

Intelligent, Privacy-Preserving Machine Learning Framework for Security and Intrusion Detection in Large-Scale IoT Networks – A Comprehensive Review

Jhansi Pandiri¹, Dr.P.J.Reginald²

¹ Department of Electronics and Communication Engineering,

Vignan's Foundation for Science, Technology & Research, Vadlamudi, Guntur, India

Department of Electronics and Communication Engineering, Aditya University, Surampalem, India

² Department of Electronics and Communication Engineering,

Vignan's Foundation for Science, Technology & Research, Vadlamudi, Guntur, India

Abstract

The swift growth of the Internet of Things has left a lot to be desired in terms of security with the number of devices it is getting connected to increasing and the data they generate being sensitive. Machine learning-based intrusion detection systems have proven to be a potential solution to the issue of detecting the malicious actions in the IoT environment. The study will offer a comprehensive literature survey of smart privacy-sensitive machine learning systems in intrusion detection in large-scale IoT networks. The research is conducted based on the method involving systematic literature review in the large scientific databases and analysed on the basis of the methods and strategies that preserve privacy and the approaches that identify the intrusions as well. The review presents the energy-efficient privacy-preserving methods to IoT security that are the most commonly used such as federated learning models, blockchain-based privacy models, and differential privacy models, as well as the graph neural network-based models of intrusion detection. The main theme is learning on the field of emerging privacy-preserving machine learning methods to ensure that the IoT environment is secure, and the study also reflects the current research tendencies and shortcomings.

Keywords: Internet of Things, Privacy-preserving Machine Learning, Federated Learning, Intrusion Detection System, Cybersecurity, Differential Privacy Introduction.

1. Introduction

The swift pace of Internet of Things (IoT) has been an enormous breakthrough to the contemporary digital infrastructures that has allowed connecting billions of intelligent devices in a variety of application fields, including healthcare, transport, smarter cities, and industrial automation. These interlinked systems drive up huge amounts of data continuously and transmit via heterogeneous systems, and this compound-raises the challenge of network administration and network security. IoT technologies have a lot of benefits related to automation and efficiency, but they also bring considerable security and privacy risks because the IoT devices do not have much computational power, whereas the interconnected systems create a huge surface of attacks (Ahmadvand et al., 2023) [1]. Elements that pose cyber threats to IoT networks have grown exponentially over the last few years and include

distributed denial-of-service (DDoS) attack, botnet infections, spread of malware, and unauthorised access. Conventional security systems like signature based intrusion detection systems are not very effective in countering advanced attacks because they cannot recognize an attack pattern that has never been witnessed before. Therefore, machine learning and deep learning methods have been extensively used to enhance the level of accuracy of intrusion detection systems (Alfahaid et al., 2025; Ghaffari et al., 2024) [2] [26]. Intrusion detection systems based on machine learning work on the traffic patterns in the network to detect the abnormalities and possible cyber threat. Other models including the convolutional neural networks, recurrent neural networks, and ensemble learning algorithms have been shown to have a promising performance in the detection of anomalies in the IoT networks. Nonetheless, the majority of classical

machine learning frameworks follow concept of centralized training models, in which data of several IoT devices has to be combined in a central server to use them in training. Such a centralized solution provokes significant privacy-related issues since the sensitive user information can be revealed in the process of sharing the data (Ali et al., 2022) [5]. Privacy-preserving machine learning methods have come up as a possible way to overcome these concerns about privacy. Federated learning is one of such techniques, which received significant popularity as it can be used to train machine learning models through collaboration without the necessity to transfer raw data between local devices. In federated learning, devices in IoTs train the models on-Isis then transmit just model parameters to a central aggregation server and, in such a way, ensure that local datasets remain a secret (Awan et al., 2023) [13]. Also, the methods of protecting privacy include differential privacy, homomorphic encryption, secure multi-party computation, which contribute to the improved privacy protection by avoiding the disclosure of sensitive data during the model training (Fouda et al., 2024) [25]. Several privacy-preservation intrusion detection structures found in the recent literature are targeted at the IoT setting. To give an example, it has been suggested to use federated learning-based intrusion detection systems that identify cyber dangers and keep data secret (Khraisat et al., 2025) [44]. Likewise, the methods of blockchain have also been proposed to guarantee secure communication and management of trust between the IoT devices (Bezanjani et al., 2024) [16]. Moreover, more sophisticated methods have been implemented to process the network architecture and reveal abnormal behaviour of large-scale IoT networks, including the use of graph neural networks (Pei et al., 2024) [59]. Although these developments have been undertaken, a number of challenges still exist in the design of effective privacy saving intrusion detection systems in IoT networks. These are problems such as communication overhead during federated learning, susceptibility to model poisoning attacks, data heterogeneity on the device, and IoT devices lack enough computing capabilities (Vyas et al., 2024) [71]. Thus, available privacy-saving machine learning models should be thoroughly examined in order to define research gaps and directions of further research. The given paper is going to present a systematic review of intelligent privacy-preserving machine learning systems to detect intrusion in massive IoT networks.

The study provides an analysis of recent research contributions, such central techniques applied regarding the protection of privacy, and open research issues in the field.

The primary contributions of this review paper can be summarized as the following ones:

- An overview of the privacy-sensitive machine learning algorithms applied on intrusion detection of an IoT network.
- Federated learning architecture study and how it can be used in the security of distributed IoT.
- Determination of the existing research pitfalls and shortcomings of the privacy-preserving IoT security frameworks.
- Minor consideration on future research directions in the strong and scalable lot intrusion detection systems.

2. Research Methodology

The research method proposed in this study will be a systematic literature review to examine the current studies associated with privacy-aware machine learning architecture to use in intrusion sensors in IoT networks. The procedure of review is based on the PRISMA transparency and reproducibility requirements of the systematic review and meta-analysis in order to be transparent and reproducible on matters of selection and appraisal of relevant studies.

2.1. Search Strategy

In the literature search, the researcher used a number of scientific databases, such as IEEE Xplore, Scopus, SpringerLink, ScienceDirect, and Google Scholar. To obtain the latest trends in machine learning privacy and IoT security, the search was limited to articles published since 2021.

The keywords that were used during search included the following:

- "IoT intrusion detection"
- "Privacy-preserving machine learning"
- "Federated learning IoT security"
- "Differential privacy intrusion detection"
- "Graph neural network intrusion detection"

The keywords were used in combination with Boolean operators to access the research articles that were related.

2.2. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria used in this study are summarized in Table 1.

Table 1. Inclusion and Exclusion Criteria for the Study

Inclusion Criteria	Exclusion Criteria
Articles published between 2021 and 2026	Non-English publications
Studies related to IoT security or intrusion detection	Articles unrelated to IoT networks
Studies focusing on privacy-preserving machine learning	Editorial notes and short papers
Articles published in peer-reviewed journals	Duplicate studies

2.3. Screening Method

Relevant research articles were filtered through PRISMA screening process in order to use them in this study. To begin with, database searches were conducted in order to identify a huge number of studies. All the articles were filtered out after eliminating the duplicate studies and then their titles and abstracts. Only the full-text analysis was performed in order to know whether the studies met the incorporation criterion or not.

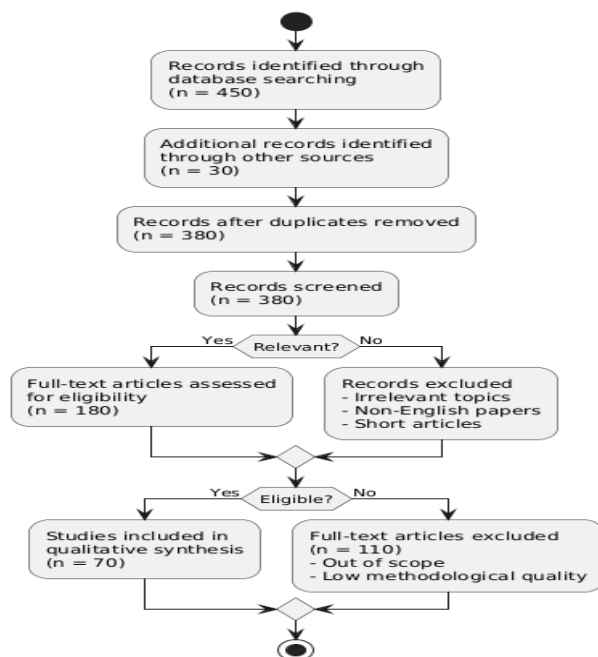


Figure 1. PRISMA flow diagram illustrating the study selection process

3. Bibliometric Overview of Research on Privacy-Preserving IoT Security

With the growing use of the Internet of Things (IoT) technologies, the research in the field of cybersecurity and machine learning that conserves privacy has recently broadened considerably. During the last ten years, the number of publications devoted to the implementation of the intelligent mechanisms of intrusion detection and privacy-protecting systems increased to ensure the security of giant IoT systems. It is this fast development of distributed machine learning method that, especially federated learning, has allowed researchers to create collaborative intrusion detection systems without involving direct exchange of sensitive information of the participating devices. Recent research has shown that machine learning methods that support the privacy issue are becoming more significant in the security of IoT infrastructures. As an illustration, federated learning is the very popular model that allows distributed training of intrusion detection models on several IoT nodes without sharing data in the air (Awan et al., 2023) [13]. Likewise, machine learning models have been trained with the use of differential privacy in place of sensitive information being leaked during training and inference (Fouda et al., 2024) [25]. Another unfulfilled research gap in the literature is the integration of sophisticated machine learning systems with privacy protection systems. Convolutional neural network (CNN), recursive neural network (RNN), and graph neural network (GNN) are among the deep learning methods that have been applied to discover network traffic patterns in IoT settings that are too complicated. These models enhance the improved identification of cyber threats unlike the previous rule-based intrusion detection systems (Ghaffari et al., 2024) [26].

Moreover, it has been suggested to combine the blockchain technology with the federated learning to enhance the issue of trust management and secured information exchange in the distributed IoT networks. Blockchain-related frameworks provide the transparency and non-alterability of model changes in the process of collaborative learning (Bezanjani et al., 2024) [16]. Moreover, more recent research points to the possibility of lightweight machine learning models that will target resource-constrained IoT devices, in particular (Alfahaid et al., 2025) [2]. The increase in the number of research papers in this field proves the rise in the interest towards privacy-saving cybersecurity

solutions to IoT networks. The reasons why this trend is occurring are due to the intensive growth of the smart devices and the necessity to have secure data processing of the data in the distributed environment.

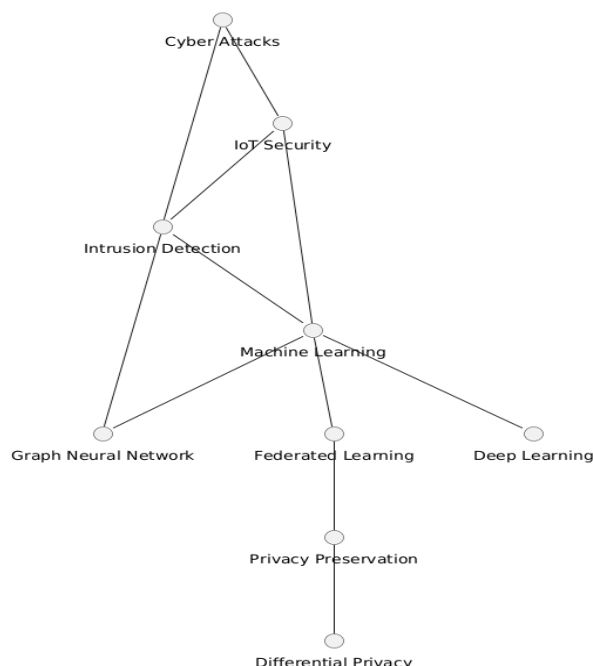


Figure 2. Bibliometric keyword network illustrating major research themes in privacy-preserving machine learning for IoT security

4. Review and Results

This section comprises a literature review of the current research studies pertaining to privacy preserving machine learning architectures in intrusion detection in the IoT networks. Although the reviewed literature pays attention to a range of issues, such as the security of IoT, machine learning-inspired intrusion detection system, federated learning architecture, privacy-mechanism, and graph-based intrusion detection system.

4.1. IoT Security and Intrusion Detection

The recent proliferation of IoT devices has posed many security challenges since the environment of the IoT is heterogeneous and that most of the devices do not have adequate computing capabilities. There are many cyberattacks that IoT networks are very compromised to, including the distributed denial-of-service (DDoS) attacks, the propagation of malware, spoofing attacks, and the infection of botnets. The conventional security controls are in most cases not effective in securing such networks because of their inefficiency in identifying the novel attack trends (Ahmadvand et al., 2023) [1]. The intrusion detection systems are essential in detecting

activities conducted by malicious persons within the IoT networks. Such systems observe the network traffic and study behavioural patterns to identify anomalies and possible cyber dangers. The traditional intrusion detection systems can be detailed into two distinct groupings which include the signature-based detection and the anomaly-based detection. The signature-based approach is based on a set of attack signatures that are used to identify threats, and the anomaly-based approach is based on machine learning algorithms that are used to detect abnormal behaviour (Elsayed et al., 2023) [21]. The applications of machine learning in intrusion detection systems have been receiving a lot of attention as a result of their capability to analyse advanced network traffic patterns to identify advanced cyber threats. Different machine learning, including decision trees, support vectors, and neural networks, have been used to enhance the accuracy of detection in an IoT setup (Alfahaid et al., 2025)[2]. It has also applied deep learning models to identify the high level features of network traffic data so that it can be more efficient in detecting the emergent cyber threats (Mohamed, 2025) [28]. Nevertheless, a number of machine learning-based intrusion detector systems are centralised in the collection of data to train the model, and hence, privacy is a big concern. The IoT devices might create sensitive information that can be revealed in the process of data transmission and data storage. This also means that privacy-protective machine learning solutions are a potentially beneficial answer to responsible intrusion detection over IoT networks (Ali et al., 2025) [6].

Table 2. Summary of Selected Studies on IoT Intrusion Detection

Author	Methodology	Key Contribution
Alfahaid et al. (2025)	Machine learning IDS	Comprehensive overview of ML-based IoT security solutions
Ghaffari et al. (2024)	Deep learning survey	Review of ML and DL methods for IoT security
Elsayed et al. (2023)	Deep learning IDS	Automatic intrusion detection framework
Mohamed (2025)	AI cybersecurity	Analysis of AI-based intrusion detection models

4.2. Machine Learning-Based Intrusion Detection

The most popular IoT network detection methods are now formulated through machine learning. However, in contrast to the antique rule-based security systems, machine learning models have self-learning capabilities that can recognize patterns by traffic data on the network and detect suspicious behaviours that can be traced back to cyberattacks. Learning algorithms (i.e., decision trees, random forests, support vector machines, etc.) under a supervised learning method have been extensively used to classify network traffic and determine normal and malicious traffic. These algorithms are based on labelled datasets through which they train models that detect patterns of attacks that are known. Nevertheless, supervised learning models usually have challenges in identifying attack cases in zero-days because they rely on labelled training data (Noor et al., 2025) [57]. Clustering and autoencoders are also methods of unsupervised learning that have been used to find anomalies in network traffic even without labelled data. These models examine the statistical trends in network traffic and determine the difference that could signal the possibility of a cyber threat. The hybrid approaches that put together supervised and unsupervised learning have been observed to be more effective in the detection of complex attacks on IoT networks (Kalodanis et al., 2025) [40]. There are also recent works that considered applying large language models and transformer-based models to cybersecurity applications. These models show potential abilities of analysing network data volumes and recognizing sophisticated patterns of attacks within a distributed IoT (Ferrag et al., 2024) [24]. In spite of the above developments, centralised machine learning models

continue to require serious privacy issues. In data aggregation processes sensitive information can be leaked and such may result in a violation of privacy and regulatory compliance problems. Federated learning has come as a potential solution to these issues to make use of a distributed machine learning system that preserves privacy to detect intrusion.

4.3. Federated Learning for Privacy-Preserving Intrusion Detection

The field of federated learning has become a potentially promising distributed machine learning method that allows joint training of models without having to collect data centrally. In this model various IoT devices are trained on local machine learning models with their own data, and only transfer model parameters to a central aggregation server. This is a decentralized training process that supports the privacy of sensitive data that is produced by the IoT devices (Ali et al., 2022) [5]. A number of papers have offered federated learning based intrusion detection systems to the IoT setting. As an example, Khraisat et al. (2025) [44] have recently proposed a federated learning model that will allow collaborative identification of threats between distributed IoT networks without violating the privacy of data. On the same note, Mahmud et al. (2024) [50] proposed a privacy-saving federated learning model that was meant to identify cyber threats in cyber-physical systems. Moderate current studies had also investigated the combination of blockchain technology and federated learning to enhance the management of trust and model sharing in the distributed network. Frames of blockchains offer a record of updates of models that is impossible to alter and provide transparency during the collaborative training procedures (Moulahi et al., 2023)[54].

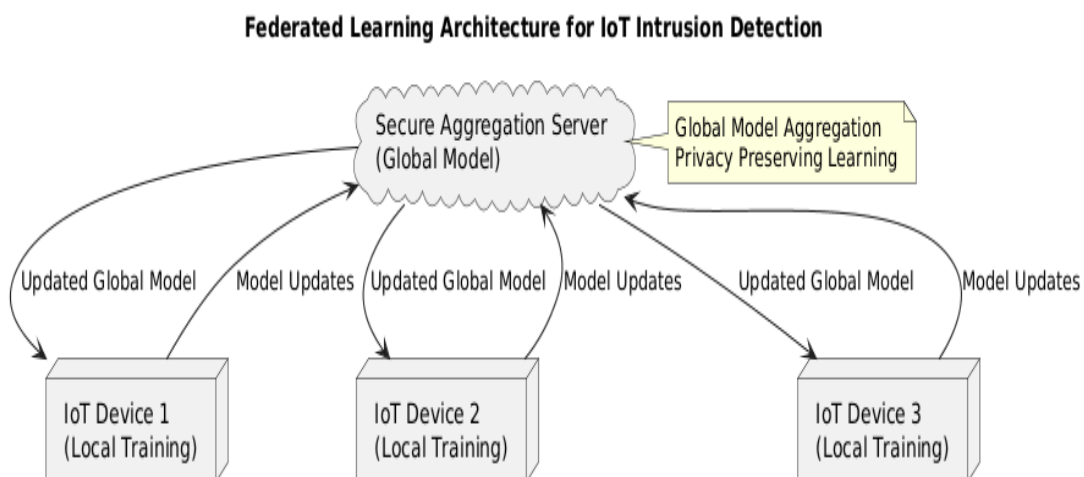


Figure 3. Federated learning architecture for privacy-preserving intrusion detection in IoT networks

4.4. Privacy-Preserving Techniques in Machine Learning

The concept of privacy is one of the major demands in machine learning systems that are based on IoT because the kinds of data produced by the connected devices are quite sensitive. There are a number of solutions that have been suggested to preserving the privacy of the users when training and performing machine learning. One of the most prevalent privacy-preserving methods is the so-called differential privacy. It adds noise to datasets or model parameters randomly to avoid that a single data point should be identified without affecting the overall statistical characteristics of the data (Zhang and Li, 2024) [75]. Homomorphic encryption enables the use of machine learning computations on encrypted data without having to join with the decryption of the encrypted data. The method is used to ensure that data processes the information in a sensitive manner (Alqazzaz, 2025) [8]. Another privacy-saving methodology is called secure multi-party computation when different parties can emerge as a result of collaboratively computing machine learning models without exposing their private information to anybody. The method comes in handy especially in a collaborative mode in intrusion detection that involves multiple organisations leading to sharing of security knowledge without divulging sensitive information (Liu et al., 2022) [49].

Table 3. Comparison of Privacy-Preserving Techniques

Technique	Key Advantage	Limitation
Differential Privacy	Protects individual data privacy	May reduce model accuracy
Homomorphic Encryption	Enables computation on encrypted data	High computational cost
Secure Multi-party Computation	Secure collaborative computation	Communication overhead
Federated Learning	Decentralized training	Vulnerable to poisoning attacks

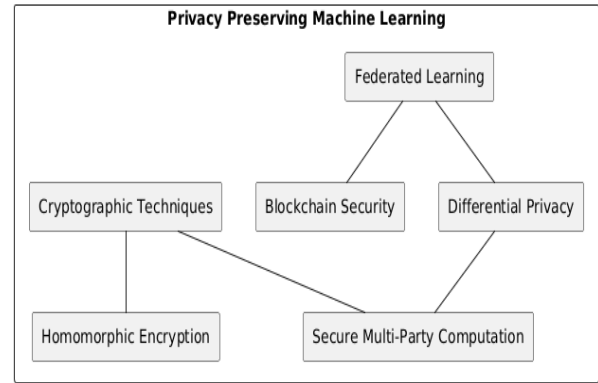


Figure 4. Taxonomy of privacy-preserving machine learning techniques for secure IoT intrusion detection

4.5. Graph Neural Network-Based Intrusion Detection

GNNs have recently been the focus of the analysis of complicated network structure in the domain of cybersecurity. This is because IoT networks are naturally graphical in nature, with nodes calling out devices and the outgoing communication connections between devices being the connections forming the edges. GNNs have the capability of relating the structural associations among entities in a network and identifying maladaptive patterns of communications that can be a sign of a cyberattack. The recent studies have proven that the use of GNN-based intrusion detection systems has the potential to discover the presence of botnet operations, malware propagation, and organized cyberattacks within massive IoT (Pei et al., 2024) [59].

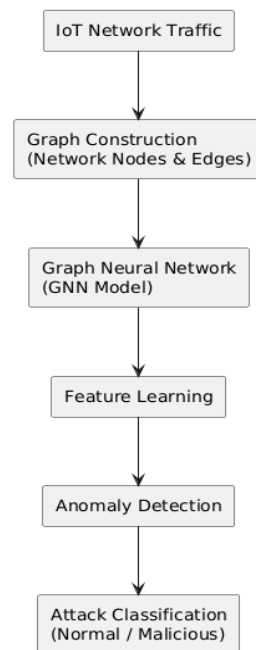


Figure 5. Graph neural network based intrusion detection framework

Table 4: Summary of Reviewed Studies on Privacy-Preserving Machine Learning for IoT Security

Author	Methodology	Key Findings / Contribution
Ahmadvand et al. (2023)	Survey on SDN-based IoT security	Identified key privacy challenges in SDN-IoT environments and proposed secure data protection mechanisms.
Alabdulatif (2025)	Federated learning with differential privacy	Introduced GuardianAI framework for privacy-preserving anomaly detection.
Alazab et al. (2023)	Federated intrusion detection	Demonstrated improved IDS accuracy using distributed federated learning models.
Alfahaid et al. (2025)	Machine learning security survey	Provided comprehensive overview of ML-based IoT cybersecurity solutions.
Ali et al. (2022)	Federated learning survey	Examined privacy-preserving learning techniques for healthcare IoT systems.
Ali et al. (2025)	Privacy-preserving ML for smart grids	Proposed secure machine learning framework for IoT-enabled smart grid systems.
Alqazzaz (2025)	Federated learning + homomorphic encryption	Developed privacy-preserving framework for smart city applications.
Alqazzaz (2026)	Adaptive federated anomaly detection	Introduced SecuFL-IoT architecture for secure industrial IoT environments.
Alrayes et al. (2025)	Statistical learning with optimization	Proposed privacy-preserving big data security model for IoT networks.
Alshdadi et al. (2025)	Federated deep learning	Designed scalable framework for detecting DDoS attacks in IoT networks.
Awan et al. (2023)	Federated learning + cryptography	Demonstrated secure big data analysis for IoT cybersecurity systems.
Baidar et al. (2025)	Hybrid deep learning + federated learning	Proposed intrusion detection system for IoT/5G edge computing environments.
Bezanjani et al. (2024)	ML + blockchain security	Introduced blockchain-based privacy-preserving data sharing architecture.
Briggs et al. (2021)	Federated learning survey	Reviewed privacy-preserving collaborative learning approaches in IoT.
Chandu et al. (2025)	Distributed federated IDS	Proposed collaborative security model for IoT threat detection.
Elsayed et al. (2023)	Deep learning intrusion detection	Developed automated IDS for IoT and SDN environments.
Fagbohunbe et al. (2021)	Edge intelligent computing	Proposed privacy-preserving edge computing framework for IoT devices.
Farooq et al. (2025)	Interpretable federated learning	Designed interpretable cyber-threat detection model for smart cities.
Ferrag et al. (2024)	BERT-based security model	Introduced lightweight language model for IoT threat detection.
Fouda et al. (2024)	Survey on privacy-preserving learning	Reviewed data-driven privacy protection mechanisms in communication networks.

Author	Methodology	Key Findings / Contribution
Ghaffari et al. (2024)	Machine learning survey	Examined ML and DL approaches for securing IoT infrastructures.
Gnanzou (2025)	Federated IDS architecture	Proposed scalable intrusion detection model for distributed IoT networks.
Hamad et al. (2025)	Federated IDS systematic analysis	Reviewed multiple federated learning IDS frameworks.
Harahsheh et al. (2024)	Federated transfer learning	Proposed real-time intrusion detection model for IoT networks.
He et al. (2023)	Federated deep learning	Developed privacy-preserving industrial IoT intrusion detection system.
Hilal et al. (2022)	Deep learning IIoT security	Proposed intelligent privacy-preserving intrusion detection model.
Holubenko et al. (2025)	Decentralized intrusion detection	Introduced autonomous privacy-preserving IDS for IoT environments.
Hossain & Islam (2025)	Federated botnet detection	Developed decentralized cybersecurity framework using federated learning.
Huang et al. (2024)	Hybrid deep learning + FL	Proposed improved intrusion detection architecture using federated training.
Islam et al. (2025)	Hierarchical federated learning	Introduced PP-HFFL framework for IoT intrusion detection.
Kalodanis et al. (2025)	ML-based IDS for 5G	Proposed adaptive intrusion detection approach for next-generation networks.
Khraisat et al. (2025)	Federated intrusion detection	Designed privacy-preserving IDS architecture for IoT networks.
Liu et al. (2022)	Secure aggregation survey	Reviewed privacy-preserving model aggregation techniques in federated learning.
Mahmud et al. (2024)	Federated IDS for cyber-physical systems	Proposed privacy-preserving machine learning detection framework.
Mosaiyebzadeh et al. (2024)	Federated IoHT intrusion detection	Introduced secure IDS for Internet of Health Things devices.
Moulahi et al. (2023)	Blockchain + federated learning	Proposed blockchain-based privacy-preserving cyber threat detection framework.
Pei et al. (2024)	Graph neural network IDS	Developed privacy-preserving GNN model for network intrusion detection.
Rampone et al. (2025)	Hybrid federated learning IDS	Proposed near real-time privacy-preserving intrusion detection model.
Raza et al. (2024)	Federated learning for SDN security	Developed privacy-preserving IDS for software-defined networks.
Tabassum et al. (2021)	Distributed incremental IDS	Proposed privacy-preserving collaborative intrusion detection framework.
Vyas et al. (2024)	Federated learning survey	Reviewed privacy-preserving intrusion detection techniques in IoT environments.

5. Discussion

Productive development of Internet of Things (IoT) technologies has established a more intricate cybersecurity environment. As billions of connected devices continuously communicate sensitive information, securing communication and good threat detection has made it a critical issue. Intrusion detection systems utilizing machine learning have become one of the potential solutions that could be applied to detect a cyber threat within an IoT environment. Nevertheless, the high level of centralization of most machine learning models, creates serious security concerns considering that any sensitive information produced by the IoT devices would have to be shared with virtual centralized servers in order to train and analyze them.

The recent studies have been directed at merging privacy-preserving mechanism with machine learning practices that will enable to overcome those predicaments. Federated learning has become a focus in the research since it is a form of decentralized training where several devices join to jointly train machine learning models without exchanging raw data. Federated learning Systems Federated learning takes place in an environment where the local devices are trained on their own datasets and only send the model updates to a central aggregation server. This technology minimizes the chances of leakages of data and enhances privacy security in distributed internet of things (Awan et al., 2023; Ali et al., 2022) [13] [5].

A number of studies have proved that federated learning is useful in enhancing the security of the IoT networks. As the example, intrusion detection frameworks based on federated learning have been created to identify cyber threats on distributed IoT devices and maintain their data privacy (Khraisat et al., 2025) [44]. In the same way, the current studies covered hierarchical federated learning frameworks aimed at enhancing the effectiveness and scalability of a large-scale IoT system (Islam et al., 2025) [37]. These models allow the cooperative learning between many edge devices with the minimization of communication overhead.

Beyond federated learning, there are a number of other privacy preserving methods that are also implemented in machine learning systems of IoT security. Differential privacy is extensively applied to avoid the exposure of

individual data points in training a model through the use of controlled noise in model training. Such a methodology can be used to secure vulnerable data and to achieve reasonable rates of model performance (Zhang and Li, 2024) [75]. Secure collaboration learning is also possible with the help of homomorphic encryption and secure multi-party computation without revealing the personal information (Liu et al., 2022) [49].

The use of graph neural networks in detection of intrusion is yet another new trend in the study of IoT security. Graph neural networks unlike the traditional machine learning models can analyze the complexity in the networks and detect patterns of abnormal communication between devices. These models are effective especially in the detection of distributed attacks like botnets and well-organized malware distribution in large-scale IoT networks (Pei et al., 2024) [59].

In addition, the recent studies have discussed how the blockchain technology may be applied in integration with privacy-protecting machine learning models. Decentralized management of trust (as well as secure storage of model updates) is a feature offered by blockchain-based architectures when it comes to collaborative learning processes. This can be used to enhance transparency and the ability to withstand model poisoning attacks (Bezanjani et al., 2024)[16].

With these developments, a number of obstacles have been experienced in the implementation of privacy enhancing machine learning frameworks to protect the IoT. Among the key issues, it is possible to mention a great communication overhead of federated learning, especially in the large-scale context of an IoT system with thousands of devices involved in the joint training. Furthermore, federated learning systems can fall prey to model poisoning and data manipulation as an example of adversarial attacks, which are likely to negatively affect the quality of a model and endanger data security (Fouda et al., 2024)[25].

The second obstacle is that most of the IoT devices have limited computational capabilities that limit the complexity of machine learning models that can execute locally. There are lightweight machine learning architectures and edge computing designs under consideration to handle this problem, but it is necessary

to carry out further research to enhance the efficiency and scalability (Alfahaid et al., 2025)[2].

In general, the literature under review shows that machine learning that ensures privacy has great potential to enhance the security of IoT networks. Nevertheless, enhancing studies are needed to manage the lack of robustness and limit the research on intrusion detection systems in large-scale IoT setups.

5.1. Research Gap

According to the systematic review of the available literature, one can define some gaps in the research in the context of privacy-preserving machine learning in the spheres of detecting intrusions in IoT.

To begin with, despite the promising outcomes of federated learning on a distributed intrusion detection system, most of the current systems are tested on a small-scale data set and within a controlled laboratory setting. Large-scale real-world assessments have not investigated the applicability of federated learning to demonstrate its efficacy in the real-world use of IoT.

Second, it is not well studied how to combine GNN with federated learning. Although it has been demonstrated that graph neural networks are especially promising when it comes to analysis of network structures, a relatively small number have been used with privacy-preserving learning models in order to enhance the accuracy of intrusion detection.

Third, most privacy-beneficial machine learning frameworks are much more concerned with ensuring that the privacy of data is upheld, yet pay insufficient attention to adversarial attacks like model poisoning and inference attacks. These vulnerabilities to security may cause a serious effect on the reliability of collaborative learning systems.

Fourth, an efficient communication is one of the significant issues with federated learning systems. Running large-scale IoT networks may pose a considerable overhead to the network when model parameters can be exchanged regularly between devices and central servers.

Lastly, the majority of the current literature deals with particular fields of applications, including healthcare IoT or smart-city intonations, and the overall security frameworks that can be applied to heterogeneous IoT environments are not well covered.

The need to address these research gaps will help in coming up with a strong and scalable privacy-preserving intrusion detection systems that would prevent the next generation of IoT networks.

6. Conclusion

The fast growth of the Internet of Things technologies has posed some critical security problems as more and more connected gadgets are becoming available along with the sensitive content they produce. Conventional security tools cannot help in these challenges especially in large information of the IoT where cyber threats are becoming more advanced.

Intrusion detection systems based on machine learning have become influential with regard to discovering the malicious activities on the IoT networks. These systems are power to analyze the network traffic pattern and identify the anomalies that can signify the possibility of cyber threats. Nonetheless, the centralized machine learning methods have most frequently been associated with concerns on privacy since sensitive information would necessarily be exchanged with the centralized servers where training would occur.

As a reassuring sign to these privacy challenges, privacy-preserving machine learning methods, such as federated learning, differential privacy, homomorphic encryption, and secure multi-party computation have been suggested as promising solutions to these challenges. Federated learning has been one of such methods, with a considerable amount of attention generally because of a capability of collaboratively training a model without necessarily exchanging raw data between devices.

Based on the reviewed literature in this study, it is seen that machine learning structures that safeguard privacy can influence the safety of the IoT network significantly and keep information confidential. As well, there is a new opportunity with new technical solutions like graph neural networks and blockchain-based architecture to boost the intrusion detection performance and enhance the system security of distributed learning.

Even with these developments there are a few challenges to the development of efficient and scalable privacy preserving intrusion detection systems. Such challenges are communication overhead, sensitivity to adversarial attacks, constraints of computational capabilities of the IoT devices and the absence of common evaluation frameworks.

The future studies need to implement lightweight machine learning models, enhance the efficiency of federated learning communication and combine novel approaches of deep learning, including graph neural networks, and build effective defense systems against adversarial attacks. It will be important to address these challenges to create privatized, scalable and security conscious IoT ecosystems.

To sum up, privacy-saving machine learning frameworks are another significant element in the IoT cybersecurity future. Further research on this subject will be instrumental in the provision of security and reliability of the next generation interconnected systems.

Reference

- [1] Ahmadvand, H., Lal, C., Hemmati, H., Sookhak, M., & Conti, M. (2023). Privacy-preserving and security in SDN-based IoT: A survey. *IEEE Access*, 11, 44772-44786.
- [2] Alabdulatif, A. (2025). GuardianAI: Privacy-preserving federated anomaly detection with differential privacy. *Array*, 26, 100381.
- [3] Alazab, A., Khraisat, A., Singh, S., & Jan, T. (2023). Enhancing privacy-preserving intrusion detection through federated learning. *Electronics*, 12(16), 3382.
- [4] Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., & Mahgoub, I. (2025). Machine learning-based security solutions for iot networks: A comprehensive survey. *Sensors*, 25(11), 3341.
- [5] Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE journal of biomedical and health informatics*, 27(2), 778-789.
- [6] Ali, M., Suchismita, M., Ali, S. S., & Choi, B. J. (2025). Privacy-preserving machine learning for IoT-integrated smart grids: Recent advances, opportunities, and challenges. *Energies*, 18(10), 2515.
- [7] Alonge, M., & Isreal, O. (2025, May). *Federated learning for Privacy-Preserving intrusion detection in VANETs*.
- [8] Alqazzaz, A. (2025). Federated learning with homomorphic encryption: A privacy-preserving solution for smart cities. *International Journal of Computational Intelligence Systems*, 18(1), 304.
- [9] Alqazzaz, A. (2026). SecuFL-IoT: an adaptive privacy-preserving federated learning framework for anomaly detection in smart industrial networks. *Scientific Reports*.
- [10] Alrayes, F. S., Maray, M., Alshuhail, A., Almustafa, K. M., Darem, A. A., Al-Sharafi, A. M., & Alotaibi, S. D. (2025). Privacy-preserving approach for IoT networks using statistical learning with optimization algorithm on high-dimensional big data environment. *Scientific reports*, 15(1), 3338.
- [11] Alshdadi, A. A., Almazroi, A. A., Ayub, N., Lytras, M. D., Alsolami, E., Alsubaei, F. S., & Alharbey, R. (2025). Federated deep learning for scalable and privacy-preserving distributed denial-of-service attack detection in internet of things networks. *Future Internet*, 17(2), 88.
- [12] Aramide, O. O. (2025). Federated Learning for Distributed Network Security and Threat Intelligence: A Privacy-Preserving Paradigm for Scalable Cyber Defense. *Journal of Data Analysis and Critical Management*, 1(02).
- [13] Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. (2023). Privacy-preserving big data security for IoT with federated learning and cryptography. *IEEE access*, 11, 120918-120934.
- [14] Baidar, R., Maric, S., & Abbas, R. (2025). Hybrid deep learning-federated learning powered intrusion detection system for iot/5g advanced edge computing network. *arXiv preprint arXiv:2509.15555*.
- [15] Baidar, R., Maric, S., & Abbas, R. (2025). Hybrid deep learning-federated learning powered intrusion detection system for iot/5g advanced edge computing network. *arXiv preprint arXiv:2509.15555*.
- [16] Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2024). Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the Internet of Things. *The Journal of Supercomputing*, 80(17), 24975-25003.
- [17] Boutassetta, M., Makhoulouf, A., Messaoudi, N., Benmachiche, A., Boutabia, I., & Derdour, M. (2025, October). Cyberattack Detection in Smart Cities Using AI: A literature review. In *2025 International Conference on Networking and Advanced Systems (ICNAS)* (pp. 1-9). IEEE.
- [18] Briggs, C., Fan, Z., & Andras, P. (2021). A review of privacy-preserving federated learning for the Internet-of-Things. *Federated learning systems: towards next-generation AI*, 21-50.
- [19] Chandu, G., Karthik, T., & Parag, B. (2025). Federated learning for distributed IoT security: A

- privacy-preserving approach to intrusion detection. *IEEE Access*.
- [20] Elijah, T. D., Samuel, A. A., & Familusi, O. B. (2025). AI-Powered Intrusion Detection and Prevention Systems for the Next Generation Network. *Path of Science*, 11(10), 2001-2009.
- [21] Elsayed, R. A., Hamada, R. A., Abdalla, M. I., & Elsaid, S. A. (2023). Securing IoT and SDN systems using deep-learning based automatic intrusion detection. *Ain Shams Engineering Journal*, 14(10), 102211.
- [22] Fagbohunge, O., Reza, S. R., Dong, X., & Qian, L. (2021). Efficient privacy preserving edge intelligent computing framework for image classification in IoT. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 6(4), 941-956.
- [23] Farooq, M. S., Saleem, M., Khan, M. A., Khan, M. F., Siddiqui, S. Y., Aslam, M. S., & Adnan, K. M. (2025). Interpretable Federated Learning Model for Cyber Intrusion Detection in Smart Cities with Privacy-Preserving Feature Selection. *Computers, Materials, & Continua*, 85(3), 5183.
- [24] Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing cyber threat detection with large language models: A privacy-preserving bert-based lightweight model for iot/iiot devices. *IEEE Access*, 12, 23733-23750.
- [25] Fouda, M. M., Fadlullah, Z. M., Ibrahim, M. I., & Kato, N. (2024). Privacy-preserving data-driven learning models for emerging communication networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 27(4), 2505-2542.
- [26] Ghaffari, A., Jelodari, N., Poralish, S., Derakhshanfard, N., & Arasteh, B. (2024). Securing internet of things using machine and deep learning methods: a survey. *Cluster Computing*, 27(7), 9065-9089.
- [27] Gnanzou, D. (2025). Federated Learning for Enhanced Intrusion Detection in IoT Networks: A Privacy-Preserving and Scalable Approach. *JANOLI International Journal of Big Data*, 1(2).
- [28] Hamad, N. A., Bakar, K. A., Qamar, F., Jubair, A. M., Mohamed, R. R., & Mohamed, M. A. (2025). Systematic analysis of federated learning approaches for intrusion detection in the Internet of Things environment. *IEEE Access*.
- [29] Hameed, K., Maqsood, F., Patwary, M. A. K., Zhenfie, W., & Sarwar, R. A Scalable Privacy-Preserving Artificial Intelligence Framework for Real-Time Threat Detection in Internet of Things Systems. Available at SSRN 5228905.
- [30] Harahsheh, K., Alzaqebah, M., & Chen, C. H. (2024). An enhanced real-time intrusion detection framework using federated transfer learning in large-scale IoT networks. *Science and Information Organization*, 15(12).
- [31] Harahsheh, K., Alzaqebah, M., & Chen, C. H. (2024). An enhanced real-time intrusion detection framework using federated transfer learning in large-scale IoT networks. *Science and Information Organization*, 15(12).
- [32] He, N., Zhang, Z., Wang, X., & Gao, T. (2023). Efficient Privacy-Preserving Federated Deep Learning for Network Intrusion of Industrial IoT. *International Journal of Intelligent Systems*, 2023(1), 2956990.
- [33] Hilal, A. M., Alzahrani, J. S., Abunadi, I., Nemri, N., Al-Wesabi, F. N., Motwakel, A., ... & Zamani, A. S. (2022). Intelligent deep learning model for privacy preserving IIoT on 6G environment. *Computers, Materials, & Continua*, 72(1), 333.
- [34] Holubenkov, V., Gaspar, D., Leal, R., & Silva, P. (2025). Autonomous intrusion detection for IoT: a decentralized and privacy preserving approach. *International Journal of Information Security*, 24(1), 7.
- [35] Hossain, M. A., & Islam, M. S. (2025). Towards decentralized cybersecurity: a novel privacy-preserving federated learning approach for botnet attack detection. *Blockchain: Research and Applications*, 100355.
- [36] Huang, J., Chen, Z., Liu, S. Z., Zhang, H., & Long, H. X. (2024). Improved intrusion detection based on hybrid deep learning models and federated learning. *Sensors*, 24(12), 4002.
- [37] Islam, M. M., Abdullah, W. M., & Saha, B. N. (2025). Privacy-preserving hierarchical fog federated learning (PP-HFFL) for IoT intrusion detection. *Sensors*, 25(23), 7296.
- [38] Islam, N., & Zulkernine, M. (2025). Privacy-preserving machine learning in internet of vehicle applications: Fundamentals, recent advances, and future direction. *arXiv preprint arXiv:2503.01089*.
- [39] Islam, U., Ullah, H., Khan, N., Ahmad, I., & Saleem, K. (2025). Adaptive Federated Learning Framework for Privacy-Preserving Consumer-

- Centric IoMT: A Novel Secure Data Collaboration Model. *IEEE Transactions on Consumer Electronics*.
- [40] Kalodanis, K., Papapavlou, C., & Feretzakis, G. (2025). Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention. *Future Internet*, 17(7), 312.
- [41] Kaur, R., Rodrigues, T., Kadir, N., & Kashef, R. (2025). A Survey on Privacy Preservation Techniques in IoT Systems. *Sensors (Basel, Switzerland)*, 25(22), 6967.
- [42] Khan, A., & Adnan, K. M. (2025). Big Data-Driven Federated Learning Model for Scalable and Privacy-Preserving Cyber Threat Detection in IoT-Enabled Healthcare Systems.
- [43] Khan, H., Tejani, G. G., AlGhamdi, R., Alasmari, S., Sharma, N. K., & Sharma, S. K. (2025). A secure and efficient deep learning-based intrusion detection framework for the internet of vehicles. *Scientific Reports*, 15(1), 12236.
- [44] Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S., & Jan, T. (2025). Federated learning for intrusion detection in iot environments: a privacy-preserving strategy. *Discover Internet of Things*, 5(1), 72.
- [45] Kumar, P., Tripathi, R., & P. Gupta, G. (2021, January). P2IDF: A privacy-preserving based intrusion detection framework for software defined Internet of Things-fog (SDIoT-Fog). In *Adjunct proceedings of the 2021 international conference on distributed computing and networking* (pp. 37-42).
- [46] Latif, N., Ma, W., & Ahmad, H. B. (2025). Advancements in securing federated learning with IDS: a comprehensive review of neural networks and feature engineering techniques for malicious client detection. *Artificial Intelligence Review*, 58(3), 91.
- [47] Li, H., Ge, L., & Tian, L. (2024). Survey: federated learning data security and privacy-preserving in edge-Internet of Things. *Artificial Intelligence Review*, 57(5), 130.
- [48] Li, J., Sun, Q., & Sun, F. (2023). Enhancing privacy-preserving intrusion detection in blockchain-based networks with deep learning. *Data Science Journal*, 22(1).
- [49] Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K. Y., & Zhao, J. (2022). Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data*.
- [50] Mahmud, S. A., Islam, N., Islam, Z., Rahman, Z., & Mehedi, S. T. (2024). Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems. *Mathematics*, 12(20), 3194.
- [51] Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 67(8), 6969-7055.
- [52] Mosaiyebzadeh, F., Pouriyeh, S., Han, M., Liu, L., Xie, Y., Zhao, L., & Batista, D. M. (2024). Privacy-preserving federated learning-based intrusion detection system for iot devices. *Electronics*, 14(1), 67.
- [53] Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S., & Rizwan, M. (2023). Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Systems*, 40(5), e13103.
- [54] Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S., & Rizwan, M. (2023). Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Systems*, 40(5), e13103.
- [55] Nagarjun, A. V., & Rajkumar, S. (2025). Quantum deep learning-enhanced ethereum blockchain for cloud security: intrusion detection, fraud prevention, and secure data migration. *Scientific Reports*, 15(1), 38711.
- [56] Naz, A., Ullah, I., Uzair, M., Khokhar, M. F., Sabir, A., & Khan, R. U. (2026). AFL-SecNet: An adaptive federated learning framework for secure and privacy-preserving network traffic analysis. *Peer-to-Peer Networking and Applications*, 19(1), 25.
- [57] Noor, K., Imoize, A. L., Li, C. T., & Weng, C. Y. (2025). A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond. *Mathematics*, 13(7), 1088.
- [58] Padmavathi, V., & Saminathan, R. (2025). A federated edge intelligence framework with trust based access control for secure and privacy preserving IoT systems. *Scientific Reports*, 15(1), 35832.
- [59] Pei, X., Deng, X., Tian, S., Jiang, P., Zhao, Y., & Xue, K. (2024). A privacy-preserving graph neural

- network for network intrusion detection. *IEEE Transactions on Dependable and Secure Computing*, 22(1), 740-756.
- [60] Prajwalasimha, S. N., Shelke, N., Pimpalkar, A., Saini, D. K. J. B., Kumar, G. H., & Ranjima, P. (2025, June). AI-Powered Intrusion Detection and Privacy Preservation in 6G Networks. In *2025 Second International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS)* (pp. 123-128). IEEE.
- [61] Ragab, M., Ashary, E. B., Alghamdi, B. M., Aboalela, R., Alsaadi, N., Maghrabi, L. A., & Allehaibi, K. H. (2025). Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. *Scientific reports*, 15(1), 4470.
- [62] Rahman, R. (2025). Federated learning: A survey on privacy-preserving collaborative intelligence. *arXiv preprint arXiv:2504.17703*.
- [63] Rahmati, M., & Pagano, A. (2025, July). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. In *Informatics* (Vol. 12, No. 3, p. 62). MDPI.
- [64] Rampone, G., Ivaniv, T., & Rampone, S. (2025). A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in IoT environments. *Electronics*, 14(7), 1430.
- [65] Raza, M., Saeed, M. J., Riaz, M. B., & Sattar, M. A. (2024). Federated learning for privacy-preserving intrusion detection in software-defined networks. *Ieee Access*, 12, 69551-69567.
- [66] Shalabi, E., Khedr, W., Rushdy, E. and Salah, A., 2025. Privacy-Preserving Federated Learning in Network Intrusion Detection: A Systematic Literature Review. *International Journal of Computers and Informatics (Zagazig University)*, 8, pp.23-43.
- [67] Shalan, M., Hasan, M. R., Bai, Y., & Li, J. (2025). Enhancing smart home security: blockchain-enabled federated learning with knowledge distillation for intrusion detection. *Smart Cities*, 8(1), 35.
- [68] Swathi, K., Durga, P., Prasad, K. V., Chaitanya, A. K., Santhi, K., Vidyullatha, P., & Rao, S. V. A. (2025). Secure blockchain integrated deep learning framework for federated risk-adaptive and privacy-preserving IoT edge intelligence sets. *Scientific Reports*, 15(1), 41133.
- [69] Tabassum, A., Erbad, A., Mohamed, A., & Guizani, M. (2021). Privacy-preserving distributed IDS using incremental learning for IoT health systems. *IEEE Access*, 9, 14271-14283.
- [70] Tahir, H. A., Alayed, W., & Hassan, W. U. (2025). Privacy-preserving federated learning with adaptive model aggregation for efficient vehicle-to-vehicle (V2V) communication in intelligent transportation systems. *IEEE Access*.
- [71] Vyas, A., Lin, P. C., Hwang, R. H., & Tripathi, M. (2024). Privacy-preserving federated learning for intrusion detection in IoT environments: A survey. *IEEE access*, 12, 127018-127050.
- [72] Wakili, A., & Bakkali, S. (2025). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. *Cyber Security and Applications*, 3, 100084.
- [73] Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. *Applied Sciences*, 14(10), 4109.
- [74] Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H. C. (2025). A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud-edge-end collaboration. *Electronics*, 14(13), 2512.
- [75] Zhang, C., & Li, S. (2024). State-of-the-art approaches to enhancing privacy preservation of machine learning datasets: A survey. *arXiv preprint arXiv:2404.16847*.
- [76] Zheng, Y., Chang, C. H., Huang, S. H., Chen, P. Y., & Picek, S. (2024). An overview of trustworthy AI: advances in IP protection, privacy-preserving federated learning, security verification, and GAI safety alignment. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 14(4), 582-607.