Federated Learning-Based Intrusion Detection and Energy Optimization for IoT Networks Using Whale Optimization Algorithm

Hamza Javed, Shahzad Latif, Saira Shaheen
Department of Department of Computer Science (SZABIST University Islamabad).
*Correspondence: shahzadlatif977@gmail.com

Citation | Javed. H, Latif. S, Shaheen. S, "Federated Learning-Based Intrusion Detection and Energy Optimization for IoT Networks Using Whale Optimization Algorithm", IJIST, Vol. 8 Issue. 3 pp 1088-1100, June 2026
Received | April 14, 2026 **Revised |** May 17, 2026 **Accepted |** May 24, 2026 **Published |** June 06, 2026.

The IoT devices plays an important role in today's technology. However, with rapid growth of IoT based technology, security of these devices and high power consumption are significant challenges. To mitigate these challenges, this research work proposed novel federated learning-based intrusion detection system to mitigate security issues. Moreover, to minimize energy consumption, a whale colony-based algorithm is proposed. The results are simulated and compared with other studied algorithms. The proposed algorithms outperformed the other understudied algorithms. Experimental results on the CIC-IoT-2023 dataset demonstrate that the proposed FL-WOA framework achieved 99.17% intrusion detection accuracy, outperforming existing federated learning approaches by up to 5.56%, while significantly reducing network energy consumption through optimized resource allocation.

Keywords: Internet of Things (IoT), Intrusion Detection Systems (IDS), Federated Learning (FL). Whale Optimization Algorithm (WOA).

Introduction:

The intrusion detection system (IDS) plays a vital role in network security of IoT devices [1]. Modern day IoT devices require high speed internet connectivity for real time applications [2]. The continuous connectivity of devices and data exchange between devices can be affected by adversaries [3]. The IDS based system are help to secure important information exchanging between IoT devices. In addition, long term energy efficiency is required for IoT devices because these devices are working mostly in wireless environment [4][5].

IoT-based healthcare solutions have enabled telemedicine, contact tracing, and remote diagnostics, improving efficiency in managing healthcare demand [6][7]. In agriculture, IoT advancements support precision farming through real-time monitoring and automated systems, enhancing yields and resource use [8]. IoT drives sustainable agriculture and IIoT transforms industries through smart manufacturing, predictive maintenance, and automated quality control, enhancing efficiency and reducing costs [9][10][11]. IoT enhances smart transportation and energy systems through real-time fleet monitoring, autonomous vehicles, smart grids, and demand response technologies, boosting efficiency and reducing costs [12][13].

Security Challenges and the Role of Intrusion Detection Systems (IDS):

The rise of IoT adoption in industries is driven by advancements in wireless technologies like 5G and Wi-Fi enhancing automation, data analysis, and remote monitoring [14][15]. IoT enhances manufacturing, smart cities, and transportation by enabling predictive maintenance, automated factories, real-time resource management, and improved urban mobility and safety [16][17][18]. The rapid IoT expansion enhances resource management and renewable integration but also raises serious cybersecurity challenges due to diverse architectures, lack of global standards, and increased attack surfaces [19][20][21]. IoT security is challenged by unmaintained firmware, diverse environments, and privacy risks, necessitating energy-efficient intrusion detection systems to protect sensitive data and critical IIoT processes [22][23][24][25]. Securing diverse, resource-limited IoT devices is hindered by lack of standard protocols, weak authentication, physical tampering risks, and outdated firmware vulnerabilities, increasing cyberattack exposure [26][27][28]. Due to device interaction in IoT networks, IDS is essential for security, but traditional centralized IDS models are often unsuitable due to high energy and communication costs [6][29][30]. Energy-efficient IDS for IoT must balance real-time detection, low latency, and low complexity, with emerging solutions like Federated Learning combined with optimization algorithms to reduce communication overhead and preserve privacy [31][32][33]. Metaheuristic optimizations like WOA and PSO enhance Federated Learning's energy efficiency in resource-constrained IoT devices by optimizing model parameters [34]. Combining FL with WOA and PSO optimizations improves IDS energy efficiency and detection accuracy by adapting to traffic variations and reducing communication costs [35].

Related Work:

Modern IDS for IoT must be energy-efficient, privacy-preserving, and leverage distributed methods like FL, while signature-based IDS effectively detects known threats but fails against unknown attacks [36][20]. Energy-efficient IDS is critical for battery-powered IoT devices, with FL and metaheuristic methods like WOA and PSO reducing power use by optimizing model parameters and minimizing communication [37]. Due to IoT's limited resources, lightweight IDS using CNN, RNN, and hybrid metaheuristic algorithms like WOA-SA or BOA-ACO optimize detection accuracy while minimizing computational overhead [38].

Designing energy-efficient IDS for IoT involves combining ML with optimization techniques like PSO-GPC and FL methods such as FedAvg, FedProx, and DAFL to balance

accuracy and energy use [39]. ML techniques enhance IDS detection in resource-constrained IoT networks, with careful selection of supervised, unsupervised, deep, and ensemble learning methods crucial for balancing accuracy and energy efficiency [40].

Decision Trees, known for their low computational cost and interpretability, are widely used in energy-aware IDS for IoT, though they require pruning and feature selection to prevent overfitting and manage memory usage [41]. Support Vector Machines (SVMs) deliver high intrusion detection accuracy for complex attacks but are resource-intensive, so energy efficiency is enhanced through support vector reduction and incremental learning; Naive Bayes, being computationally light and fast, suits real-time IDS but struggles with correlated features, requiring feature extraction for better accuracy and energy efficiency [41]. K-Means and DBSCAN are popular unsupervised clustering techniques used in IDS for anomaly detection; while K-Means is efficient for large datasets with clear cluster boundaries, DBSCAN excels in identifying arbitrarily shaped clusters and outliers, and both are optimized for energy efficiency using adaptive distance metrics and ANN search techniques [42].

Deep learning techniques like CNNs, RNNs (including LSTM), and DNNs are highly effective in IDS for extracting complex patterns and detecting intrusions, and energy-efficient variants—such as lightweight CNNs, memory-optimized LSTMs, and DNNs integrated with optimization algorithms like WOA—enable their deployment on resource-constrained IoT devices [43]. Ensemble learning techniques like boosting (AdaBoost, Gradient Boosting) and bagging (Random Forest) improve IDS detection accuracy and robustness while balancing energy consumption, though boosting may overfit noisy data and bagging requires more memory; meanwhile, Federated Learning offers a decentralized, privacy-preserving IDS solution that reduces communication overhead and single points of failure in growing IoT networks [23]. Federated Learning (FL) enhances privacy and scalability in IDS by keeping data local and only sharing model updates, reducing data leakage risks and aiding regulatory compliance, while addressing non-IID data across devices; however, to mitigate vulnerabilities like gradient inversion and model poisoning, FL is combined with techniques such as Differential Privacy and Secure Aggregation to maintain security without sacrificing accuracy [44][45].

Federated Averaging (FedAvg) enables efficient global model training by averaging local model updates from clients instead of raw data, making it communication-efficient and suitable for resource-constrained IoT devices; however, it can suffer from model divergence with non-IID data and is vulnerable to poisoning attacks, yet remains widely used in IoT intrusion detection for its lightweight and privacy-preserving nature [46][41]. FedSGD averages client gradients for model training, requiring synchronized updates that increase communication and computation costs, making it suited for large models; it enhances privacy and distributes load compared to centralized IDS [47]. Energy efficiency is crucial for IDS in resource-limited IoT devices, with optimization algorithms like Evolutionary Algorithms, Whale Optimization Algorithm (WOA), and hybrid FL-based methods helping to reduce energy use while maintaining detection accuracy [48]. Evolutionary algorithms, inspired by natural evolution processes like selection and mutation, effectively optimize energy-efficient IDS, with Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) being the most commonly used [2]. Genetic Algorithms (GA) optimize energy-efficient IDS by selecting features and fine-tuning model parameters, such as in GA-SVM hybrids, to improve detection accuracy and reduce energy use, though they can be computationally expensive and risk premature convergence [49].

Particle Swarm Optimization (PSO), inspired by bird flocking behavior, optimizes energy-efficient IDS by refining clustering and model parameters to reduce energy use while maintaining accuracy, offering fast convergence and simplicity but risking local optima in high-dimensional spaces [39]. The Whale Optimization Algorithm (WOA) mimics humpback

whales' bubble-net feeding behavior to efficiently solve complex optimization problems through encircling prey, bubble-net attacking, and global search phases, offering fast convergence and avoidance of local optima [50]. Hybrid optimization techniques combine federated learning (FL) with metaheuristic algorithms like WOA and PSO to enhance energy efficiency by optimizing model aggregation, reducing communication overhead, and addressing non-IID data challenges through dynamic weighting and update frequency adjustments [51].

Most existing IDS models rely on centralized data aggregation, which raises privacy concerns and increases communication and energy overheads. These centralized, non-adaptive approaches are also ill-suited for diverse IoT environments.

This research proposes a novel IDS framework combining Federated Learning (FL) and the Whale Optimization Algorithm (WOA) to address these issues. FL enhances data privacy and reduces communication costs by enabling decentralized model training, while WOA optimizes resource use, minimizing energy consumption without sacrificing detection performance. Together, they offer an adaptive, energy-efficient, and secure solution for modern and future IoT networks. Recent studies have demonstrated significant advancements in applying Federated Learning (FL) to intrusion detection systems (IDS) for IoT and IIoT environments.

Asiri [52] proposed an explainable FL framework that enhances the interpretability of intrusion detection decisions using causal reasoning, improving trust in distributed security systems. Liang and Luo [53] optimized FL-based distributed IDS architectures to improve detection accuracy while preserving data privacy across heterogeneous IoT networks. In addition, block chain-assisted FL models have been introduced to strengthen trust, integrity, and secure collaboration among IoT devices [54]. Du [55] integrated attention mechanisms with lightweight transformer models under FL settings to improve detection efficiency in resource-constrained industrial IoT environments.

Similarly, Nguyen et al. [56] focused on feature reduction techniques to reduce computational overhead while maintaining detection performance. Alqazzaz [57] developed privacy-preserving anomaly detection frameworks that further enhance secure data handling in FL-based systems. [58] Conducted comprehensive evaluations of FL-based IDS approaches, highlighting their strengths and limitations in real-world deployments. Furthermore, [59] and [60] emphasized decentralized datasets and blockchain-enabled FL architectures, demonstrating improved scalability, robustness, and security in IoT intrusion detection. Despite these advancements, existing approaches still largely overlook the joint optimization of detection performance and energy efficiency, particularly in resource-constrained IoT environments, motivating further research in this direction.

Research Gap:

Most IoT intrusion detection systems (IDS) use centralized architectures, which can cause privacy risks, high communication overhead, and increased energy consumption. Although Federated Learning (FL) has been introduced to enhance privacy, many FL-based IDS solutions lack efficient resource optimization. Moreover, existing optimization-based approaches mainly focus on improving detection accuracy while overlooking energy efficiency in resource-constrained IoT devices.

To address this gap, the proposed FL-WOA framework combines Federated Learning with the Whale Optimization Algorithm (WOA) to achieve both effective intrusion detection and energy-efficient operation.

Research Objectives:

To develop a privacy-preserving Intrusion Detection System (IDS) using Federated Learning (FL) to enable collaborative threat detection without sharing sensitive data.

To apply the Whale Optimization Algorithm (WOA) to minimize energy consumption

in IoT devices while maintaining system efficiency.

To enhance intrusion detection accuracy and overall security performance in resource-constrained IoT environments.

Novelty and Contributions:

Proposes a novel framework that integrates Federated Learning and the Whale Optimization Algorithm for both intrusion detection and energy optimization in IoT networks.

Introduces a decentralized, privacy-preserving learning approach that allows IoT devices to collaboratively train detection models without exposing local data.

Incorporates an energy-aware optimization strategy to extend the operational lifetime of resource-constrained IoT devices.

Achieves improved intrusion detection performance while reducing energy consumption, making the framework suitable for practical IoT deployments.

Material and Methods:

Proposed Model:

The proposed methodology integrates FL and WOA to address the challenges of intrusion detection and energy efficiency in IoT networks. FL allows multiple IoT devices to train a shared IDS model while keeping raw data localized on each device. Each device processes its local data and sends model updates to a central server, where the updates are aggregated to improve the global model. This decentralized approach reduces data transmission costs and preserves user privacy while enabling real-time adaptation to emerging security threats.

Federated Learning for Intrusion Detection:

Figure 1 illustrates the FL framework used for IoT-based intrusion detection. Each device locally trains its model on its own dataset, including potentially infected data, before sending model updates to the central aggregator. The global model continuously evolves by integrating knowledge from multiple devices, leading to a more comprehensive and adaptive IDS.

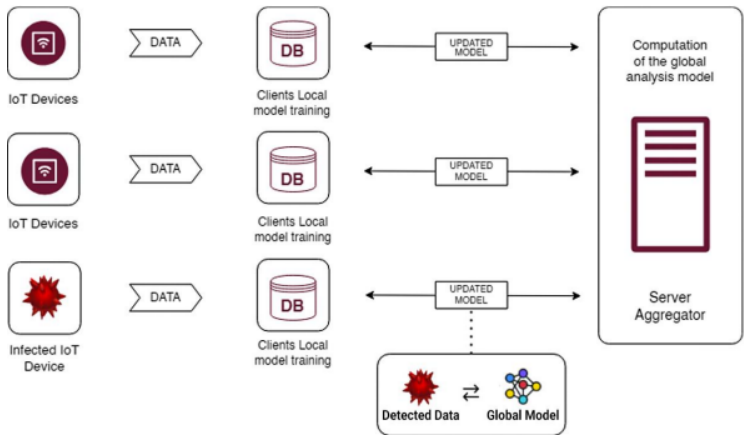

Figure 1. FL Framework for IoT Intrusion Detection

Whale Optimization Algorithm for Energy Efficiency:

To minimize the energy consumption in IoT network, whale optimization algorithm (WOA) is proposed inspired by hunting behavior of whales. The initial population is based on IoT sensor nodes wireless network. The energy evaluation is evaluated and updated using spiral motion of whale and random motion [50]. The minimization energy consumption is selected as best configured network that used the minimize the energy. Figure 2 shows that energy of IoT sensors is accumulated and optimized by whale optimization algorithm in order to optimize overall energy of the network.

$$D = |C.X_{best} - X| \qquad \text{Equation (1)}$$

In equation (1), *D* represents the distance between the whale's current position *X* and the best-known position X_{best} . The coefficient *C* is governed by random variables and adaptive parameters that regulate the balance between exploration and exploitation during the optimization process. Through iterative updates of *D*, the whales simulate the encircling behavior around prey, progressively moving closer to the optimal solution. This mechanism enables the algorithm to effectively navigate the search space and converge toward the global optimum in a stable and efficient manner.

$$E_{total} = \sum_{u=1}^{U} \left(E_{comp}^{u} + E_{trans}^{u} + E_{sampling}^{u} \right) \qquad \text{Equation (2)}$$

In equation 2, E_{total} represents the cumulative energy usage of all devices participating in the network during a complete training round or communication cycle. It provides an overall measure of how much energy the system requires to perform distributed learning tasks. The variable U denotes the total number of users or edge devices involved in the network. Each device contributes individually to the overall energy consumption depending on its local computation, communication activity, and data handling processes. In Equation (2), the total energy consumption $E^{u}comp$ represents the cumulative energy usage of all devices participating in the network during a complete training round or communication cycle. It provides an overall measure of how much energy the system requires to perform distributed learning tasks. ($E^{u}trans$) refers to the communication energy consumed when transmitting the locally trained model updates (such as gradients or weights) to the central server or neighboring nodes. This part is often influenced by network conditions, transmission distance, and data size. Moreover $(E^{u}sampling)$, denotes the energy required for data sampling and preprocessing at the device level. This may include reading sensor data, select training samples, and perform basic data cleaning operations before model training begins. Therefore, the total energy consumption can be understood as the sum of computation, communication, and data acquisition costs across all participating devices, providing a comprehensive view of energy efficiency.

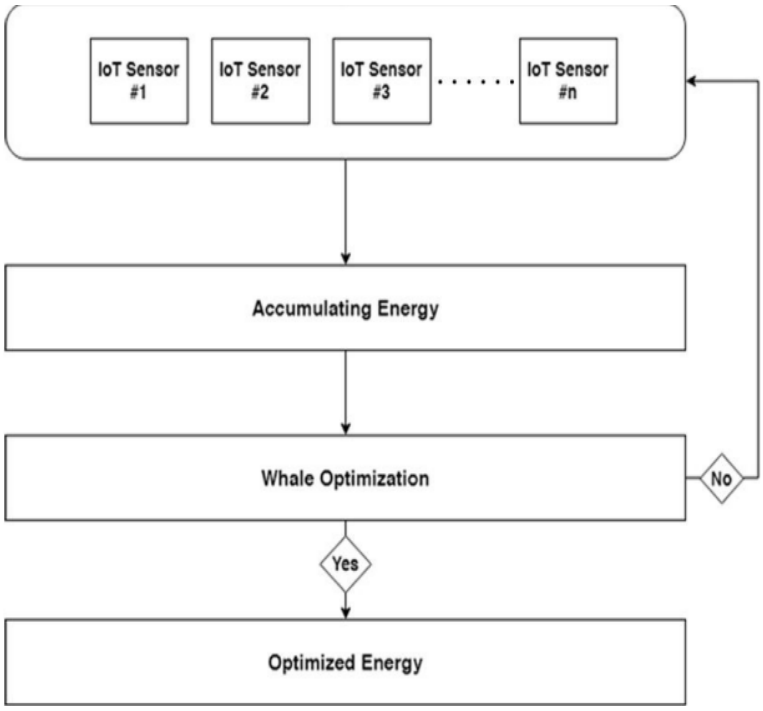

Figure 2. Architecture for Whale Optimization Algorithm

Figure 3 represents the flowchart of proposed work.

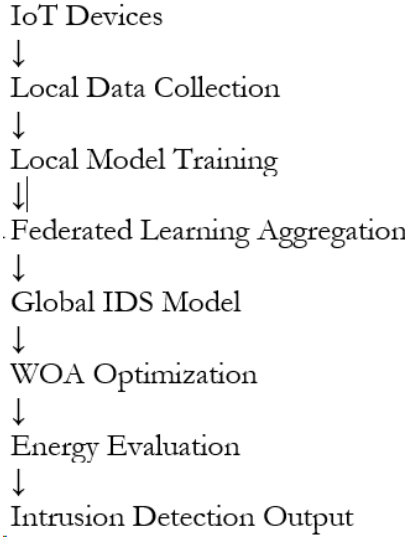

Figure 3. Flowchart of Proposed Model

Experimental Setup:

The hardware experiment specifications include NVIDIA Tesla P100 GPU, 16 GB RAM, and 35 GB of disk space, a Linux-based operating system managed by Kaggle, with Python 3.8 as the primary programming language, and experiments conducted in Jupyter Notebook [61][62]. The CIC-IoT-2023 dataset is considered which consists of traffic from 105 IoT devices and 33 attack scenarios classified into seven categories, including DDoS, DoS, Spoofing, and Mirai botnet activities [63][64][52].

Results and Discussions:

To compare the performance of the models, several machine learning models were trained and tested on the prepared dataset. The models used were XGBoost, Random Forest, KNN, and Logistic Regression. In addition, an improved federated learning model with XGBoost was developed with LDP and WOA optimization to investigate the effectiveness of privacy-preserving and optimization methods for energy efficiency [65][66].

Federated Learning Model Results:

The performance of each model was evaluated based on Accuracy, F1-Score, Precision, Recall and F1 Score. Table 1 represents these results.

Table 1. Intrusion detection accuracy Comparison

Study	Methodology	Energy Efficiency Metrics	Accuracy (%)
Proposed Model	XGBoost Algorithm + Federated Learning	Estimators*LR	99.17
Proposed Model	Simple XGBoost	Estimators*LR	99.06
[67]	Federated Learning for Intrusion Detection (Fed-IDS)	High detection rate in IoT networks	98.00
[40]	MV-FLID (Multi-View Federated Learning for IoT)	Reduced communication overhead with accuracy improvement	95.97
[39]	DAFL (Dynamic Aggregation Federated Learning)	Low communication overhead with improved intrusion detection	94.64

Energy Consumption:

Compared with other algorithms, WOA is the most energy efficient one and can achieve the maximum energy conservation as soon as possible. GA reduces the consumption in a slow manner and it was found to be more effective than PSO in terms of energy use. The graph Figure 4 showcasing energy consumption highlights that the WOA is the best performer

in terms of energy efficiency. WOA consistently shows a steeper decline in energy consumption compared to both the GA and PSO. By the 20th iteration, WOA reaches the lowest energy usage, making it the most energy-efficient algorithm in this experiment.

Interestingly, the GA outperforms PSO in energy efficiency, despite its resource-intensive operations like mutation and crossover. GA exhibits a steady decline in energy consumption, eventually surpassing PSO in reducing energy usage. On the other hand, PSO demonstrates the slowest rate of energy reduction and consumes the most energy by the end of the iterations, making it the least energy-efficient among the three algorithms.

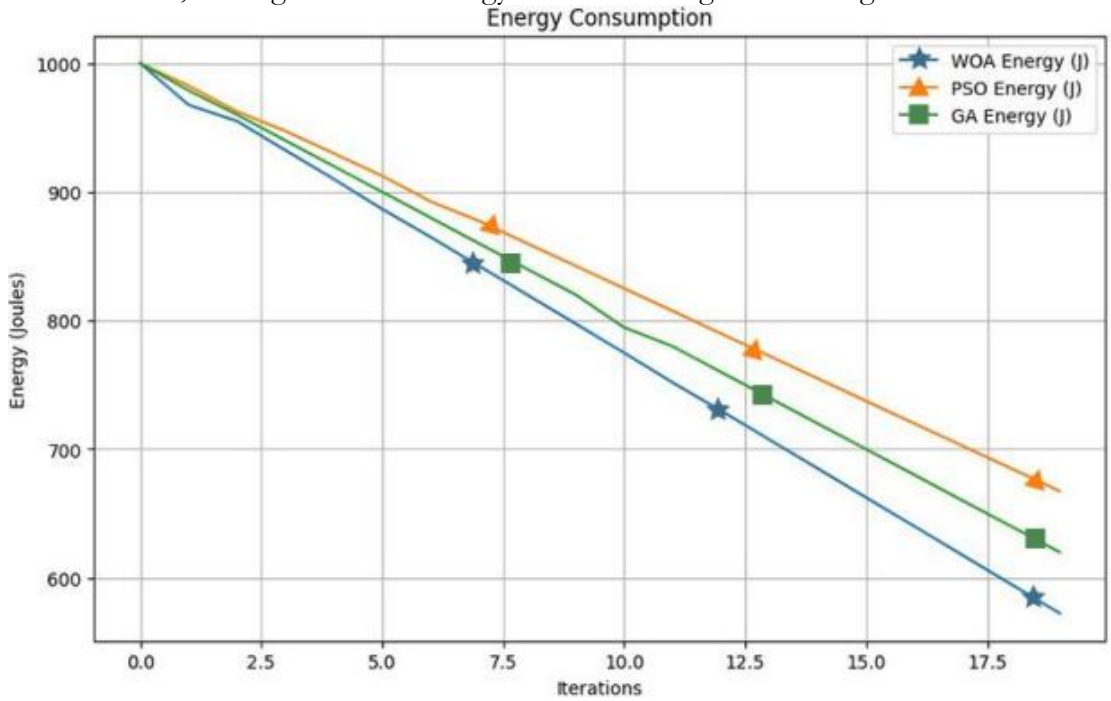

Figure 4. Comparison of energy consumption trends over 20 iterations.

Federated learning training complexity is O(K×N×M), where: K = communication rounds, N = devices, M= training samples.

WOA complexity is O(T×P×D), where:T = iterations, P = population size, D = dimensions

Conclusion:

This study presents a novel and energy-efficient Intrusion Detection System (IDS) framework that integrates Federated Learning (FL) with the Whale Optimization Algorithm (WOA), offering a powerful solution for modern IoT security challenges. By preserving data privacy through decentralized learning and optimizing energy consumption with metaheuristic tuning, the proposed system addresses both security and sustainability concerns in resource-constrained environments. The synergy of FL's scalability and data confidentiality with WOA's dynamic resource management yields a resilient and adaptive IDS. Experimental results confirm significant improvements in detection accuracy, energy efficiency, and computational performance, marking this approach as a forward-thinking benchmark for future IoT security deployments.

Future Research Directions:

Future research may focus on the real-time deployment of the proposed FL-WOA framework in large-scale IoT environments and its implementation on edge devices for low-latency intrusion detection. The integration of blockchain and differential privacy techniques can further enhance security and privacy preservation. Additionally, developing lightweight federated learning models for resource-constrained IoT devices, incorporating Explainable AI (XAI) for improved decision transparency, and exploring quantum-resistant security

mechanisms represent promising directions for future investigation.

References:

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/J.COMNET.2014.11.008.

[2] H. Ren, D. Anicic, and T. A. Runkler, "The synergy of complex event processing and tiny machine learning in industrial IoT," *DEBS 2021 - Proc. 15th ACM Int. Conf. Distrib. Event-Based Syst.*, pp. 126–135, Jun. 2021, doi: 10.1145/3465480.3466928; Topic:Conference collections>Debs;Page:String:Article/Chapter.

[3] M. Sayad Haghighi, F. Farivar, A. Jolfaei, A. B. Asl, and W. Zhou, "Cyber Attacks via Consumer Electronics: Studying the Threat of Covert Malware in Smart and Autonomous Vehicles," *IEEE Trans. Consum. Electron.*, vol. 69, no. 4, pp. 825–832, Nov. 2023, doi: 10.1109/TCE.2023.3297965.

[4] A. A. S. & J. A. Adeel Abbas, Muazzam A. Khan, Shahid Latif, Maria Ajaz, "A New Ensemble-Based Intrusion Detection System for Internet of Things," *Arab. J. Sci. Eng.*, vol. 47, pp. 1805–1819, 2022, doi: https://doi.org/10.1007/s13369-021-06086-5.

[5] Rayeesa Malik, Yashwant Singh, "[Retracted] An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems," *J. Adv. Transp.*, 2022, [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1155/2022/7892130

[6] V. S. and I. K. S. U. Jan, S. Ahmed, "Toward a Lightweight Intrusion Detection System for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019, doi: 10.1109/ACCESS.2019.2907965.

[7] B. Gopalakrishnan and P. Purusothaman, "A new design of intrusion detection in IoT sector using optimal feature selection and high ranking-based ensemble learning model," *Peer-to-Peer Netw. Appl. 2022 155*, vol. 15, no. 5, pp. 2199–2226, Jun. 2022, doi: 10.1007/S12083-022-01336-1.

[8] T. K. Das Manikant Panthi, "Intelligent Intrusion Detection Scheme for Smart Power-Grid Using Optimized Ensemble Learning on Selected Features," *Int. J. Crit. Infrastruct. Prot.*, vol. 39, p. 100567, 2022, doi: https://doi.org/10.1016/j.ijcip.2022.100567.

[9] Cristiano Antonio de Souza, Carlos Becker Westphall, "Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments," *Comput. Electr. Eng.*, vol. 98, p. 107694, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107694.

[10] K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[11] A. A. G. Euclides Carlos Pinto Neto, Sajjad Dadkhah, Raphael Ferreira, Alireza Zohourian, Rongxing Lu, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023, doi: https://doi.org/10.3390/s23135941.

[12] Dr Lachit Dutta, Swapna Bharali, "TinyML Meets IoT: A Comprehensive Survey," *Internet of Things*, vol. 16, no. 9, p. 100461, 2021, doi: 10.1016/j.iot.2021.100461.

[13] Souradip Roy, Juan Li, "A Two-layer Fog-Cloud Intrusion Detection Model for IoT Networks," *Internet of Things*, vol. 19, p. 100557, 2022, doi: https://doi.org/10.1016/j.iot.2022.100557.

[14] Xiaoxuan Wang, Feiyu Zhao, "Evaluating computing performance of deep neural network models with different backbones on IoT-based edge and cloud platforms," *Internet of Things*, vol. 20, p. 100609, 2022, doi: https://doi.org/10.1016/j.iot.2022.100609.

[15] Bayi Xu, Lei Sun, "IoT Intrusion Detection System Based on Machine Learning," *Electronics*, vol. 12, no. 20, p. 4289, 2023, doi: https://doi.org/10.3390/electronics12204289.

[16] P. García-Teodoro, J. Díaz-Verdejo, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, 2009, doi: https://doi.org/10.1016/j.cose.2008.08.003.

[17] S. Guan, J. Wang, C. Jiang, J. Tong, and Y. Ren, "Intrusion detection for wireless sensor networks: A multi-criteria game approach," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2018-April, pp. 1–6, Jun. 2018, doi: 10.1109/WCNC.2018.8377427.

[18] K. D. & B. H. FatimaEzzahra Laghrissi, Samira Douzi, "IDS-attention: an efficient algorithm for intrusion detection systems using attention mechanism," *J. Big Data*, vol. 8, no. 149, 2021, doi: https://doi.org/10.1186/s40537-021-00544-5.

[19] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, Farhan Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, 2020.

[20] T. S. Wooyeon Jo, Sungjin Kim, Changhoon Lee, "Packet Preprocessing in CNN-Based Network Intrusion Detection System," *Electronics*, vol. 9, no. 7, p. 1151, 2020, doi: https://doi.org/10.3390/electronics9071151.

[21] H. Rajadurai and U. D. Gandhi, "A stacked ensemble learning model for intrusion detection in wireless network," *Neural Comput. Appl.*, vol. 34, no. 18, pp. 15387–15395, Sep. 2022, doi: 10.1007/S00521-020-04986-5/METRICS.

[22] S. Z. Owais Bukhari, Parul Agarwal, Deepika Koundal, "Anomaly detection using ensemble techniques for boosting the security of intrusion detection system," *Procedia Comput. Sci.*, vol. 218, pp. 1003–1013, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.080.

[23] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, and L. Lu, "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection," *IEEE Netw.*, vol. 33, no. 5, pp. 75–81, Sep. 2019, doi: 10.1109/MNET.001.1800479.

[24] Sauptik Dhar, Junyao Guo, "A Survey of On-Device Machine Learning: An Algorithms and Learning Theory Perspective," *ACM Trans. Internet Things*, vol. 2, no. 3, 2021, [Online]. Available: https://dl.acm.org/doi/10.1145/3450494

[25] Xiaokang Zhou, Qiuyue Yang, Xuzhe Zheng, Wei Liang, Kevin I-Kai Wang, Jianhua Ma, Yi Pan, Qun Jin, "Personalized Federated Learning With Model-Contrastive Learning for Multi-Modal User Modeling in Human-Centric Metaverse," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, 2024, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10384325

[26] T. R. G. Shaashwat Agrawal, Sagnik Sarkar, Ons Aouedi, Gokul Yenduri, Kandaraj Piamrat, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, "Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions," *arXiv:2106.09527*, 2021, doi: https://doi.org/10.48550/arXiv.2106.09527.

[27] V. C. Riccardo Lazzarini, Huaglory Tianfield, "Federated Learning for IoT Intrusion Detection," *AI*, vol. 4, no. 3, pp. 509–530, 2023, doi: https://doi.org/10.3390/ai4030028.

[28] M. E. Md Mamunur Rashid, Shahriar Usman Khan, Fariha Eusufzai, Md. Azharuddin Redwan, Saifur Rahman Sabuj, "A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks," *Network*, vol. 3, no. 1, pp. 158–179, 2023, doi: https://doi.org/10.3390/network3010008.

[29] R. S. Aashmi, T. Jaya, "Intrusion Detection Using Federated Learning for Computing," *Comput. Syst. Sci. Eng.*, vol. 45, no. 2, pp. 1295–1308, 2023, doi:

10.32604/csse.2023.027216.
[30] P. Ruzafa-Alcázar et al, "Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 19, no. 2, pp. 1145–1154, 2023, doi: 10.1109/TII.2021.3126728.
[31] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li and H. Vincent Poor, "Federated Learning for Internet of Things: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021, doi: 10.1109/COMST.2021.3075439.
[32] Mir Shahnawaz Ahmad, Shahid Mehraj Shah, "A lightweight mini-batch federated learning approach for attack detection in IoT," *Internet of Things*, vol. 25, p. 101088, 2024, doi: https://doi.org/10.1016/j.iot.2024.101088.
[33] S. Chatterjee and M. K. Hanawal, "Federated learning for intrusion detection in IoT security: a hybrid ensemble approach," *Int. J. Internet Things Cyber-Assurance*, vol. 2, no. 1, p. 62, 2022, doi: 10.1504/IJITCA.2022.124372.
[34] F. Wang, G. Xu and M. Wang, "An Improved Genetic Algorithm for Constrained Optimization Problems," *IEEE Access*, vol. 11, pp. 10032–10044, 2023, doi: 10.1109/ACCESS.2023.3240467.
[35] M. L. and M. L. J. Liu, D. Yang, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," *IEEE Access*, vol. 9, pp. 38254–38268, 2021, doi: 10.1109/ACCESS.2021.3063671.
[36] M. Dorigo, V. Maniezzo, and A. Colorni, "Ant system: Optimization by a colony of cooperating agents," *IEEE Trans. Syst. Man, Cybern. Part B Cybern.*, vol. 26, no. 1, pp. 29–41, 1996, doi: 10.1109/3477.484436.
[37] J. Zhang, C. Luo, M. Carpenter, and G. Min, "Federated Learning for Distributed IIoT Intrusion Detection Using Transfer Approaches," *IEEE Trans. Ind. Informatics*, vol. 19, no. 7, pp. 8159–8169, Jul. 2023, doi: 10.1109/TII.2022.3216575.
[38] J. Zhang, C. Luo, M. Carpenter, and G. Min, "Federated Learning for Distributed IIoT Intrusion Detection Using Transfer Approaches," *IEEE Trans. Ind. Informatics*, vol. 19, no. 7, pp. 8159–8169, Jul. 2023, doi: 10.1109/TII.2022.3216575.
[39] J. Li, X. Tong, J. Liu, and L. Cheng, "An Efficient Federated Learning System for Network Intrusion Detection," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2455–2464, Jun. 2023, doi: 10.1109/JSYST.2023.3236995.
[40] D. C. Attota, V. Mothukuri, R. M. Parizi and S. Pouriyeh, "An Ensemble Multi-View Federated Learning Intrusion Detection for IoT," *IEEE Access*, vol. 9, pp. 117734–117745, 2021, doi: 10.1109/ACCESS.2021.3107337.
[41] Bingqin Su, Yuting Lin, "Sewage treatment system for improving energy efficiency based on particle swarm optimization algorithm," *Energy Reports*, vol. 8, pp. 8701–8708, 2022, doi: https://doi.org/10.1016/j.egyr.2022.06.053.
[42] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, "A metaheuristic optimization approach for energy efficiency in the IoT networks," *Softw. - Pract. Exp.*, vol. 51, no. 12, pp. 2558–2571, Dec. 2021, doi: 10.1002/SPE.2797;REQUESTEDJOURNAL:JOURNAL:1097024X.
[43] K. V. Prachi Maheshwari, Ajay K. Sharma, "Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization," *Ad Hoc Networks*, vol. 110, p. 102317, 2021, doi: https://doi.org/10.1016/j.adhoc.2020.102317.
[44] Jayavardhana Gubbi, Rajkumar Buyya, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: https://doi.org/10.1016/j.future.2013.01.010.
[45] M. F. Alam, P. Singla, and R. N. Phursule, "Design of Detection System using Deep

Learning Algorithm for Attack on Network," *2022 IEEE 7th Int. Conf. Converg. Technol. I2CT 2022*, 2022, doi: 10.1109/I2CT54291.2022.9824150.

[46] M. Spirito *et al.*, "Internet of Things applications - From research and innovation to market deployment," *Internet Things Appl. From Res. Innov. to Mark. Deploy.*, pp. 243–286, Jun. 2014, doi: 10.1201/9781003338628/Internet-Things-Applications-Research-Innovation-Market-Deployment-Peter-Friess-Ovidiu-Vermesan/Rights-And-Permissions.

[47] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," *2014 Fed. Conf. Comput. Sci. Inf. Syst. FedCSIS 2014*, pp. 1–8, Oct. 2014, doi: 10.15439/2014F503.

[48] Valerian Rey, Pedro Miguel Sánchez Sánchez, "Federated learning for malware detection in IoT devices," *Comput. Networks*, vol. 204, 2022, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621005582

[49] Kelton A.P. da Costa, João P. Papa, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Networks*, vol. 151, 2019, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128618308739

[50] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2017-October, pp. 267–272, Dec. 2017, doi: 10.1109/MILCOM.2017.8170867.

[51] Q. V. Pham, S. Mirjalili, N. Kumar, M. Alazab, and W. J. Hwang, "Whale Optimization Algorithm with Applications to Resource Allocation in Wireless Networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4285–4297, Apr. 2020, doi: 10.1109/TVT.2020.2973294.

[52] Akash Dogra, "CIC IoT dataset 2023," *Kaggle*, 2023, [Online]. Available: https://www.kaggle.com/datasets/akashdogra/cic-iot-2023

[53] Fatima Asiri, "Explainable federated learning through causal reasoning for intrusion detection in IoT," *Discov. Internet Things*, vol. 6, no. 23, 2026, [Online]. Available: https://link.springer.com/article/10.1007/s43926-026-00292-z

[54] Luo, Yiqiong Liang & Mingwan, "Optimization of distributed network intrusion detection system based on internet of things and federated learning," *Discov. Internet Things*, vol. 6, no. 3, 2026, [Online]. Available: https://link.springer.com/article/10.1007/s43926-025-00260-z

[55] M. Kamran *et al.*, "A blockchain-assisted secure federated learning architecture for intrusion detection in internet of things networks," *Sci. Reports 2026*, May 2026, doi: 10.1038/S41598-026-53053-X.

[56] J. Du, "A novel intrusion detection system for IIoT in 5G networks using attention-augmented federated learning and lightweight transformer architectures," *Sci. Reports 2026*, May 2026, doi: 10.1038/S41598-026-54748-X.

[57] Thien D. Nguyen, Ammar Alazab, Ansam Khraisat & Tony Jan, "Feature reduction in federated learning for intrusion detection in IoT networks," *Cybersecurity*, vol. 9, no. 102, 2026, [Online]. Available: https://link.springer.com/article/10.1186/s42400-025-00509-8

[58] Ali Alqazzaz, "SecuFL-IoT: an adaptive privacy-preserving federated learning framework for anomaly detection in smart industrial networks," *Sci. Rep.*, vol. 16, 2026, [Online]. Available: https://www.nature.com/articles/s41598-025-11883-1

[59] Muhammad Ahmad Bilal, Ihtesham Ul Islam, Sarmad Idrees, "Dataset-centric evaluation of federated intrusion detection models in IoT networks," *Sci. Rep.*, vol. 16, 2026, [Online]. Available: http://nature.com/articles/s41598-025-32567-w

[60] Chao Feng, Alberto Huertas Celdrán, Jing Han, "A crowdsensing intrusion detection

dataset for decentralized federated learning models," *Sci. Data*, 2026, [Online]. Available: https://www.nature.com/articles/s41597-026-07155-w

[61] Q.-V. P. Minh Ngoc Luu, Minh-Duong Nguyen, Ebrahim Bedeer, Van Duc Nguyen, Dinh Thai Hoang, Diep N. Nguyen, "Sample-Driven Federated Learning for Energy-Efficient and Real-Time IoT Sensing," *arXiv:2310.07497*, 2023, doi: https://doi.org/10.48550/arXiv.2310.07497.

[62] "GitHub - iZRJ/Federated-Learning-Based-Intrusion-Detection-System: FL-based intrusion detection system development using model averaging. · GitHub." Accessed: May 31, 2026. [Online]. Available: https://github.com/iZRJ/Federated-Learning-Based-Intrusion-Detection-System

[63] Peter Kairouz, H. Brendan McMahan, Brendan Avent, Peter Kairouz, H. Brendan McMahan, Brendan Avent, "Advances and Open Problems in Federated Learning," *arXiv:1912.04977*, 2019, [Online]. Available: https://arxiv.org/abs/1912.04977

[64] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, "Towards Federated Learning at Scale: System Design," *arXiv:1902.01046*, 2019, [Online]. Available: https://arxiv.org/abs/1902.01046

[65] Aditya Durgadas Naik, Raj Mani Shukla, "Beyond data sharing: enhancing IoT intrusion detection with blockchain-enabled federated learning," *Front. Comput. Sci.*, vol. 8, 2026, doi: https://doi.org/10.3389/fcomp.2026.1770179.

[66] Hafiz Bilal Ahmad, Haichang Gao, "FedMamba: Robust multimodal federated intrusion detection for heterogeneous IoT systems," *Internet of Things*, vol. 6, p. 101877, 2026, doi: https://doi.org/10.1016/j.iot.2026.101877.

[67] N. Hamdi, "Federated learning-based intrusion detection system for Internet of Things," *Int. J. Inf. Secur.*, vol. 22, no. 6, pp. 1937–1948, Dec. 2023, doi: 10.1007/S10207-023-00727-6/METRICS.