Federated Learning–Driven Intrusion Detection in Cloud–IoT Settings: A Security-Centric Survey

[1]Kayode MATTHEW
matthew.kayode@lcu.edu.ng
+234 815 925 4723

&

[2]Temilola JOHN-DEWOLE
johndewole.temilola@lcu.edu.ng
+234 8162047784

[1&2]Department of Computer Science, Lead City University Ibadan, Nigeria

Abstract
The integration of Cloud–IoT ecosystems has accelerated automation and intelligent decision-making but simultaneously introduced critical vulnerabilities that traditional intrusion detection systems (IDS) struggle to address. Centralized IDS approaches suffer from scalability limitations, privacy risks, and single points of failure, making them inadequate for highly distributed IoT environments. Federated Learning (FL) has emerged as a promising paradigm to enhance IDS by enabling collaborative model training without sharing raw data, thereby preserving privacy, reducing communication overhead, and improving detection accuracy. This survey provides a comprehensive review of FL-driven IDS for Cloud–IoT networks, examining architectures, datasets, evaluation metrics, and current methodologies. It discusses state-of-the-art solutions, including cloud–IoT collaboration, hybrid federated frameworks, and privacy-preserving mechanisms such as differential privacy and secure aggregation. Key challenges are identified, including poisoning and inference attacks, client heterogeneity, non-IID data, and the absence of standardized benchmarks. Future research directions highlight the integration of FL with edge intelligence, 6G, explainable AI, energy-efficient protocols, and blockchain to build robust, transparent, and scalable IDS. Ultimately, FL is positioned as a cornerstone for securing next-generation Cloud–IoT infrastructures by balancing performance, privacy, and adaptability.

Keywords: Federated Learning, Intrusion Detection Systems, Cloud–IoT Security

Word Count: 197

Introduction

The rapid proliferation of Cloud–IoT ecosystems has created a vast and heterogeneous infrastructure where billions of interconnected devices generate and transmit sensitive data across networks. While this integration enhances automation, analytics, and intelligent decision-making, it also exposes critical vulnerabilities that can be exploited through attacks such as denial-of-service, malware injection, and unauthorized access (Ahmad et al., 2022; Aqeel et al., 2022). These threats compromise confidentiality, integrity, and availability, making intrusion detection systems (IDS) indispensable. However, traditional centralized IDS solutions are increasingly inadequate in such distributed and dynamic environments, as they face severe scalability, latency, and single-point-of-failure issues (Li et al., 2022).

In addition, centralizing sensitive IoT data raises privacy risks and regulatory concerns, further limiting the practicality of conventional approaches. To overcome these limitations, federated learning (FL) has emerged as a promising paradigm for intrusion detection in Cloud–IoT networks. By enabling collaborative model training across distributed IoT devices without transferring raw data, FL reduces latency, preserves privacy, and scales more effectively in heterogeneous environments (Abreha et al., 2022; Alazab et al., 2023). Its decentralized architecture is particularly advantageous for resource-constrained IoT devices, as only model updates, not raw datasets are shared, lowering bandwidth consumption and exposure to data breaches (Brecko et al., 2022).

Furthermore, FL facilitates cross-organizational collaboration in intrusion detection while adhering to confidentiality requirements, thus improving detection accuracy against sophisticated attacks in real-world IoT and cloud settings (Fedorchenko et al., 2022). These features position FL as a key enabler for next-generation intrusion detection systems in Cloud–IoT ecosystems. This survey provides a comprehensive review of FL-driven intrusion detection for Cloud–IoT environments, covering system architectures, benchmark datasets, evaluation metrics, and state-of-the-art methodologies.

It highlights both the advantages and limitations of FL in addressing security threats, with particular emphasis on challenges such as poisoning attacks, gradient leakage, client heterogeneity, and scalability constraints (Gosselin et al., 2022; Psychogyios et al., 2023). While the survey focuses on the application of FL to intrusion detection in Cloud–IoT systems, it does not extend to adjacent areas such as blockchain-based trust management or purely edge-centric detection frameworks unless directly integrated with FL. The contributions of this work lie in synthesizing existing research, identifying open challenges, and outlining promising future directions to enhance security, robustness, and scalability in FL-based IDS.

Background and Preliminaries

Cloud–IoT Ecosystem

The Internet of Things (IoT) ecosystem represents a complex multi-layered architecture comprising interconnected physical devices, sensors, gateways, communication networks, and

cloud services that collectively enable data collection, processing, and intelligent decision-making (Chatterjee et al., 2023). At its foundation, the IoT conceptual model includes four fundamental entities: digital entities (applications, services, data stores), physical entities (real-world objects embedded with sensors), IoT users (human or digital), and communication networks that facilitate data flow through proximity, access, service, and user networks (Paolone et al., 2022). The ecosystem operates through a hierarchical structure where IoT devices in the sensing and controlling domain capture data, which is then transmitted through gateways and access networks to cloud platforms or edge/fog computing nodes for processing and analytics.

This architecture supports diverse communication technologies including LoRa, Wi-Fi, and Bluetooth Low Energy (BLE), each offering different coverage ranges and power consumption profiles to meet specific application requirements (Ferreira et al., 2022). Security and privacy challenges pose significant threats throughout the IoT ecosystem, with vulnerabilities spanning from device-level physical attacks to network-based intrusions and application-layer exploits (Aqeel et al., 2022).

The interconnected nature of IoT systems creates multiple attack vectors including denial-of-service (DoS) attacks, man-in-the-middle attacks, data breaches, malware injection, and unauthorized access, which can compromise the confidentiality, integrity, and availability of IoT services (Ahmad et al., 2022; Aqeel et al., 2022). To address these security concerns, emerging solutions integrate advanced technologies such as blockchain for decentralized trust management, artificial intelligence and machine learning for intelligent threat detection, and edge computing paradigms that process data closer to devices to reduce latency and improve security (Dubey & Yadav, 2024).

The cloud-IoT integration presents both opportunities for scalable data processing and analytics, as well as additional security challenges requiring comprehensive multi-layered security frameworks that encompass device authentication, secure communication protocols, encrypted data storage, and robust access control mechanisms (Ahmad et al., 2022).

Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are fundamental in identifying malicious activities and unauthorized access within networks or hosts. They primarily rely on two detection approaches: signature-based and anomaly-based methods. Signature-based IDSs detect threats by matching network traffic or system activities against a database of known attack patterns, making them effective for identifying previously catalogued attacks but less capable of detecting new threats (Azam et al., 2023; Nandan et al., 2025). In contrast, anomaly-based IDSs analyze deviations from normal system or network behavior, allowing them to identify unknown or zero-day attacks but often at the cost of higher false positives (Abdelmoumin et al., 2022; Vaigandla et al., 2022). To address the shortcomings of both methods, hybrid IDS solutions integrate signature and anomaly detection, thereby improving detection accuracy while balancing sensitivity and specificity (Azam et al., 2023; Nandan et al., 2025).

Beyond detection techniques, IDSs are also categorized by deployment models, such as centralized, distributed, and hybrid frameworks. Centralized IDS architectures rely on a single monitoring point, which simplifies management but suffers from scalability and single points of failure. Distributed IDSs (DIDSs), on the other hand, deploy multiple nodes that collaborate to share detection data, offering broader visibility and resilience against large-scale or coordinated attacks (Li et al., 2022).

Hybrid models combine centralized coordination with distributed detection, integrating trust-based mechanisms to improve accuracy and reduce false alarms in collaborative environments (Li et al., 2022). This combination enhances the scalability of distributed systems while retaining the efficiency of centralized oversight, making hybrid IDS architectures particularly effective for large, dynamic, and heterogeneous networks, such as the Internet of Things (Nguyen et al., 2022).

Federated Learning (FL) Basics

Federated learning (FL) is a distributed machine learning paradigm where multiple clients, such as IoT devices or organizations, collaboratively train a global model without sharing their raw data. In this architecture, clients train local models on their private datasets and send only model updates to a central server, which aggregates them commonly using Federated Averaging (FedAvg) to produce an improved global model (Alazab et al., 2023; Brecko et al., 2022). This process iterates until convergence, ensuring that sensitive data never leaves the clients' devices. Beyond FedAvg, algorithms such as FedProx and FedNova have been developed to address challenges like heterogeneous data distributions and system variability by introducing regularization or variance reduction mechanisms (Abreha et al., 2022).

The client–server structure may be implemented in different forms, including cloud-based, edge-based, or hierarchical architectures, depending on deployment needs and resource constraints (Abreha et al., 2022). FL offers significant advantages for the IoT ecosystem, where devices are resource-constrained, geographically distributed, and generate sensitive data. By keeping data localized, FL ensures privacy preservation, reduces the risks of breaches, and aligns with regulatory requirements such as GDPR (Brecko et al., 2022). Furthermore, decentralization lowers communication costs since only model parameters, not raw data, are transmitted, making FL scalable for large IoT networks with limited bandwidth (Abreha et al., 2022). In security-sensitive domains such as intrusion detection, FL enables collaborative anomaly detection across multiple clients while protecting confidential logs and network traffic data (Alazab et al., 2023). This collaborative yet privacy-preserving approach makes FL highly promising for IoT applications, providing efficiency, robustness, and enhanced trustworthiness in distributed machine learning.

Security and Privacy Concerns in FL

Federated learning (FL) provides privacy benefits by allowing decentralized training, but it also introduces significant vulnerabilities. One key concern is data poisoning, where malicious clients introduce corrupted or mislabeled data into the training process, degrading accuracy or

inserting backdoors into the global model. For instance, label-flipping or GAN-generated poisoning attacks can manipulate the global model's behavior while evading detection (Psychogyios et al., 2023). Similarly, model poisoning occurs when adversaries alter their local updates before aggregation, which can either reduce overall performance or bias predictions toward targeted outcomes (Chen & Koushanfar, 2023). These attacks highlight the fragility of the aggregation process and the need for robust defenses against malicious updates. In addition to poisoning attacks, FL is vulnerable to inference attacks, where adversaries exploit exchanged gradients or parameters to recover sensitive client information. Recent studies have shown that even without direct data sharing, model updates can leak private details about training datasets, particularly when generative adversarial networks (GANs) are employed for reconstruction (Gosselin et al., 2022). This threat undermines one of FL's main promises: privacy preservation and emphasizes the need for techniques such as differential privacy and secure aggregation. Without these safeguards, adversaries could infer personal attributes or reconstruct raw data from model gradients, exposing users to privacy violations.

Beyond malicious behaviors, FL faces system-level challenges that raise both security and efficiency concerns. Communication overhead is a critical issue, as repeated exchanges of large model updates between clients and servers consume bandwidth and can slow training (Gosselin et al., 2022). Additionally, heterogeneity of client devices and data introduces vulnerabilities: non-IID data distributions and varying device capabilities make models more susceptible to targeted poisoning and degrade aggregation quality (Gosselin et al., 2022). These challenges not only complicate defenses against adversarial manipulation but also reduce scalability and fairness across participants. Therefore, addressing both attack vectors and systemic inefficiencies is essential to making federated learning secure and practical.

Review of State-of-the-Art Approaches in Federated Learning for Intrusion Detection

Federated Learning in IoT Networks

Intrusion Detection Systems (IDS) in Internet of Things (IoT) environments face challenges such as device heterogeneity, limited computational resources, and large-scale distributed data. Federated Learning (FL) has emerged as a promising approach to address these constraints by enabling decentralized training without sharing raw data. FL supports IoT IDS by allowing devices to collaboratively train models while maintaining data locality, thereby mitigating privacy risks (Fedorchenko et al., 2022). However, IoT-based FL IDS must contend with non-IID (non-independent and identically distributed) data, high dropout rates of devices, and skewed data volumes across clients, which can impact model performance (Muneer et al., 2024). Despite these issues, FL has demonstrated potential in reducing communication overhead and improving detection rates in smart home and industrial IoT environments.

Cloud–IoT Collaborative Security

Cloud–IoT collaboration introduces a layered architecture where IoT devices act as local clients while cloud servers aggregate and analyze model updates. This hybrid paradigm leverages the computational power of the cloud while respecting IoT devices' limitations. In practice,

hierarchical federated systems have been proposed, where IoT devices perform preliminary intrusion analysis, and cloud servers aggregate updates to refine detection models (Fedorchenko et al., 2022). This distributed hierarchy ensures scalability and reduces the risk of single points of failure. Moreover, cloud–IoT collaborative IDS frameworks enable cross-silo FL, allowing organizations with sufficient computing resources (e.g., ISPs, data centers) to collaborate while preserving data confidentiality. This paradigm enhances detection accuracy by combining insights from heterogeneous IoT environments with cloud-level intelligence (Muneer et al., 2024).

Privacy-Preserving and Secure Federated Learning

One of the primary motivations for adopting FL in IDS is its ability to enhance privacy and data security. By avoiding centralized data collection, FL minimizes the risk of breaches and complies with privacy regulations. Nonetheless, FL remains vulnerable to inference attacks, gradient leakage, and poisoning attacks. To mitigate these risks, state-of-the-art privacy-preserving techniques have been integrated into FL-based IDS, including differential privacy, homomorphic encryption, secure multiparty computation, and Trusted Execution Environments (Fedorchenko et al., 2022). Differential privacy introduces noise to gradients, balancing accuracy and confidentiality, while secure aggregation protocols protect model updates during transmission. These approaches enhance trustworthiness, though they introduce trade-offs in terms of computational complexity and communication costs. FL's distributed nature thus provides an inherent privacy advantage, further strengthened by cryptographic and hardware-based safeguards (Muneer et al., 2024).

Hybrid Federated Learning Architectures

Hybrid FL architectures combine centralized, decentralized, and hierarchical approaches to achieve resilience, scalability, and adaptability in IDS. In hybrid models, IoT devices, edge servers, and cloud nodes form multi-tier federated systems, balancing local detection efficiency with global intelligence. For example, decentralized peer-to-peer FL among IoT clusters can improve fault tolerance, while cloud-based aggregation ensures consistency across wider networks (Fedorchenko et al., 2022). Such architectures also accommodate both horizontally and vertically partitioned data, a critical factor in intrusion detection where data sources differ across devices and applications. The hybrid paradigm is particularly well-suited for complex environments like smart grids and cyber-physical systems, where cross-domain collaboration is required for robust intrusion detection (Muneer et al., 2024).

Comparative Analysis of Federated Learning for Intrusion Detection

Benchmark Datasets

Benchmark datasets are critical for evaluating intrusion detection systems (IDS), as they provide standardized environments to test accuracy, scalability, and robustness. Within federated learning (FL)-based IDS, several datasets have been widely used:

- NSL-KDD and its predecessors (KDD'99) remain popular due to their historical relevance, despite limitations in representing modern attack patterns (Fedorchenko et al., 2022).
- CICIDS2017 and CIC-DDoS2019 offer realistic and diverse traffic flows, making them particularly suitable for modern IoT and cloud environments (Fedorchenko et al., 2022).
- TON_IoT and Edge-IIoTset datasets address IoT-specific threats, capturing heterogeneous device activity and distributed attack scenarios (Rashid et al., 2023).
- Additional datasets such as MNIST (for testing FL mechanisms rather than intrusion detection directly) and REDD (for power IoTs) are occasionally employed to simulate FL constraints (Rashid et al., 2023).

These datasets differ in complexity and attack representation. For instance, CICIDS2017 and TON_IoT better reflect real-world traffic diversity, while NSL-KDD supports baseline evaluations for algorithmic comparison.

Evaluation Metrics

Federated IDS performance is typically measured with standard machine learning metrics. The most commonly applied include:

- Accuracy, precision, recall, and F1-score for measuring classification correctness and balance between false positives/negatives (Fedorchenko et al., 2022).
- Detection rate (DR) and false alarm rate (FAR), which are critical in IDS evaluation, especially for anomaly-based systems (Rashid et al., 2023).
- Area Under the ROC Curve (AUC) is employed in some studies to evaluate robustness across varying thresholds (Fedorchenko et al., 2022).
- Communication overhead, convergence rate, and resource efficiency are FL-specific metrics, since bandwidth and computational heterogeneity strongly influence IDS applicability (Fedorchenko et al., 2022).

These metrics ensure that both security performance and federated efficiency are assessed simultaneously.

Comparative Review of Existing Works

Recent literature provides comparisons across architectures, datasets, and results. For example:

- Rashid et al. (2023) proposed a CNN- and RNN-based FL model for IIoT intrusion detection using Edge-IIoTset, achieving 92.49% accuracy, closely matching centralized models (93.92%) while preserving privacy.
- Tang et al. used CICIDS2017 with GRU models in FL, achieving high detection accuracy but constrained by the dataset's simulated nature (Rashid et al., 2023).
- Attota et al. developed MV-FLID with multi-view ensemble learning, demonstrating enhanced classification of diverse IoT attacks without centralizing data (Rashid et al., 2023).
- Fedorchenko et al. (2022) reviewed eight recent works and highlighted challenges such as non-IID data, client heterogeneity, and inference attacks, while systematically comparing system architectures, datasets, and performance outcomes.

Table 1: Table showing Comparison of Federated Learning-Based IDS"

Study	Dataset(s)	Model(s)	Accuracy / Key Results	Notable Contribution
Rashid et al. (2023)	Edge-IIoTset	CNN, RNN	92.49%	Privacy-preserving IIoT IDS
Tang et al. (cited in Rashid et al., 2023)	CICIDS2017	GRU	High detection rate	Iterative local training with privacy
Attota et al. (cited in Rashid et al., 2023)	IoT traffic datasets	MV-FLID ensemble	Improved attack classification	Multi-view FL ensemble
Tabassum et al. (cited in Rashid et al., 2023)	IoT datasets	GAN (FEDGAN-IDS)	Faster convergence, higher accuracy	Federated GAN for IDS
Fedorchenko et al. (2022)	Multiple (NSL-KDD, CICIDS2017, TON_IoT, CIC-DDoS2019)	Multiple ML/DL models	Varies (80–95%)	Systematic comparative review

Challenges and Open Issues of Federated Learning

System Challenges

Federated Learning (FL) operates in environments characterized by large-scale deployments, diverse devices, and resource limitations. Scalability is a significant challenge because FL must coordinate updates from potentially millions of edge devices, leading to communication bottlenecks and inefficiencies in global model aggregation (Shaheen et al., 2022). Device heterogeneity further complicates training since participants may have vastly different hardware capabilities, network connectivity, and energy constraints, resulting in stragglers and inconsistent participation (Jiang et al., 2020). Additionally, resource constraints on computation, memory, and bandwidth make it difficult for lightweight devices such as IoT sensors to sustain iterative model training without optimization or specialized protocols (Shen et al., 2020).

Security Challenges

FL is vulnerable to adversarial attacks that exploit its decentralized nature. Poisoning attacks allow malicious clients to inject corrupted updates, distorting the global model's performance (Gosselin et al., 2022). A subset of these, backdoor attacks, stealthily insert hidden triggers into the model to cause misclassifications under specific conditions, posing threats to critical applications such as healthcare and intrusion detection systems (Zhang et al., 2022). Moreover, model aggregation servers themselves can become attack points, as compromised or malicious servers may manipulate updates to bias the learning outcome (Shen et al., 2020).

Privacy Challenges

Despite being more privacy-preserving than centralized learning, FL is still exposed to inference risks. Gradient leakage attacks can reconstruct sensitive raw data from shared model updates using techniques such as Deep Leakage from Gradients (DLG) (Zhang et al., 2022). Additionally, membership inference attacks can determine whether a user's data was part of the training set, which has serious implications for applications involving sensitive domains like healthcare or finance (Gosselin et al., 2022). These vulnerabilities highlight that transmitting gradients instead of raw data does not guarantee absolute privacy.

Data Challenges

The decentralized nature of FL exacerbates data-related issues. Label scarcity is a key limitation since many edge devices generate unlabeled or weakly labeled data, undermining supervised training effectiveness (Shaheen et al., 2022). Furthermore, imbalanced attack distribution can hinder the detection of anomalies in security-sensitive systems such as Cloud–IoT intrusion detection, where malicious data may be concentrated on specific clients (Jiang et al., 2020). Domain shifts across participants, caused by non-IID (non-independent and identically distributed) data, reduce global model generalization and increase bias, making robust aggregation strategies critical (Shen et al., 2020).

Standardization Issues

A final barrier to advancing FL is the lack of unified benchmarks and standardized evaluation protocols. In particular, Cloud–IoT intrusion detection systems (IDS) using FL lack consistent frameworks for comparing datasets, attack models, and defense mechanisms across studies (Jiang et al., 2020). Without standardized benchmarks, it is difficult to measure progress, replicate experiments, or establish best practices for deploying FL in real-world cyber-physical environments.

Future Research Directions of Federated Learning

Integration with Edge Intelligence and 6G-Enabled IoT

The rapid expansion of Internet of Things (IoT) ecosystems demands scalable, intelligent, and privacy-preserving computation paradigms. Integrating FL with edge intelligence enables real-

time analytics while mitigating communication overhead and privacy risks (Abreha et al., 2022). With the advent of 6G-enabled IoT, FL can leverage ultra-low latency, massive connectivity, and distributed intelligence, allowing billions of heterogeneous devices to collaboratively train models without centralized data transfer. Research should focus on designing hybrid FL and split learning frameworks that optimize both resource utilization and privacy in edge-centric and ubiquitous intelligence scenarios (Duan et al., 2022).

Trustworthy Federated Learning: Robust Aggregation and Byzantine Resilience

Although FL preserves privacy, it remains vulnerable to poisoning, inference, and Byzantine attacks. Trustworthy Federated Learning (TFL) frameworks aim to ensure robustness, security, and privacy throughout the lifecycle of data processing, training, and deployment (Zhang et al., 2023). Future research should emphasize robust aggregation mechanisms that can filter malicious or noisy updates while maintaining model accuracy. Byzantine-resilient FL algorithms, capable of identifying and mitigating adversarial client contributions, are critical for deployments in safety-sensitive domains such as healthcare and finance (Chen et al., 2023).

Explainable Intrusion Detection Systems (IDS)

As FL is increasingly applied in network security, explainability becomes essential. FL-driven Intrusion Detection Systems (IDS) should not only achieve high accuracy but also provide interpretable insights into anomalies and attacks. Enhancing interpretability will foster trust among administrators and end-users while meeting regulatory requirements. Research should explore explainable AI techniques adapted to the decentralized nature of FL, ensuring that IDS models remain transparent despite distributed and heterogeneous data sources (Shaheen et al., 2022).

Energy-Efficient FL for Resource-Limited IoT Devices

Many IoT devices have constrained computational power and limited energy resources. Future work must optimize energy-efficient training and communication protocols to make FL sustainable at scale. This includes model compression, adaptive client participation, and offloading strategies to balance workloads across edge nodes (Abreha et al., 2022). The integration of split learning with FL is another promising approach, as it allows resource-constrained devices to offload portions of training to nearby edge servers (Duan et al., 2022).

Benchmarking Frameworks for Fair Comparison

The lack of standardized benchmarks hinders fair evaluation of FL algorithms across diverse IoT and edge scenarios. Establishing benchmarking frameworks with consistent datasets, performance metrics, and evaluation protocols is essential for reproducibility and meaningful comparison of methods. Research should focus on building publicly available benchmarking suites that capture heterogeneity, communication constraints, and adversarial scenarios typical of real-world FL deployments (Shaheen et al., 2022).

Cross-Disciplinary Convergence: FL with Blockchain and Secure Multiparty Computation

Cross-disciplinary convergence offers powerful opportunities to strengthen FL. Blockchain can provide decentralized trust management and immutable audit trails, while Secure Multiparty Computation (SMPC) can enhance privacy in collaborative learning. Future research should explore the synergy of FL with these technologies to develop transparent, secure, and tamper-resistant learning ecosystems (Chen et al., 2023). Such convergence will be particularly relevant for applications in finance, healthcare, and critical infrastructure, where trustworthiness and verifiability are non-negotiable.

Conclusion

This survey underscores the transformative role of federated learning (FL) in enhancing intrusion detection systems (IDS) for Cloud–IoT ecosystems. The review highlighted that FL effectively addresses the limitations of centralized IDS by preserving data privacy, reducing communication overhead, and enabling scalable, collaborative learning across heterogeneous devices. Despite challenges such as poisoning attacks, gradient leakage, non-IID data, and device heterogeneity, state-of-the-art solutions integrating differential privacy, secure aggregation, and hybrid architectures demonstrate FL's potential to deliver resilient and privacy-preserving IDS. These findings reaffirm FL as a promising enabler of secure and intelligent Cloud–IoT infrastructures, particularly as future directions focus on trustworthy aggregation, explainability, energy efficiency, and benchmarking. Moving forward, a clear roadmap involves integrating FL with emerging technologies such as edge intelligence, 6G, blockchain, and secure multiparty computation to ensure robust, transparent, and scalable deployments. Ultimately, FL-driven IDS stand as a cornerstone for building secure, adaptive, and sustainable Cloud–IoT environments.

References

Abdelmoumin, G., Whitaker, J., Rawat, D. B., & Rahman, A. (2022). A survey on data-driven learning for intelligent network intrusion detection systems. *Electronics, 11*(213), 1–22. https://doi.org/10.3390/electronics11020213

Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: A systematic survey. *Sensors, 22*(450), 1–45. https://doi.org/10.3390/s22020450

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics, 11*(1), 16. https://doi.org/10.3390/electronics11010016

Alazab, A., Khraisat, A., Singh, S., & Jan, T. (2023). Enhancing privacy-preserving intrusion detection through federated learning. *Electronics, 12*(3382), 1–16. https://doi.org/10.3390/electronics12163382

Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022). A review of security and privacy concerns in the Internet of Things (IoT). *Journal of Sensors, 2022*, 5724168. https://doi.org/10.1155/2022/5724168

Azam, H., Dulloo, M. I., Majeed, M. H., Phang, J. H. W., Xin, L. T., Tajwar, M. A., & Sindiramutty, S. R. (2023).Defending the digital frontier: IDPS and the battle against cyber threat. *International Journal of Emerging Multidisciplinaries: Computer Science and Artificial Intelligence, 2*(1), 1–28. https://doi.org/10.54938/ijemdcsai.2023.02.1.253

Brecko, A., Kajati, E., Koziorek, J., & Zolotova, I. (2022). Federated learning for edge computing: A survey. *Applied Sciences, 12*(9124), 1–36. https://doi.org/10.3390/app12189124

Chen, H., & Koushanfar, F. (2023). Tutorial: Toward robust deep learning against poisoning attacks. *ACM Transactions on Embedded Computing Systems, 22*(3), 42. https://doi.org/10.1145/3574159

Chen, D., Jiang, X., Zhong, H., & Cui, J. (2023). Building trusted federated learning: Key technologies and challenges. *Journal of Sensor and Actuator Networks, 12*(13), 1–18. https://doi.org/10.3390/jsan12010013

Chatterjee, A., Lobato, C. N., Zhang, H., Bergne, A., Esposito, V., Yun, S., … Pryds, N. (2023). Powering internet-of-things from ambient energy: A review. *JPhys Energy, 5*(2), 022001. https://doi.org/10.1088/2515-7655/acb5e6

Duan, Q., Hu, S., Deng, R., & Lu, Z. (2022). Combined federated and split learning in edge computing for ubiquitous intelligence in Internet of Things: State-of-the-art and future directions. *Sensors, 22*(5983), 1–37. https://doi.org/10.3390/s22165983

Dubey, A., & Yadav, S. K. (2024). Basics of Internet of Things. *International Journal of Scientific Research in Engineering and Management (IJSREM), 8*(10). [PDF without DOI]

Fedorchenko, E., Novikova, E., & Shulepov, A. (2022). Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges. *Algorithms, 15*(7), 247. https://doi.org/10.3390/a15070247

Ferreira, D., Jr., Oliveira, J. L., Santos, C., Filho, T., Ribeiro, M., Freitas, L. A., Moreita, W., & Oliveira-Jr, A. (2022). Planning and optimization of software-defined and virtualized IoT gateway deployment for smart campuses. *Sensors, 22*(13), 4710. https://doi.org/10.3390/s22134710

Gosselin, R., Vieu, L., Loukil, F., & Benoit, A. (2022). Privacy and security in federated learning: A survey. *Applied Sciences, 12*(19), 9901. https://doi.org/10.3390/app12199901

Jiang, J. C., Kantarci, B., Oktug, S., & Soyata, T. (2020). Federated learning in smart city sensing: Challenges and opportunities. *Sensors, 20*(21), 6230. https://doi.org/10.3390/s20216230

Li, W., Meng, W., & Kwok, L. F. (2022). Surveying trust-based collaborative intrusion detection: State-of-the-art, challenges and future directions. *IEEE Communications Surveys & Tutorials, 24*(1), 280–305. https://doi.org/10.1109/COMST.2021.3139052

Muneer, S., Farooq, U., Athar, A., Raza, M. A., Ghazal, T. M., & Sakib, S. (2024). A critical review of artificial intelligence based approaches in intrusion detection: A comprehensive analysis. *Journal of Engineering, 2024*, 3909173. https://doi.org/10.1155/2024/3909173

Nandan, S., Nayak, P., Amar, B. M., Manikanta, & Madakari, K. T. P. (2025). A review on machine learning framework for detection of intrusion. *International Journal of Advanced Research in Science, Communication and Technology, 5*(1), 90–91. https://doi.org/10.48175/IJARSCT-22908

Nguyen, X.-H., Nguyen, X.-D., Huynh, H.-H., & Le, K.-H. (2022). Realguard: A lightweight network intrusion detection system for IoT gateways. *Sensors, 22*(432), 1–18. https://doi.org/10.3390/s22020432

Paolone, G., Iachetti, D., Paesani, R., Pilotti, F., Marinelli, M., & Di Felice, P. (2022). A holistic overview of the Internet of Things ecosystem. *IoT, 3*(4), 398-434. https://doi.org/10.3390/iot3040022

Psychogyios, K., Velivassaki, T.-H., Bourou, S., Voulkidis, A., Skias, D., & Zahariadis, T. (2023). GAN-driven data poisoning attacks and their mitigation in federated learning systems. *Electronics, 12*(8), 1805. https://doi.org/10.3390/electronics12081805

Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in industrial Internet of Things networks. *Network, 3*(1), 158–179. https://doi.org/10.3390/network3010008

Shaheen, M., Farooq, M. S., Umer, T., & Kim, B.-S. (2022). Applications of federated learning: Taxonomy, challenges, and research trends. *Electronics, 11*(4), 670. https://doi.org/10.3390/electronics11040670

Shen, S., Zhu, T., Wu, D., Wang, W., & Zhou, W. (2020). From distributed machine learning to federated learning: In the view of data privacy and security. *arXiv preprint* arXiv:2010.09258. https://arxiv.org/abs/2010.09258

Vaigandla, K. K., Azmi, N., & Karne, R. (2022). Investigation on intrusion detection systems (IDSs) in IoT. *International Journal of Emerging Trends in Engineering Research, 10*(3), 158–166. https://doi.org/10.30534/ijeter/2022/041032022

Zhang, J., Zhu, H., Wang, F., Zhao, J., Xu, Q., & Li, H. (2022). Security and privacy threats to federated learning: Issues, methods, and challenges. *Security and Communication Networks, 2022*, 2886795. https://doi.org/10.1155/2022/2886795

Zhang, Y., Zeng, D., Luo, J., Xu, Z., & King, I. (2023). A survey of trustworthy federated learning with perspectives on security, robustness, and privacy. *arXiv preprint* arXiv:232.10637. https://doi.org/10.48550/arXiv.2302.10637