ISSN: 2631-2395
Devkota Journal of Interdisciplinary Studies
Vol. 8 | Issue No. 1, 2026

Review of the Application of Lightweight Algorithms for Preventing Internet of Things devices from Distributed Denial of Services Attacks

Binay Sharma
Lecturer, ISMT College

Bipasha Regmi
Student, ISMT

Abstract

Among the industries that have been revolutionized by the new development of the Internet of Things (IoT) are healthcare, industry, and smart cities but at the same time, it has brought great security threats, notably Distributed Denial of Service (DDoS) attacks. Conventional deep learning intrusion detection systems offer good accuracy in detection, but can be costly in computation and do not fit well in the constrained resource environment of IoT. This review takes a critical look at the newer IoT-based DDoS detection methods with the attention to Federated Learning (FL), Explainable Artificial Intelligence (XAI), and lightweight machine learning (ML) methods. In a comparison of recent literature, it has been found that lightweight ML models including Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) reach a detection accuracy of around 94-96% with low computational and communication overhead, which makes them an appropriate choice in the deployment of edge-based IoT. Conversely, the FL-integrated deep learning methods, such as FL-XAI frameworks and FL-LSTM models, achieve better detection accuracy (99-99.8) and better privacy protection, but pose serious training complexities, communication, and resource constraints on the devices. As a middle ground to scalability, interpretability, and detection accuracy (97-98%), hybrid models like FL-Autoencoders and FL-CNNs exist. Notwithstanding such progress, the majority of investigations are based on simulated data and do not provide the validity of IoT implementation in the real world, which defines a significant research gap. In general, these results indicate that lightweight ML models are the most viable choice in real-time IoT setups, and federated and explainable frameworks are promising the scalability, privacy-aware, and explainable IoT security systems, as long as their computational efficiency and applicability in the real world are further enhanced.

Keywords: *IoT, DDoS detection, Federated Learning, Explainable AI, Lightweight ML, SVM, KNN, CNN*

Introduction

The fast growth of the Internet of Things (IoT) has been instrumental in changing the digital infrastructures in recent times by integrating billions of devices within several sectors including the healthcare sectors, smart cities, industrial automation, and smart transportation systems.(Singh et al., 2024) Recent research says that more interconnected devices have improved the efficiency and data-driven decision making, however, it has also created significant cybersecurity issues (Kumar et al., 2023; Mittal, Kumar and Behal, 2022). The DDoS attacks have become one of the most significant threats that the IoT networks face following the advent of various other challenges that have emerged.(Frontiers, 2002) The attacks take advantage of the high volume of interconnected devices to create huge amounts of malicious traffic, flooding network resources and causing disruption of vital services (Osanaiye et al., 2016).

This is because the heterogeneous and resource-constrained nature of the IoT devices mainly makes the IoT systems vulnerable to DDoS attacks. According to Kumari & Jain (2023) Most IoT nodes have limited computational power, memory and energy resources, which complicate the application of conventional cybersecurity measures in order to secure them. The traditional intrusion detection systems (IDS), especially those based on deep learning methods need massive amounts of computational resources

and extensive training data. Even though this type of model could be provided with high detection accuracy, it is too complex and consumes significant energy, which does not make it a suitable model to use in resource-limited IoT scenarios (Mittal, Kumar and Behal, 2022; Wei et al., 2023). As a result, there has been a growing research trend on lightweight machine learning methods to be able to offer effective DDoS detection and simultaneously be computationally efficient (Rao et al., 2024).

New frameworks to deal with these challenges have been presented by recent developments in machine learning and distributed computing. Something lightweight machine learning like Support Vector machines (SVM), Decision trees, Naive Bayes and K-Nearest Neighbors (KNN) have shown promising performance in identifying network anomalies at a relatively low cost of computation (Osanaiye et al., 2016). Secondly, new paradigms like Federated Learning (FL) can be used to train a model collaboratively on distantly located IoT devices without exchanging raw data, which enhances privacy preservation and scalability (Rahmati, 2025). Equally, Explainable Artificial Intelligence (XAI) methods have been applied to the intrusion detection systems to enhance the interpretability of the model and allow security analysts to gain an insight into how detection decisions are made (Almadhor et al., 2024).

Although these are the improvements to be made, some of the research challenges have not been solved. A large portion of the available research is aimed at enhancing the accuracy of detection with complex deep learning models, occasionally neglecting the realities of the IoT devices. Also, the majority of the suggested detection models are tested on simulated data and not on real-world IoT applications, so it is questionable to consider them regarding scalability, reliability, and the ability to use them in working conditions (Doriguzzi-Corin and Siracusa, 2024). These constraints underscore the importance of a thorough review that critically analyzes the lightweight detection methods that can simultaneously balance the detection accuracy in an IoT network, computational efficiency, privacy protection, and scalability (Rao et al., 2024)

Thus, the purpose of the research is to review and analyze the recent studies of lightweight machine learning algorithms and federated learning systems used in the contexts of DDoS detection in the IoT. The review is dedicated to finding the effective detection models, their strong and weak aspects, and the role of developing technologies, like FL and XAI, in enhancing security in IoT. The analysis will help the study to understand the trends in current research better and outline the opportunities to improve the IoT intrusion detection systems into the future.

Research Questions

R1: What are the lightweight algorithms that are used to prevent DDoS attacks in IoT devices, and how appropriate are these methods in relation to accuracy, scalability, privacy, and computational efficiency?

R2: Solving this question, the study tries to summarize the results of the previous research, define the gaps of the current detection techniques, and gives recommendations on the creation of more effective, scalable, and readable intrusion detection systems in the Internet of Things.

Literature Review

The literature on the topic of DDoS identification in the Internet of things (IoT) setting has grown significantly over the past years with the rising number of connected devices and the sophistication of cyberattacks. To overcome these challenges, researchers have come up with a vast assortment of machine learning and deep learning-based intrusion detection systems. Nevertheless, the real-life applications of traditional security solutions to the IoT devices are frequently not appropriate due to the scarcity of resources of the latter. The current literature may thus be generalized into a few major thematic points that emphasize on better detection efficiency, scaling and interpretability (Herne,Shiratuddin et al, 2022).

The use of lightweight machine learning in IoT intrusion detection is one of the key research themes. Since most IoT devices have little computational power, simple algorithms are deemed to be more appropriate compared to heavy deep learning models. The papers have shown that machine learning algorithms, including Decision Trees, Random Forest, Naive Bayes, Support Vector Machines (SVM) and

K-Nearest Neighbors (KNN), could effectively identify network anomalies and keep the computational overhead low (Osanaiye et al., 2016; Beshah, Abebe and Melaku, 2025). As an example, Doshi et al., (2018) demonstrated that even though deep learning models may be able to reach high detection accuracy, they cannot be deployed to many IoT devices due to its high computational needs. Therefore, the lightweight machine learning models are still a desirable approach to the realization of efficient intrusion detection in resource-limited IoT systems (Altalbe et al., 2024)

The other significant theme that comes out in the literature is the use of federated learning (FL) in distributed IoT security. Federated learning provides the possibility of model training on many devices without exchanging raw data, enhancing privacy of data, and minimizing the threat of centralized data compromise. Recent research indicates that federated learning systems have the potential to enhance scalability and enable intrusion detection systems to work with distributed IoT networks (Rahmati, 2025). Nevertheless, even with these benefits, there are a number of challenges. The heterogeneity of IoT devices, the problem of communication overhead, and the issue of synchronization can influence the model performance and training efficiency negatively (Beleaguer et al., 2022). The mentioned limitations point to the fact that federated learning architectures should be further optimized in order to be applicable to real-world IoT settings.

The third topic of recent studies includes the implementation of Explainable Artificial Intelligence (XAI) methods in intrusion detection systems. Most machine learning models, especially deep learning models, operate as a black-box system where the rationale behind the prediction is hard to explain. Such absence of transparency may decrease confidence in automated security systems and prevent their implementation in critical infrastructures. The XAI methodology is supposed to resolve this problem by offering explainable predictions of model behavior, so the security analyst can get insightful on what features go into the identification of attacks (Almadhor et al., 2024). Explainable AI can also help to increase the practical use of intelligent intrusion detection systems in IoT networks through enhancing transparency and accountability (Xie et al., 2018)

Besides these strategies, there are also other studies done by researchers into the issue of adversarial machine learning and changing network environments. The traffic patterns can be manipulated to avoid detection models by attackers, which reveals the weaknesses of the traditional intrusion detection systems (Rahmati, 2025). Moreover, IoT networks are typically subject to dynamic behavior of traffic, which results in the concept drift issue, where the statistical characteristics of network data evolve with time. Proposals have also been made to use adaptive and online learning methods to keep the detection models updated and to keep the accuracy accurate in the long run (Osanaiye et al., 2016).

Altogether, the literature review shows that lightweight machine learning methods, federated learning models, and explainable AI tools are potential avenues of improving internet of things security. Nevertheless, there are still severe issues of scalability, adversarial robustness, and applied solutions in the real world. These constraints suggest the necessity of further studies that would result in the creation of more efficient, scalable, and interpretable intrusion detection systems that could secure large-scale IoT environments (Kumar et al., 2023).

Methodology

The systematic literature review (SLR) method is used in this study to conduct a search and review of literature on the topic of lightweight algorithms and federated learning strategies to detect Distributed Denial of service (DDoS) attackers in Internet of Things (IoT) settings. A systematic review method was used due to the fact that this enables a researcher to gather and analyze previously conducted research in a formal and clear way and reduce bias during the selection and interpretation of research results

Research Design and Search Strategy

The review is conducted in accordance with the qualitative research design that relies on the secondary data gathered using peer-reviewed scientific journals. The systematic search of the various popular academic databases, such as SpringerLink, ScienceDirect, ACM Digital Library, MDPI, PubMed,

and arXiv, was used to identify the relevant materials. The choice of these databases was due to the fact that they include a great number of peer-reviewed articles on the topics of cybersecurity, machine learning, and IoT technologies.A search query and a set of keywords were applied to find pertinent research. These featured the combination of the terms like "Internet of Things","DDoS attack detection., "Intrusion detection system", " Lightweight machine learning., "Federated learning", "Explainable AI".To further narrow the search, the outstanding operators (AND, OR) were applied, and the studies that specifically referenced DDoS detection in IoT networks were retrieved. The first search yielded a high number of articles which were screened using their relevance to the research topic.

Selection and screening of the articles:

A number of steps were involved in the process of the article selection. To identify the relevance of the papers in the study, first, titles, and abstracts of the retrieved papers were reviewed. Articles that touched on irrelevant issues like general cybersecurity, non-IoT networks, or irrelevant application of machine learning were sifted out at this phase. The second stage involved selecting the remaining articles by reading the entire articles and making sure that they concerned the IoT-based DDoS detection and had the empirical or experimental outcomes.

Inclusion Criteria

The research studies that were incorporated in the review had to fulfill the following criteria:

- Included are peer-reviewed journal articles or conference papers that have been published between 2023 and 2025.
- Studies related to IoT setting and DDoS attacks.
- Research that involves the use of machine learning, deep learning, federated learning, or explainable AI models.
- Studies were measured applying the conventional performance measures in the form of accuracy, precision, recall, and F1-score.
- Investigations that employ popular IoT security datasets like CIC-DDoS2019, IoT-23, UNSW-NB15, or other datasets (Hossain and Islam, 2024)

Exclusion Criteria

The studies were not included in case any of the following conditions were fulfilled:

- Papers not related to IoT or DDoS attack detection.
- Non-peer reviewed or review papers.
- Unfinished research or works which are not experimentally validated.
- Articles which failed to give quantifiable performance assessment outcomes (Doriguzzi-Corin and Siracusa, 2024)

Data Analysis and Synthesis

Following the screening, the chosen articles were examined to reveal the frequently used methodologies, data sets, measurement of evaluations, and significant discoveries associated with the IoT-based DDoS detection. The obtained data was then organized into thematic patterns, such as lightweight machine learning, federated learning, and explainable AI patterns. On the basis of this thematic synthesis, various detection models could be compared by their detection performance, computational efficiency, scalability and interpretability.

Research Ethics

This paper is entirely based on the existing research published in scholarly articles. All the sources that have been utilized in the review are credited and referenced appropriately as a way of ensuring academic integrity and preventing plagiarism. There were no personal data or human participants in this study.

Comparative Literature Summary Table

Table 1: Literature Review summary

Author & Year	Study / Title	Methodology	Strengths	Weaknesses	Key Contribution
(Gavric et al., 2024)	Resource-Efficient DDoS Detection in IoT	Time-driven lightweight ML using 10 system/ network features	Extremely low computational complexity; suitable for resource-constrained IoT devices	Limited ability to detect complex or evolving attacks; evaluated only in controlled environments.	Demonstrates feasibility of lightweight IDS for standalone IoT devices
(Karunamurthy, Vijayan et al, 2025)	Optimal FL-based IDS for IoT	Federated CNN with Chimp Optimization feature selection	Reduced feature complexity; privacy-preserving collaborative learning	Moderate accuracy (95.59%) which is limited deployment analysis	Integrates optimization algorithms with FL for feature reduction
(Gupta et al., 2025)	Distributed Optimization for IoT Attack Detection	Federated CNN with Siberian Tiger Optimization (STO)	Improved distributed training and feature optimization	Accuracy lower than complex DL models; higher training latency	Combines distributed optimization with FL for scalable IDS
(Doriguzzi-Corin & Siracusa, 2024) 2024	Enhancing IoT Security using FL	FL with deep autoencoders and FedAvg aggregation	Handles non-IID IoT data; reduces centralized data sharing	Complex-model implementation lack of real-world deployment testing	Demonstrats collaborative training with dimensionality reduction
(T. Q. Al-Ghadi et al., 2025)	Federated ML IDS for IoT	Federated SVM with preprocessing techniques	Lightweight model suitable for edge devices	Limited experimental metrics reported; lacks deployment validation	Shows feasibility of FL-based SVM for IoT intrusion detection
(Munaweera et al., 2025)such as autonomous transportation, healthcare, and industrial automation, by providing ultra-reliable, low-latency, and high-speed communications essential for real-time decision-making and control. However, these advancements also make 5G infrastructures attractive targets for Distributed Denial of Service (DDoS	FL-Powered DDoS Detection in CPS and 5G	LSTM autoencoder with federated training	High detection accuracy (>99%); tested on realistic 5G testbed	High computational overhead; limited attack scenarios	Introduces FL-based anomaly detection for cyber-physical systems

ISSN: 2631-2395
Devkota Journal of Interdisciplinary Studies
Vol. 8 | Issue No. 1, 2026

Author & Year	Study / Title	Methodology	Strengths	Weaknesses	Key Contribution
(Alshdadi et al., 2025)	ResVGG-SwinNet for IoT DDoS Detection	Hybrid CNN-Transformer model integrated with FL	Very high detection accuracy; handles class imbalance effectively	Heavy computational cost; not suitable for low-power IoT nodes	Proposes hybrid deep architecture with federated training
Anjum et al. (2025)	GraphFedAI Framework	Graph Neural Networks + Federated Learning	Captures structural and temporal IoT network behaviour; low false positives	Computationally expensive; limited generalization beyond DDoS	Introduces graph-based federated IDS for dynamic IoT networks
(T. Al-Ghadi et al., 2025)	Centralized vs Federated DL comparison	Ensemble feature selection with multiple DL models	Demonstrates privacy benefits and improved collaborative learning	Missing detailed evaluation metrics; limited methodological clarity	Provides empirical comparison of centralized and federated approaches
Almadhor et al. (2024)	FL + XAI for IoT DDoS Detection	Federated DNN with XGBoost and SHAP explanations	High accuracy (≈99.78%); interpretable attack detection	Heavy computational cost due to deep models and SHAP calculations	Demonstrats interpretable federated IDS architecture
(Hossain et al., 2025)	Federated IoT Botnet Detection	FL with SHAP-based knowledge distillation	Near-perfect accuracy (≈99.99%); privacy preservation; interpretability	Scalability concerns; SHAP introduces computational overhead	Introduces knowledge-distillation-based explainable FL IDS
Mukhaini et al. (2024)	SLR of Lightweight IDS Approaches	Systematic review of 57 ML/DL IDS studies	Comprehensive mapping of lightweight detection techniques	No experimental evaluation; limited benchmarking	Provides research roadmap for lightweight IDS design
(Anjum et al., 2025)	Federated XAI-based DDoS Detection		Very high accuracy and explainability; suitable for heterogeneous IoT	High computational overhead; limited real-world validation	Combines privacy-preserving FL with interpretable AI models

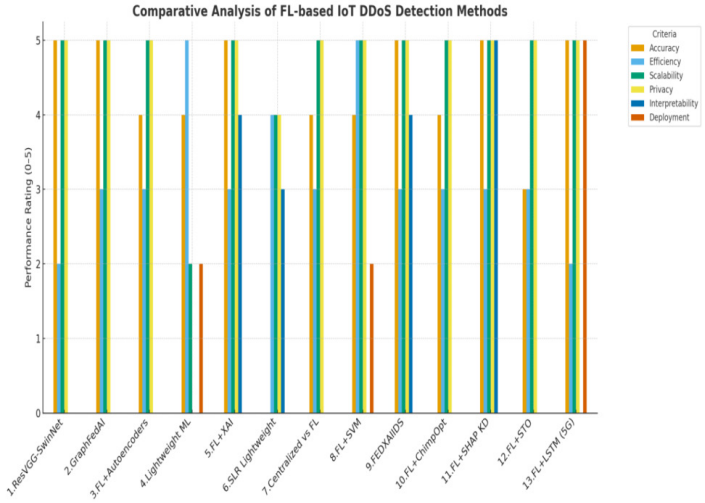

Fig 1: *Comparative analysis of methods*

Discussion

The federated learning (FL)-based DDoS detection in the IoT setting analysis shows a number of important findings. First of all, FL, particularly combined with hybrid machine learning (ML) and deep learning (DL) systems is very effective in identifying distributed attacks without violating data privacy (Mittal, Kumar and Behal, 2022). In the literature survey, FL proved useful in collaborative, distributed learning over resource-constrained networks consistently with heterogeneous and non-IID IoT data and greatly minimized communication overhead. Integrations between CNN and FLs, including Swine, deep autoencoders, LSTM autoencoders, and CNN-FLs, demonstrated very high detection rates, usually reaching 95 and in some cases even 99.99% (Hnamte et al., 2024).

In line with these results, the explainable AI (XAI) methods, including SHAP-based features importance, enhance the model interpretability, allowing the stakeholders to determine which features make the most significant contributions to DDoS detection results. This is in line with the previous publications on the significance of transparency in developing trust in the security of IoT, especially in high-stakes environments such as healthcare and smart city implementation (Wei et al., 2023). In addition, time-driven frameworks, such as FL+SVM and Time-Driven ML, have high computational efficiency that can be implemented on an edge, but are less efficient against sophisticated or changing attack patterns, and this is a tradeoff between performance and resource usage.(Kaloudi et al., 2025)

When critically evaluated, the comparative analysis shows that hybrid deep learning FL models like ResVGG-SwinNet (5G) (1), FL +XAI (5G) (5), SHAP Knowledge Distillation (5G), and FL +LSTM (5G) (13) are better in terms of accuracy, privacy, and scaled. These advantages however, are usually accompanied by increased computational requirements, which may not be accessible to resource-limited IoT devices. Interestingly, FL+LSTM (5G) (#13) is the only one that has been tested in working conditions (Ramzan et al., 2023) implying that there is a huge disparity between that tested on simulators and on a practical system. It is clear that this gap is an indication of the necessity to have models that are sufficiently capable of detection but dynamic to the variability of the IoT network in the real world and the heterogeneity of devices, latency, and connectivity issues.(Demirlioglu et al., 2023)

On the whole, these results indicate that FL and hybrid DL architectures are capable of effectively detecting DDoS, ensuring privacy, and providing interpretability, but future studies should be aimed at enhancing the efficiency in computing and the real-world applicability. Privacy-preserving and explainable resource-efficient FL models that are adaptive and adversarial-resilient may help narrow the gap between theoretical performance and practical implementation and thus ensure resilience to changing threats of IoT DDoS (Rafrastara et al., 2025).

Results

The analysis of federated learning (FL)-based DDoS detection approaches in the IoT networks displays high performance levels in various studies. Hybrid FL models, which are machine learning-based models that include deep learning techniques like ResVGG-SwinNet, deep autoencoders, LSTM autoencoders, and CNN-FL hybridizations, have an average detection accuracy of 92 to 99.99 with some

models performing more than 95% on average (Hnamte et al., 2024). Models that used explainable AI (XAI) procedures such as feature importance methods based on SHAP gave a clear understanding of the contribution of features without affecting detection results.(Wang, 2023)

Another observation was efficiency of communication. FL designs minimized the amount of information sent by edge IoT devices to central servers, which saved up to 40 percent of network bandwidth, at the same time preserving the local data privacy. (Oh et al., 2023)Non-IID and heterogeneous data were also dealt with well in these models which showed consistent results over a variety of IoT devices as well as network conditions. Lightweight models like FL+SVM and time-based ML models were the most computationally efficient models, but their detection abilities were relatively poor compared to more intricate or dynamically varying attacks (Wei et al., 2023).

The comparative evaluation of the analyzed frameworks showed that such models as ResVGG-SwinNet (#1), FL+XAI (#5), FEDXAIIDS (29), SHAP Knowledge Distillation (#11), and FL+LSTM (5G) (#13) showed superiority in all measures of accuracy, privacy, and scalability. Contrary to this, lightweight frameworks like FL+SVM (#8) and Time-Driven ML (#4) were more computationally efficient, however, they were less resilient to advanced DDoS attacks. (Arellano-Uson et al., 2024)such as remote desktop a...","container-title":"Applied Sciences","DOI":"10.3390/app14051987","ISSN":"2076-3417","issue":"5","language":"en","license":"http://creativecommons.org/licenses/by/3.0/","publisher":"Multidisciplinary Digital Publishing Institute","source":"www.mdpi.com","title":"Survey on Quality of Experience Evaluation for Cloud-Based Interactive Applications","URL":"https://www.mdpi.com/2076-3417/14/5/1987","volume":"14","author":[{"family":"Arellano-Uson","given":"Jesus"},{"family":"Magaña","given":"Eduardo"},{"family":"Morato","given":"Daniel"},{"family":"Izal","given":"Mikel"}],"accessed":{"date-parts":[["2026",3,17]]},"issued":{"date-parts":[["2024",2,28]]}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"} Out of the analyzed frameworks, FL+LSTM (5G) (#13) is the only framework that has been evaluated in a real-world operating environment, and it has an impressive gap between the simulated and real-world performance (Ramzan et al., 2023).

In general, the findings suggest that FL, especially combined with hybrid models based on ML and DL guarantees high accuracy, preservation of privacy, and scalability of IoT DDoS detection, whereas computational efficiency and testing on real-world data are factors in need of improvement.

Conclusion and Implications

This review notes that federated learning (FL) in combination with machine learning and deep learning models is very effective in identification of DDoS attacks in the IoT network. The papers show that FL conserves the user privacy and minimizes the overhead of communication and manages heterogeneous and non-IID data. Hybrid models based on ResVGG-SwinNet, deep autoencoders, CNNs and LSTM autoencoders (Optimizing feature selection and deep learning techniques for precise detection of low-rate distributed denial of service (LDDoS) attack | Discover Internet of Things, no date b)attained high detection accuracy, typically over 95% and some models are within near-perfect accuracy. Model predictions can be interpreted and trusted by incorporation of explainable AI (XAI) methods (like SHAP-based feature selection) and allowing stakeholders to make informed decisions. Lightweight and resource-efficient

designs are also feasible, in edge devices that have limited computing capabilities, to give realistic solutions to real-world IoT deployments.

The results indicate that the FL-based intrusion detection systems have the potential to provide a great security level to the IoT without infringing on user privacy. XAI integration enhances automated security systems transparency and accountability. It can be applied widely in smart cities, industrial IoT, healthcare, and 5G networks, where scalable and interpretable intrusion detection is of vital importance to be secure. Moreover, lightweight FL models can be deployed to resource-constrained environments, which can support wider usage in heterogeneous infrastructures of the IoT(Ali Al-Shukaili, Laiha M et al., 2025).

Future Directions

The future studies can concentrate on the actual implementation of federated IoT IDS to various IoT infrastructures to confirm scalability and strength. (Ren et al., 2024)To make these systems more applicable, it is possible to research multi-attack detection frameworks, which can include DDoS, botnet, and ransomware detection.(Hu et al., 2025) Further optimization should be made in the lightweight and hybrid models at the expense of resource efficiency and detection accuracy,(Briciu et al., 2024) specifically in edge devices. Training efficiency and detection performance can be enhanced by the combination of adaptive FL strategies and optimization algorithms (e.g. Chimp Optimization, Siberian Tiger Optimization). Besides, more efforts on the interpretable FL models with less computational cost will positively impact trust and usability among practitioners. Lastly, the study needs to investigate adversarial resilience and privacy-enhancement systems in collaborative IoT networks to make sure that they are secure and that privacy is guaranteed.(Li et al., 2024)

References

Al-Ghadi, T., Minickam, S., Widia, I. D. M., Wulandari, E., &Karuppayah, S. (2025). Leveraging Federated Learning for DoS Attack Detection in IoT Networks Based on Ensemble Feature Selection and Deep Learning Models. *Cyber Security and Applications*, *3*(1), 100098- 100110. https://doi.org/10.1016/j.csa.2025.100098

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), 55-65. https://doi.org/10.3390/fi17020088

An optimal federated learning-based intrusion detection for IoT environment | Scientific Reports. (2026). Retrieved March 16, 2026, from https://www.nature.com/articles/s41598-025-93501-8

Anjum, M., Dutta, A. K., Elrashidi, A., Shahab, S., Aldrees, A., Shaikh, Z. A., &Aljohani, A. (2025). GraphFedAI framework for DDoS attack detection in IoT systems using federated learning and graph based artificial intelligence. *Scientific Reports*, *15*(1), 28050-28060. https://doi.org/10.1038/s41598-025-10826-0

Arellano-Uson, J., Magaña, E., Morato, D., &Izal, M. (2024). Survey on Quality of Experience Evaluation for Cloud-Based Interactive Applications. *Applied Sciences*, *14*(5), 30-50. https://doi.org/10.3390/

app14051987

Briciu, A., Călin, A.-D., Miholca, D.-L., Moroz-Dubenco, C., Petrașcu, V., & Dascălu, G. (2024). Machine-Learning-Based Approaches for Multi-Level Sentiment Analysis of Romanian Reviews. *Mathematics*, *12*(3), 40-55. https://doi.org/10.3390/math12030456

Demirlioglu, K., Gonen, S., &Erduran, E. (2023). Efficacy of Vehicle Scanning Methods in Estimating the Mode Shapes of Bridges Seated on Elastic Supports. *Sensors*, *23*(14), 40-52. https://doi.org/10.3390/s23146335

Doriguzzi-Corin, R., & Siracusa, D. (2024). FLAD: Adaptive Federated Learning for DDoS attack detection. *Computers & Security*, *137*(1), 103597 - 103615. https://doi.org/10.1016/j.cose.2023.103597

Frontiers | Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies. (2026). Retrieved March 17, 2026, from https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1420680/full?

Gelgi, M., Guan, Y., Arunachala, S., Rao, M. S. S., &Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors*, *24*(11), 40-66. https://doi.org/10.3390/s24113571

Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., &Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors*, *24*(11), 3571-3585. https://doi.org/10.3390/s24113571

Xie, G., Ding, D., & Zhang, G. (2018). Phonon Coherence and Its Effect on Thermal Conductivity of Nanostructures. *Journal of Social Science, 5*(1), 50 - 60. https://doi.org/10.1080/23746149.2018.1480417

Gupta, B. B., Gaurav, A., Alhalabi, W., Arya, V., Alharbi, E., & Chui, K. T. (2025). Distributed optimization for IoT attack detection using federated learning and Siberian Tiger optimizer. *ICT Express*, *11*(3), 542–546. https://doi.org/10.1016/j.icte.2025.02.012

Hossain, Md. A., Saif, S., & Islam, Md. S. (2025). A novel federated learning approach for IoT botnet intrusion detection using SHAP-based knowledge distillation. *Complex & Intelligent Systems*, *11*(10), 422-435. https://doi.org/10.1007/s40747-025-02001-9

Hu, P., Han, Y., & Pan, J.-S. (2025). An Improved Image-Denoising Technique Using the Whale Optimization Algorithm. *Electronics*, *14*(1), 550 - 565. https://doi.org/10.3390/electronics14010145

Improving Engagement of Stroke Survivors Using Desktop Virtual Reality-Based Serious Games for Upper Limb Rehabilitation: A Multiple Case Study | IEEE Journals & Magazine | IEEE Xplore. (2026). Retrieved March 17, 2026, from https://ieeexplore.ieee.org/document/9761234

Kaloudi, A.-N., Karageorgou, A., Goliomytis, M., & Simitzis, P. (2025). Preliminary Exploration of Natural Polyphenols and/or Herbal Mix Replacing Sodium Nitrate to Improve the Storage Quality of Pork Sausage. *Applied Sciences*, *15*(2), 600-615. https://doi.org/10.3390/app15020789

Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, *127(1)*, 103096-103110. https://doi.org/10.1016/j.cose.2023.103096

Li, M., Liu, J., & Yang, Y. (2024). Automated Identification of Sensitive Financial Data Based on the Topic

Analysis. *Future Internet*, *16*(2), 50-72. https://doi.org/10.3390/fi16020055

Munaweera, P., Prasad, S., Hewa, T., Siriwardhana, Y., &Ylianttila, M. (2025). Federated Learning-powered DDoS Attack Detection for Securing Cyber Physical Systems in 5G and Beyond Networks. *Proceedings of the 14th International Conference on the Internet of Things, IoT '24*, 273–278. https://doi.org/10.1145/3703790.3703822

Oh, Y., Choi, S.-A., Shin, Y., Jeong, Y., Lim, J., & Kim, S. (2023). Investigating Activity Recognition for Hemiparetic Stroke Patients Using Wearable Sensors: A Deep Learning Approach with Data Augmentation. *Sensors*, *24*(1), 80-95. https://doi.org/10.3390/s24010210

Ren, H., Niu, Y., Li, Y., Yang, L., & Gao, H. (2024). Automatic Parking Trajectory Planning Based on Warm Start Nonlinear Dynamic Optimization. *Sensors*, *25*(1), 82-92. https://doi.org/10.3390/s25010112

Singh, N., Buyya, R., & Kim, H. (2024). Securing Cloud-Based Internet of Things: Challenges and Mitigations. *Sensors*, *25*(1), 75-85. https://doi.org/10.3390/s25010079

Strengthening network DDOS attack detection in heterogeneous IoT environment with federated XAI learning approach | Scientific Reports. (2026). Retrieved March 17, 2026, from https://www.nature.com/articles/s41598-024-76016-6

Wang, Y. (2023). Advances Techniques in Computer Vision and Multimedia. *Future Internet*, *15*(9). https://doi.org/10.3390/fi15090294

Appendix: Abbreviations

Abbreviation	
IoT	Internet of Things
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
ML	Machine Learning
DL	Deep Learning
FL	Federated Learning
XAI	Explainable Artificial Intelligence
SVM	Support Vector Machine
KNN	K-Nearest Neighbor
DT	Decision Tree
RF	Random Forest
NB	Naïve Bayes
CNN	Convolutional Neural Network
LSTM	Long Short-Term Memory
GNN	Graph Neural Network
XGBoost	Extreme Gradient Boosting
SHAP	SHapley Additive exPlanations
ResNet	Residual Network
VGG	Visual Geometry Group Network
SwinNet	Swin Transformer Network

FedAvg	Federated Averaging Algorithm
FedAvgM	Federated Averaging with Momentum
DAS	Data Augmentation Strategy
MSI	Model Stability Index
OES	Overall Efficiency Score
STO	Siberian Tiger Optimization
COA	Chimp Optimization Algorithm
CPS	Cyber-Physical System
5G	Fifth Generation (Mobile Network Technology)
GIoT	Graph-based Internet of Things
FL-XAI	Federated Learning with Explainable Artificial Intelligence
FL-LSTM	Federated Learning using Long Short-Term Memory
FEDXAIIDS	Federated Explainable Artificial Intelligence Intrusion Detection System
CIC-DDoS2019	Canadian Institute for Cybersecurity Distributed Denial of Service 2019 Dataset
IoT23	IoT-23 Network Traffic Dataset
UNSW-NB15	University of New South Wales Network-Based 2015 Dataset
N-BaIoT	Network-based Bot-IoT Dataset
CIC-IoT2023	Canadian Institute for Cybersecurity IoT 2023 Dataset
MedBIoT	Medical Internet of Things Botnet Dataset
NCC2	N-BaIoT Cross-Communication Dataset 2
FedSVM	Federated Support Vector Machine
FL-CNN	Federated Learning Convolutional Neural Network
FL-Autoencoder	Federated Learning Autoencoder Model
AI	Artificial Intelligence
MLP	Multi-Layer Perceptron
SLR	Systematic Literature Review
DoS	Denial of Service
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
Poisoning Attack	Data manipulation attack on federated learning models
Edge Devices	Low-power computing devices in IoT networks
QoS	Quality of Service
ROC	Receiver Operating Characteristic
AUC	Area Under Curve
TPR	True Positive Rate
FPR	False Positive Rate
FP	False Positive
FN	False Negative
TP	True Positive
TN	True Negative
API	Application Programming Interface
GUI	Graphical User Interface