuracy and response time.
4) **Adaptability** to rapidly learn new threats

1.4.2 The Three Intrusion Detection System Methods

1) Signature-Based Intrusion Detection
2) Anomaly-Based Intrusion Detection
3) Hybrid Intrusion Detection

2. FEDERATED LEARNING ENABLED IDS IN IOT

Internet of Things (IoT) are one of the most effective combinations of physical objects and networks. It involves the uses of embedded systems, wireless networks, machine learning, automation and many other fields. As IoT are becoming critical infrastructure, they can be targets of attackers and need to be proactively protected. Intrusion detection system (IDS) is one of the most common security mechanisms used to thwart malicious attacks. IDS may be anomaly-based or signature-based. Signature-based models generally work well for previously known attacks but not for new/unknown attacks. Machine learning models are increasingly applied in IDS, which work better in detecting previously unknown attack**s**. The individual and integration use of the Internet of Things (IoT) and Federated Learning (FL) have recently been used in several network-related scenarios and have consequently experienced a growing interest in the research community. Federated learning addresses the privacy and security issues of the IoT data in a decentralized manner. Also, it can be capable of training the multiple learning algorithms through local content except for exchanging data through intelligent Artificial Intelligence (AI)-based algorithms. With the growing number of always-online connected devices, the challenges facing modern network environments have also grown. Most of the attacks in IoT networks can be broadly categorized into four groups: Denial of Service (DoS), Probe, Remote to Local (R2L), User to Root (U2R). According to the literature [20], [21], U2R and R2L mimic normal traffic characteristics to a huge extent and hence, difficult to detect.

3. FEDERATED LEARNING ENABLED IDS IN IIOT

Developed a federated learning-enabled framework to construct a comprehensive intrusion detection model which can collaboratively train the model on multiple data from different industries without disclosing it to each other. As data does not leave the premises, thus data privacy is also achieved. An intrusion detection system (IDS) is a specialized security system that continuously examines network or computer system events for signs of an intrusion [27]. It examines the metadata found in network packets and employs pre-established rules to determine whether to allow or deny traffic. Intrusion detection methods can primarily be divided into two types: deployment-based techniques and detection-based techniques. Additionally, each of these categories can be grouped into a further two subcategories. Depending on how they are used, the intrusion detection systems can be of two types: host-based IDS (HIDS) and network-based IDS (NIDS). Depending on how intrusions are detected, IDS techniques can be categorized as either signature-based or anomaly-based systems.[28].

4. CHALLENGES

This section thus discusses the key challenges and issues of using FL for IDS.

a) Communication Overhead

The primary limitation of any FL application is the cost of communication per round of training [29]. The server traffic, packet transmission loss, the time taken to communicate the parameters may vary greatly depending on the network bandwidth. Also, the use of different devices in a network entail that the computation capability of each is different. Considering all such aspects, it is coherent that in practical situations the overall throughput of any federated network would be low.

b) Communication requirements

The need for a significant communication bandwidth to exchange global model updates represents a well-known issue associated with the use of FL [30]. This problem can be exacerbated in IoT scenarios where end devices acting as FL clients need to communicate their model updates through constrained networks and devices, which can degrade the network or IoT performance [31]. In general, there are two main factors that impose strong communication requirements between FL clients and coordinator. The first aspect is related to the amount of data associated with the gradient exchange [32], which is required between clients and the coordinator for the learning process. This is generally addressed by gradient compression techniques, such as quantization and scarification, as described by [33]. The second aspect is related to the number of training rounds required to converge the model that can vary depending on the scenario, dataset, data distribution, or the ML algorithm being considered. Hence, the use of compression techniques, as well as to reach a tradeoff between number of epochs and rounds in a certain FL setting are crucial aspects to be considered in future FL deployments.

c) Federated Poisoning Attacks

The superiority of federated architectures comes from the distributed nature of data present in client edge devices. Although this property protects the privacy of the data in transit and avoids their collection in a central location, the data in question is still at risk. In the device of a client (i.e. the source of FL data), the labels of the data can easily be modified. These attacks are called poisoning attacks. If a client pretends to be a benign participant, they are capable of modifying the local and global models to produce poisoned predictions. In the worst case, the global model either collapses during training or shows a false performance against the integrity of the data it was trained on [34]. It inserts small amounts of malicious traffic in the training data to slowly create a backdoor resulting in poisoning attacks. The work proves the significance of the damage that can be caused by these attacks.

d) Client Selection

In each training round, the coordinator can select a subset of devices to participate as FL clients in the training process. For this purpose, different aspects such as device status, battery level, computing/communication capacity, or ML technique's accuracy could be considered [35,36]. Indeed, the client selection process can have an impact on the obtained accuracy and, therefore, on the de-taction of potential security attacks in the scope of an IDS approach. we found that even a static client selection process can help to obtaining a better performance of the ML algorithm. However, more sophisticated client selection strategies must consider the dynamic aspects of an IoT environment in each training round. For example, some devices may not be available in a certain round due to mobility issues or loss of connectivity [37].

e) High False Alarms through the use of non-IID data

The characteristics of flowing traffic cannot simply be determined by studying some samples. Although its properties are discrete, numerous attributes are needed to analyze network traffic, many of which may play a significant role in some cases and maybe negligible in others. The complexity of intrusion detection data itself makes the task of classification tougher. This variance is not only due to the heterogeneity of data sources but also the non-IID nature of the data. The failure of one local model may not affect the system, but considering the practicality of Realtime situations, the probability of multiple client failures is significant [38].

f) Vulnerabilities in Intrusion Detection Setups

Intrusion Detection Systems may typically be installed as the first line of defense for a single workstation or a computer network. An FL architecture primarily employs DL algorithms to classify or cluster the abnormal properties of the network packets to raise an alert. This leaves the IDS susceptible to a wide array of vulnerabilities. These vulnerabilities can be deemed fatal and threatening to the Confidentiality and Integrity of the system under protection [39]. Thus the detection of such an anomaly is random and can cause damage without any alarm to the respective authorities. At the same time, labeling all the traffic requires huge effort of human annotators sometimes with a specific domain of expertise [40].

g) Aggregator as bottleneck

The use of blockchain can increase the level of trust in an FL environment, where the centralized coordinator is replaced by a set of nodes with distributed functionality, which is carried out through smart contracts [41,42]. Indeed, blockchain has been proposed in recent works to make model updates accountable and avoid potentially malicious updates [43]. Furthermore, as described by [44], the use of permissionless blockchains can raise privacy concerns, which must be addressed by proper encryption or differential privacy techniques.

h) Heterogeneity device type

The main challenge is to link all devices to each other is that the various heterogeneous devices are running on various platforms and frameworks. The IoT features, the mass of diverse devices, complexity at the network level, various communication protocols communicate including an ultra-largescale network of things, device, and network-level heterogeneity, and huge amounts of actions produced naturally by these sensors will make the development of the IDS a very challenging task.

i) Data privacy

The majority of IoT datasets are existing with big organizations that are unwilling to share it so certainly. Access to copyrighted datasets or privacy considerations. These are more general in the area with personal data such as healthcare and education.

5. FUTURE DIRECTION

After a critical review of FL-IDS systems and their challenges in the previous sections, the future scope of development in the field is discussed. Covering those issues, directions and possible solutions are provided for each. Considering the current literature and technological advancement on FL systems, many state-of-the-art solutions seem feasible and applicable to the domain of IDS. Plausible solutions include the incorporation of modern communication protocols.

a.) Communication Efficient Federated IDS

Important factors contributing to the communication overhead of a federated architecture are the transmission cost of bulky model parameters and the lag in packet transmissions. The more complex an application the bulkier the resultant global model would be. Transferring them to and from all clients for each round definitely consumes a lot of energy. To overcome this limitation various compression and encryption standards can be utilized. More importantly, lightweight DL technology can be used for reducing the size of parameters that need to be transferred as well as improve their prediction efficiency [45].

b.) Improving privacy-preserving techniques:

Federated learning already provides privacy benefits, but further research can explore advanced techniques to enhance privacy in the data sharing process. Differential privacy, homomorphic encryption, and secure multi-party computation are some of the potential techniques that can be explored. The major concern of FL is privacy. The transfer of the information about the data through weights and their subsequent update in the server model is a feature of FL. This transfer of weights does not contain the user data rather, they incorporate the features of this data, thus protecting the user's private information. These weights however could represent some features of the data that are sensitive and could cause harm if extracted by a third party [46].

c.) Edge Computing in FL based IDS

Edge devices are not limited to our smartphones or laptops but extend to low-power IoT devices, sensors, etc. The processing power of each is different through which their computation support for federated architectures is reflected. Edge computing involves processing data at the edge of the network, closer to where data is generated. Future research will explore the use of federated learning for edge computing to improve the efficiency and scalability of intrusion detection [47].

e.) Implementation of FL through secure channels

Intrusion detection systems are placed to prevent cyber-attacks on the targeted systems. Deploying such IDS systems using FL increases the possibility of intrusions despite the better performance of the overall system. This is due to the creation of various vulnerable points on becoming a huge network. This is to say that no defense mechanism is full proof and as FL is integrated, the system is not only at risk from a single network channel or a virtual machine but an entire network consisting of the server and numerous clients. To overcome these, collaborative learning has adopted the use of secure communication and transaction channels like blockchain. Blockchain has emerged as a secure way of storing transactions or recording information that makes it almost impossible to hack or intruder[48].

f.) Federated learning for real-time intrusion detection:

Real-time intrusion detection requires fast and efficient algorithms that can detect and respond to threats in real-time. Future research will explore the use of federated learning for real-time intrusion detection to improve the efficiency and effectiveness of intrusion detection systems in real-world scenarios.

6. HETEROGENEOUS DATA

In a federated learning setting, the data used for training the model is distributed across multiple devices, which may have different characteristics. This can lead to challenges in training a model that can generalize well to all devices. In the case of intrusion detection, devices may have different types of network traffic or different network topologies, which can affect the performance of the model. Existing FL solutions mainly use the same ML/DL model (i.e., all the clients have the same model and same model architecture), where edge devices are highly heterogeneous in terms of hardware (e.g., CPU, memory). Developing the same ML/DL may not be possible on some devices. Moreover, using different models/architectures could help the FL system to benefit from this heterogeneity and hence can increase its performance [49]

7. CONCLUSIONS

Federated learning offers a promising approach to intrusion detection by allowing models to be trained on decentralized data without compromising data privacy. However, there are several challenges that need to be addressed to make federated learning an effective tool for intrusion detection. One of the key challenges is the heterogeneity of data, which can affect the performance of the model. Another challenge is ensuring data privacy in a federated learning setting, which requires the development of secure protocols for data sharing and aggregation. Communication overhead, model heterogeneity, and label imbalance are also challenges that need to be addressed.

Future research in federated learning for intrusion detection should focus on developing more robust algorithms that can handle heterogeneous data and model architectures. Researchers should also continue to investigate new techniques for protecting data privacy and reducing communication overhead. Finally, there is a need for more comprehensive evaluation frameworks that can measure the effectiveness of federated learning approaches for intrusion detection. By addressing these challenges and advancing the state of the art, federated learning has the potential to become a powerful tool for intrusion detection in the years to come. For future research, it is important to solve these problems, which make the global model much less accurate.

REFERENCES

1. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: Techniques, datasets and challenges,” Cybersecurity,vol. 2, no. 1, pp. 1–22, 2019.
2. N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera,and A. Skarmeta, “Distributed real-time SlowDoS attacks detection over encrypted traffic using artificial intelligence,” J. Netw. Comput. Appl., vol. 173, 2021, Art. no. 102871.
3. LiW. et al. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments J. Netw. Comput. Appl.(2020)
4. uoHongzhi *et al* .Vehicular intelligence in 6 g: Networking, communications, and computingVeh. Commun. (2022)
5. ZhouYiqing *et al.*Service-aware 6 g: An intelligent and open network based on the convergence of communication, computing and cachingDigit. Commun. Netw. (2020)
6. https://timesofindia.indiatimes.com/education/news/future-of-internet-of-things-iot-in-india/articleshow/93969472.cms
7. A systematic literature review of methods and datasets for anomaly-based network intrusion detection Comput. Secur. (2022)
8. E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, Opportunities, and Directions,” IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724– 4734, Nov. 2018.
9. M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, ``Challenges and recommended technologies for the industrial Internet of Things: A comprehensive review," Measurement, vol. 151, Feb. 2020, Art. no. 107198.
10. Z. Mahmood, The Internet of Things in the Industrial Sector. Springer, 2019.

11. P. Zhang, Y. Wu, and H. Zhu, ``Open ecosystem for future industrial Internet of Things (IIoT): Architecture and application," CSEE J. Power Energy Syst., vol. 6, no. 1, pp. 111, Mar. 2020.
12. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas,"Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artif. Intell. Statist., 2017, pp. 1273–1282.
13. 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, 2021.
14. Z. Ji, Z. C. Lipton, and C. Elkan, "Differential privacy and machine learning: A survey and review," 2014. [Online]. Available: https://arxiv.org/abs/1412.7584
15. O. Choudhury et al., "Anonymizing data for privacy-preserving federated learning," 2020. [Online]. Available: https://arxiv.org/abs/2002.09096
16. SchmidhuberJ. Deep learning in neural networks: An overview Neural Netw. (2015)
17. AburommanA.A. *et al.* A survey of intrusion detection systems based on ensemble and hybrid classifiers Comput. Secur. (2017)
18. LiY. *et al.*A hybrid malicious code detection method based on deep learning
Int. J. Secur. Appl.**(2015)**
19. AouediO. *et al.* Internet of things and ambient intelligence for mobile health monitoring: A review of a decade of research Int. J. Comput. Inf. Syst. Ind. Manag. Appl.(2018)
20. H. Haddad Pajouh, R. Javadian, R. Khayamiand, A. Dehghantanha, and R. Choo, "A two layer dimension reduction and two tier classification model for anomaly based intrusion detection in IoT backbone networks," IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, 2016.
21. H. H. Pajouh, G. Dastghaibyfard, and S. Hashemi, "Two-tier network anomaly detection model: a machine learning approach," J. Intell. Inf. Syst., pp. 1–14, 2015.
22. Bhattacharya et al.(2020)Bhattacharya, Maddikunta, Kaluri, Singh, Gadekallu, Alazab, Tariq, et al
23. 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," *Mobile Networks and Management (MONAMI)*, vol. 235, pp. 30–44, 2017.
24. R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Physical Communication*, vol. 42, 2020.
25. S. Hosseini, "A new machine learning method consisting of GA-LR and ANN for attack detection," *Wireless Networks*, vol. 26, no. 6, pp. 4149–4162, 2020.
26. B. Molina-Coronado, U. Mori, A. Mendiburu, and J. Miguel-Alonso, "Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2451–2479, 2020

27. Liao, H.-J.; Lin, C.-H.R.; Lin, Y.-C.; Tung, K.-Y. Intrusion detection system: A comprehensive review. *J. Netw. Comput. Appl.* **2013**, *36*, 16–24.
28. Kirvan, P. Single Point of Failure (SPOF). Available online: https://www.techtarget.com/searchdatacenter/definition/Single-point-of-failure-SPOF
29. [Asad et al.(2021)Asad, Moustafa, Ito, and Aslam] Muhammad Asad, Ahmed Moustafa, Takayuki Ito, and Muhammad Aslam. Evaluating the communication efficiency in federated learning algorithms. In 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pages 552–557. IEEE, 2021
30. A. Imteaj, U. Thakker, S. Wang, J. Li, M.H. Amini, Federated learning forresource-constrained IoT devices:Panoramas and state-of-the-art, 2020, ArXiv:2002.10610v1.
31. R. Hu, Y. Guo, E.P. Ratazzi, Y. Gong, Differentially private federated learning forresource-constrained Internet of Things, 2020, arXiv preprint arXiv:2003.12705.
32. J. Hamer, M. Mohri, A.T. Suresh, FedBoost: A communication-efficient algo-rithm for federated learning, in: International Conference on Machine Learning,PMLR, 2020, pp. 3973–3983.
33. Y. Liu, N. Kumar, Z. Xiong, W.Y.B. Lim, J. Kang, D. Niyato, Communication-efficient federated learning for anomaly detection in industrial Internet ofThings, in: GLOBECOM, 2020, 2020, pp. 1–6.
34. Zhang, Chen, Wu, Chen, and Yu] Jiale Zhang, Junjun Chen, Di Wu, Bing Chen, and Shui Yu. Poisoning attack in federated learning using generative adversarial nets. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 374–380. IEEE, 2019b
35. S. AbdulRahman, H. Tout, A. Mourad, C. Talhi, FedMCCS: Multicriteria client selection model for optimal IoT federated learning, IEEE Internet Things J. 8 (6) (2020) 4723–4735.
36. I. Mohammed, S. Tabatabai, A. Al-Fuqaha, F. El Bouanani, J. Qadir, B. Qolomany, M. Guizani, Budgeted online selection of candidate IoT clients to participate in federated learning, IEEE Internet Things J. (2020)
37. P. Kairouz, H.B. McMahan, B. Avent, A. Bellet, M. Bennis, A.N. Bhagoji, K.Bonawitz, Z. Charles, G. Cormode, R. Cummings, et al., Advances and openproblems in federated learning, 2019, arXiv preprint arXiv:1912.04977
38. Mothukuri, Khare, Parizi, Pouriyeh, Dehghantanha, and Srivastava]Viraaji Mothukuri, Prachi Khare, Reza M Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, and Gautam Srivastava. Federated learning-based anomaly detection for iot security attacks. IEEE Internet of Things Journal, 2021a.
39. Arkadiusz Warzynski and Grzegorz ´ Kołaczek. Intrusion detection systems vulnerability on adversarial examples. In 2018 Innovations in Intelligent Systems and Applications (INISTA), pages 1–4. IEEE, 2018

40. Ankit Thakkar and Ritika Lohiya. A review on machine learning and deep learning perspectives of ids for iot: recent updates, security issues, and challenges. Archives of Computational Methods in Engineering, 28(4):3211–3243, 2021.
41. Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.
42. M. Ali, H. Karimipour, M. Tariq, Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges, Comput.Secur. (2021) 102355
43. D.C. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, J. Li, H.V. Poor,Federated learning for Internet of Things: A comprehensive survey, 2021, arXivpreprint arXiv:2104.07914.
44. G. Wood, et al., Ethereum: A secure decentralised generalised transactionledger, Ethereum Proj. Yellow Pap. 151 (2014) (2014) 1–32.
45. Qin, Poularakis, Leung, and Tassiulas] Qiaofeng Qin, Konstantinos Poularakis, Kin K Leung, and Leandros Tassiulas. Line-speed and scalable intrusion detection at the network edge via federated learning. In 2020 IFIP Networking Conference (Networking), pages 352–360. IEEE, 2020
46. Hongyu Li and Tianqi Han. An end-to-end encrypted neural network for gradient updates transmission in federated learning. arXiv preprint arXiv:1908.08340, 2019.
47. Prabadevi, Deepa, Pham, Nguyen, Reddy, Pathirana, Dobre, et al.] B Prabadevi, Natarajan Deepa, Quoc-Viet Pham, Dinh C Nguyen, Thippa Reddy, Pubudu N Pathirana, Octavia Dobre, et al. Toward blockchain for edge-of-things: A new paradigm, opportunities, and future directions. IEEE Internet of Things Magazine, 2021.
48. Alkadi, Moustafa, Turnbull, and Choo] Osama Alkadi, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks. IEEE Internet of Things Journal, 2020
49. Yang, Wang, Xu, Wang, Bian, and Liu] Chengxu Yang, QiPeng Wang, Mengwei Xu, Shangguang Wang, Kaigui Bian, and Xuanzhe Liu. Heterogeneity-aware federated learning. arXiv preprint arXiv:2006.06983, 2020.