International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 12, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i12.1552

Federated Industrial IoT Threats Detection

Benjamin Agyekum[1]; Daniel Seffah- Duodu[2]; Agyapong Gloria[3]

[1]Department of Electrical and computer engineering, Colorado State University, Fort Collins, USA.
[2]Department of electrical and computer, Colorado State University, Fort Collins, USA
[3]Department of Geosciences, Texas Tech University, Lubbock, TX, USA

Publication Date: 2025/12/28

Abstract

Industrial Internet of Things networks are increasingly exposed to coordinated cyber threats, including denial-of-service attacks, botnet propagation, command injection, data exfiltration, false-data injection, and lateral movement across cyber-physical production systems. Conventional centralized intrusion detection models often require raw industrial traffic to be transmitted to cloud servers, creating privacy risks, bandwidth overhead, latency constraints, and weak adaptability across heterogeneous plants. This paper proposes a privacy-preserving federated threat-detection framework titled Fed-IIoTGuard, a novel hybrid algorithm that integrates temporal convolutional feature extraction, gated recurrent traffic profiling, attention-based client weighting, and adaptive secure aggregation for detecting threats in distributed Industrial IoT environments. The proposed model is designed to learn from multiple edge gateways, programmable logic controller networks, smart sensors, supervisory control and data acquisition nodes, and industrial robots without exposing raw operational data.

Fed-IIoTGuard is compared with traditional machine learning and federated learning baselines, including Random Forest, Support Vector Machine, XGBoost, centralized CNN-LSTM, FedAvg, FedProx, FedYogi, FedNova, and SCAFFOLD. The evaluation is structured around key performance indicators such as accuracy, precision, recall, F1-score, false alarm rate, detection latency, communication overhead, convergence speed, and robustness under non-IID data distribution. The paper further presents comparative graphs showing algorithmic performance across normal traffic, denial-of-service traffic, reconnaissance attacks, command injection, spoofing, and data manipulation attacks. The proposed Fed-IIoTGuard framework is expected to demonstrate superior performance by improving minority attack detection, reducing false positives, accelerating convergence, and maintaining data confidentiality across distributed industrial sites. The study contributes a scalable and privacy-aware threat-detection architecture for next-generation smart factories, energy systems, manufacturing plants, and critical industrial infrastructures.

Keywords: *Federated Learning; Industrial IoT; Threat Detection; Intrusion Detection; Cybersecurity.*

I. INTRODUCTION

➢ *Background of Industrial IoT Threat Detection*

Industrial Internet of Things threat detection has become a strategic requirement because modern factories, energy plants, logistics systems, maritime platforms, and process-control environments now depend on dense interconnection among sensors, actuators, programmable logic controllers, supervisory control and data acquisition nodes, edge gateways, and cloud-based analytics platforms. This connectivity improves real-time monitoring, predictive maintenance, autonomous decision-making, and operational optimization, but it also extends the industrial attack surface beyond traditional perimeter-based security. In such environments, cyber threats are not limited to information theft; they can manipulate machine states, corrupt sensor values, delay control commands, disrupt vessel-to-shore communication, degrade safety-critical automation, or cause production downtime. The virtualization, containerization, and IoT-enabled communication models discussed by Ibokette et al. (2024) are directly relevant because the same technologies that improve scalability and real-time data handling also increase the need for continuous anomaly detection across distributed industrial traffic streams.

The proposed paper therefore positions federated Industrial IoT threat detection as a technical response to the privacy, scale, heterogeneity, and latency limitations of centralized intrusion detection. Conventional machine learning models can detect anomalies in industrial control systems, but their effectiveness depends on representative training data, careful feature selection, and robust

Agyekum, B., Duodu, D. S.-., & Gloria, A. (2025). Federated Industrial IoT Threats Detection.
International Journal of Scientific Research and Modern Technology, *4*(12), 226–244.
https://doi.org/10.38124/ijsrmt.v4i12.1552

evaluation across network-level and process-level behavior (Umer et al., 2022). Federated learning extends this logic by allowing distributed industrial clients to train a shared detection model without exposing raw operational data, a direction strongly aligned with the open challenges identified in privacy-preserving collaborative learning (Kairouz et al., 2021). In the context of this study, Fed-IIoTGuard is conceptualized as a federated algorithm that learns temporal traffic patterns, device-specific behavior, and attack signatures from multiple industrial nodes while preserving data locality. This is particularly relevant to advanced IoT and ubiquitous computing environments where intelligent machines, synthetic agents, and automated decision systems increasingly interact with cyber-physical infrastructure (Idoko et al., 2024).

- *Cybersecurity Challenges in Distributed Industrial Networks*

Distributed industrial networks face a difficult cybersecurity problem because their operating conditions combine real-time control, heterogeneous device capabilities, legacy communication protocols, human-machine interaction, and strict availability requirements. Unlike ordinary enterprise networks, Industrial IoT environments cannot always tolerate aggressive packet inspection, frequent shutdowns, heavy cryptographic operations, or delayed inference because control loops may depend on millisecond-level responsiveness. Cyber-physical systems also involve tight coupling between computation and physical processes, meaning that a spoofed sensor reading, unauthorized actuator command, or delayed controller response may trigger safety, environmental, or production consequences (Ashibani & Mahmoud, 2017). IoT-enabled monitoring improves industrial visibility, but it also generates continuous telemetry that must be protected against tampering, replay, interception, and unauthorized profiling (Ussher-Eke et al., 2025). These challenges become more severe when multiple plants, suppliers, contractors, and remote monitoring stations exchange operational data across shared infrastructure.

The threat landscape is further complicated by advanced persistent threats, insider actions, phishing-enabled credential compromise, vendor access abuse, and adversarial manipulation of machine learning pipelines. Human-enabled security breaches remain relevant in industrial environments because operators, maintenance engineers, third-party technicians, and system administrators often possess privileged access to operational technology assets (Ijiga et al., 2025). Federated learning addresses part of this challenge by reducing raw-data transfer, but it introduces its own security concerns, including poisoned model updates, inference attacks, malicious clients, aggregation manipulation, and privacy leakage from gradients (Mothukuri et al., 2021). Consequently, Fed-IIoTGuard must not be treated merely as a distributed classifier; it must function as a resilient industrial security framework. Its design should include secure aggregation, client-trust estimation, abnormal-update filtering, and performance monitoring across non-IID traffic partitions. In practical terms, a refinery gateway, a robotic production cell, and a smart energy substation may each observe different attack frequencies and normal behavior profiles, yet all must contribute safely to a shared threat-detection model.

- *Limitations of Centralized Intrusion Detection Systems*

Centralized intrusion detection systems are limited in Industrial IoT because they often require raw traffic, logs, telemetry, and process data to be transferred from distributed industrial sites to a central server for model training or analysis. This creates four major technical weaknesses: privacy exposure, communication overhead, delayed detection, and weak scalability. In a smart factory or power distribution network, raw operational data may reveal production schedules, equipment states, proprietary process parameters, maintenance weaknesses, or security configurations. Sending such data to a cloud server increases the risk of unauthorized access and conflicts with zero-trust principles that require continuous protection of sensitive workloads and infrastructure states (Abiola & Ijiga, 2025). Centralized collection also becomes expensive when high-frequency sensor streams, programmable logic controller logs, and network flows are generated continuously across several industrial locations.

A second limitation is that centralized models often fail to generalize across heterogeneous sites. An intrusion detection model trained on traffic from one production line may underperform when deployed in another plant where devices, communication protocols, workloads, and attack distributions differ. Federated learning studies in IoT intrusion detection have shown that decentralized training can preserve data locality while producing competitive performance against centralized alternatives (Lazzarini et al., 2023). However, even federated systems must be carefully designed because client imbalance, non-IID data, aggregation strategy, and model drift affect performance (Campos et al., 2022). Centralized systems are also vulnerable to adversarial machine learning threats because attackers may poison training data, evade detection by crafting subtle traffic variations, or exploit overfitted decision boundaries (Ijiga et al., 2024). These limitations justify the need for Fed-IIoTGuard as a more adaptive architecture that compares favorably against Random Forest, SVM, XGBoost, CNN-LSTM, FedAvg, FedProx, FedYogi, FedNova, and SCAFFOLD. Its novelty lies in combining temporal feature extraction, gated recurrent profiling, attention-based client weighting, and secure aggregation to improve detection without centralizing industrial data.

- *Motivation for Federated Learning in Industrial IoT Security*

The motivation for federated learning in Industrial IoT security is grounded in the need to learn collaboratively from distributed industrial environments without weakening privacy, bandwidth efficiency, or operational autonomy. Industrial organizations often cannot pool raw security data because traffic captures may contain sensitive machine states, proprietary control logic, plant-layout information, or regulatory-relevant operational records. Federated learning provides a

practical alternative by allowing each edge gateway, sensor cluster, SCADA node, or industrial subnet to train locally and share model updates rather than raw data. This is directly aligned with privacy-preserving threat-detection research in IoT environments, where decentralized learning is used to improve security analytics without central data exposure (Idika & Salami, 2024). In Industrial IoT, this advantage is especially important because threat intelligence must be built across many geographically separated and operationally diverse sites.

The proposed Fed-IIoTGuard framework is motivated by the observation that ordinary federated intrusion detection is not sufficient unless it also addresses non-IID data, class imbalance, communication cost, poisoning risk, and site-specific behavior. Agrawal et al. (2022) identify these issues as central challenges in federated intrusion detection, while Pecherle et al. (2025) show that federated Industrial IoT detection can reduce privacy risk and transmission overhead when compared with traditional centralized learning. The present study extends this direction by proposing attention-based client weighting, temporal convolutional extraction, gated recurrent profiling, and adaptive secure aggregation (Olumba, et al., 2025). This makes the model suitable for detecting denial-of-service attacks, reconnaissance, command injection, spoofing, false-data injection, and data manipulation across heterogeneous industrial clients. The motivation also extends to insider-risk contexts because distributed enterprise systems require security models that learn from local behavior while minimizing exposure of confidential logs and access patterns (Ijiga et al., 2025). Thus, the research treats federated learning not only as a privacy tool but as a scalable industrial-defense mechanism.

➢ *Problem Statement*

The central problem addressed in this study is that existing Industrial IoT threat-detection systems remain insufficiently adaptive, privacy-preserving, and robust under distributed industrial conditions. Although machine learning and deep learning models have improved attack classification, many still depend on centralized datasets, balanced traffic assumptions, static feature spaces, and laboratory conditions that do not fully represent real industrial deployments. Industrial IoT networks generate heterogeneous data from predictive-maintenance sensors, transportation infrastructure, embedded controllers, safety systems, and edge devices, making model generalization technically difficult (Ebika et al., 2024). Deep recurrent neural networks can learn temporal intrusion patterns in IoT traffic, but they may require large centralized datasets and substantial computational resources (Almiani et al., 2020). Hybrid deep learning models can also achieve strong performance on benchmark datasets, yet their deployment in distributed industrial sites remains constrained by privacy, latency, and communication overhead (Khan et al., 2023).

The problem is therefore not simply whether an algorithm can detect an attack, but whether it can detect diverse attacks across multiple industrial clients without exposing raw data, degrading real-time response, increasing false alarms, or failing under non-IID traffic distributions. Existing models also provide limited protection against sophisticated threat evolution, including adversarial manipulation, synthetic attack patterns, and explainability gaps. Explainable CNN-based cybersecurity research demonstrates the growing importance of interpretable detection in complex threat environments, particularly where operators must understand why a model flags suspicious activity (James et al., 2025). This study responds to the problem by proposing Fed-IIoTGuard, a novel federated algorithm designed to outperform conventional machine learning, centralized deep learning, and standard federated baselines. The unresolved technical gap is the absence of a unified framework that jointly optimizes privacy preservation, temporal threat learning, client-specific weighting, communication efficiency, and robust detection across distributed Industrial IoT attack classes. Addressing this gap is essential for smart factories, energy systems, transportation infrastructure, and critical industrial facilities where cyber compromise can produce operational, financial, and safety consequences.

➢ *Research Objectives and Research Questions*

- *The Objectives of this Study are:*

✓ To design a federated Industrial IoT threat-detection framework capable of learning from distributed industrial clients without transferring raw operational data.
✓ To develop the proposed Fed-IIoTGuard algorithm using temporal convolutional feature extraction, gated recurrent traffic profiling, attention-based client weighting, and adaptive secure aggregation.
✓ To compare Fed-IIoTGuard with selected baseline algorithms, including Random Forest, SVM, XGBoost, centralized CNN-LSTM, FedAvg, FedProx, FedYogi, FedNova, and SCAFFOLD.
✓ To evaluate the model using accuracy, precision, recall, F1-score, false alarm rate, detection latency, communication overhead, convergence speed, and robustness under non-IID data distributions.
✓ To generate comparative graphs that demonstrate the performance behavior of the proposed model across denial-of-service, reconnaissance, spoofing, command injection, false-data injection, and data manipulation attacks.

- *The Research Questions are*:

✓ How can federated learning be structured to improve privacy-preserving threat detection in distributed Industrial IoT networks?
✓ How does Fed-IIoTGuard perform when compared with traditional machine learning, centralized deep learning, and standard federated learning baselines?

✓ To what extent does attention-based client weighting improve detection performance under non-IID industrial traffic conditions?

- ✓ How does the proposed model affect false alarm rate, latency, communication cost, and convergence speed?
- ✓ What operational value does the proposed framework provide for securing smart factories, industrial control systems, energy facilities, and cyber-physical production environments?

➢ *Contributions and Significance of the Study*

This study contributes a technically grounded framework for privacy-preserving Industrial IoT threat detection by proposing Fed-IIoTGuard as a novel federated algorithm tailored to heterogeneous industrial networks. Its first contribution is architectural: it defines a distributed detection model in which edge gateways, sensors, PLC-linked nodes, SCADA-connected devices, and industrial robots participate in collaborative learning without exposing raw traffic or process data. Its second contribution is algorithmic: it integrates temporal convolutional learning, gated recurrent profiling, attention-based client scoring, and secure aggregation into a unified model intended to improve detection accuracy, reduce false positives, and stabilize convergence under non-IID conditions. Its third contribution is comparative: it benchmarks the proposed algorithm against conventional classifiers, centralized deep learning, and established federated baselines to show whether performance superiority is achieved across multiple evaluation metrics. Its fourth contribution is practical: it produces graph-based evidence for industrial cybersecurity decision-makers by comparing accuracy, F1-score, false alarm rate, detection latency, communication overhead, and convergence behavior. The significance of the study lies in its relevance to smart manufacturing, industrial automation, critical infrastructure, and energy systems where threat detection must be accurate, privacy-aware, scalable, and operationally deployable.

➢ *Scope of the Review and Structure of the Paper*

The scope of this paper covers federated threat detection in Industrial IoT environments, with emphasis on distributed intrusion detection, privacy-preserving learning, non-IID industrial traffic, edge-based model training, secure aggregation, and algorithmic comparison. The review focuses on Industrial IoT networks involving sensors, actuators, programmable logic controllers, supervisory control systems, edge gateways, smart machines, industrial robots, and cloud-coordinated analytics platforms. It considers major threat classes such as denial-of-service attacks, reconnaissance, spoofing, command injection, false-data injection, data manipulation, botnet behavior, and unauthorized access. The paper is structured into five main sections. Section 1 introduces the background, cybersecurity challenges, limitations of centralized detection, motivation for federated learning, problem statement, research objectives, research questions, contributions, significance, and scope. Section 2 reviews Industrial IoT architecture, cyber-physical attack surfaces, machine learning and deep learning intrusion detection, federated learning-based detection, and research gaps. Section 3 describes the proposed system model, threat model, Fed-IIoTGuard algorithm, privacy mechanism, and evaluation metrics. Section 4 discusses the comparative results using graphs and performance metrics. Section 5 presents the conclusions, recommendations, limitations, and future research directions.

II. LITERATURE REVIEW

➢ *Industrial IoT Architecture and Cyber-Physical Attack Surfaces*

Industrial IoT architecture is typically organized as a layered cyber-physical environment in which sensors, actuators, embedded controllers, programmable logic controllers, edge gateways, supervisory control systems, industrial networks, cloud services, and analytics platforms interact continuously. This architecture differs from ordinary enterprise computing because digital events are directly coupled with physical production processes, including temperature regulation, robotic motion, pressure control, energy distribution, optical fiber communication, and automated safety interlocks as represented in figure 1. Boyes et al. (2018) describe IIoT as an extension of cyber-physical and Industry 4.0 systems, where devices are not merely connected but operationally embedded within industrial value chains. In this context, the attack surface includes physical devices, firmware, fieldbus communication, remote terminal units, SCADA servers, historian databases, wireless links, virtualized services, and third-party remote access channels.

For the proposed Fed-IIoTGuard framework, the architecture is important because threat detection must occur close to the industrial source of data without exposing raw process traffic. Optical fiber anomaly detection research shows that high-speed industrial communication systems require real-time cyberattack mitigation because latency and signal integrity directly affect operational reliability (Gabla et al., 2025). Similarly, blockchain-based intrusion detection in decentralized healthcare exchange networks demonstrates how distributed trust and tamper resistance can strengthen sensitive data environments, a principle transferable to federated Industrial IoT security (Idika & Ijiga, 2025). However, SCADA risk assessment literature warns that industrial systems contain legacy assets, protocol weaknesses, and safety-critical dependencies that make purely centralized monitoring inadequate (Cherdantseva et al., 2016). Fed-IIoTGuard therefore treats each edge gateway as a local intelligence node capable of learning plant-specific threat behavior while contributing encrypted model updates to a global detection layer. This design reduces raw-data movement while expanding detection coverage across heterogeneous cyber-physical attack surfaces.

Fig 1 Industrial IoT Architecture Showing Human-Machine Interaction, Robotic Automation, Real-Time Analytics, and Cyber-Physical Attack Surfaces (Verma, D. 2024).

Figure 1 illustrates a layered *Industrial IoT architecture* in which a human operator interacts with cyber-physical production assets through digital control interfaces, edge devices, industrial robots, and real-time analytics dashboards. The worker standing beside the control panel represents the human-machine interface layer, where operators monitor equipment status, issue commands, and interpret production data through tablets, SCADA screens, and supervisory consoles. The robotic arms in the background represent the physical automation layer, where actuators execute commands received from controllers, sensors, and programmable logic controllers. The transparent digital dashboards, charts, telemetry indicators, and system icons represent the IIoT data layer, where machine states, packet flows, device health, process variables, production metrics, and anomaly signals are collected and analyzed. From a cybersecurity perspective, the image also reveals several cyber-physical attack surfaces: the operator tablet may be exposed to credential theft or malware; the control panel may be vulnerable to unauthorized command injection; the robotic controllers may be affected by spoofed instructions or false-data injection; and the networked analytics interface may be targeted through denial-of-service, reconnaissance, or data manipulation attacks. In the context of Fed-IIoTGuard, each of these industrial nodes can act as a local federated client that learns threat patterns from its own traffic and operational behavior without transmitting raw plant data to a centralized server. This makes the architecture suitable for privacy-preserving, low-latency, and distributed threat detection across smart factories and other Industrial IoT environments.

➢ *Threat Categories in Industrial IoT Networks*

Threat categories in Industrial IoT networks can be grouped according to the layer, target, and operational consequence of the attack. At the perception layer, adversaries may compromise sensors, manipulate actuator signals, inject false measurements, clone device identities, or exploit weak firmware. At the network layer, common threats include denial-of-service, distributed denial-of-service, reconnaissance, packet replay, man-in-the-middle interception, spoofing, routing abuse, and protocol exploitation. At the application and control layers, attacks may involve command injection, malware deployment, unauthorized remote access, privilege escalation, data exfiltration, ransomware, and manipulation of SCADA or historian records as presented in table 1. Knowles et al. (2015) emphasize that industrial control systems are increasingly exposed because formerly isolated systems now interact with enterprise netw orks and external services. This interconnection transforms local equipment faults into enterprise-wide cyber-physical risks. The threat taxonomy adopted in Fed-IIoTGuard is designed to capture both network-level and process-level anomalies. Deep learning-driven malware classification in edge computing architectures is relevant because industrial malware may spread through containerized services, microservices, and edge nodes before reaching operational technology assets (Idika et al., 2021). Graph-based anomaly detection is also relevant because many Industrial IoT attacks are relational: compromised devices may communicate with unusual peers, create abnormal transaction paths, or generate near-real-time behavioral deviations that are more visible in graph structures than in isolated packet features (Amebleh et al., 2021). Mitchell and Chen (2014) classify cyber-physical intrusion detection according to detection method and audit material, which supports the need for hybrid monitoring across network traffic, host behavior, and physical process signals. In this paper, threat classes such as DoS, reconnaissance, spoofing, command injection, false-data

injection, botnet propagation, and lateral movement are used to test whether Fed-IIoTGuard can detect both frequent and minority attacks (Igwenagu, et al., 2025). This is technically necessary because industrial environments often exhibit severe class imbalance, where rare attacks may be more operationally destructive than common scanning traffic.

Table 1 Summary of Threat Categories in Industrial IoT Networks

Threat Category	Attack Description	Industrial IoT Target Area	Possible Operational Impact
Denial-of-Service Attacks	Floods industrial devices, gateways, or servers with excessive traffic to exhaust processing or network resources.	Edge gateways, SCADA servers, PLC networks, industrial routers	Production downtime, delayed control signals, loss of monitoring visibility
Reconnaissance Attacks	Scans devices, ports, protocols, and network paths to identify exploitable weaknesses.	IIoT sensors, controllers, remote access points, industrial subnets	Exposure of vulnerable assets and preparation for advanced intrusion
Spoofing and Impersonation	Uses forged device identities or falsified communication sources to appear as a trusted industrial node.	Sensor nodes, PLCs, human-machine interfaces, authentication channels	Unauthorized command execution, false trust relationships, manipulated control decisions
Command Injection	Sends unauthorized or malicious control instructions to industrial devices or automation systems.	PLCs, actuators, robotic controllers, SCADA command interfaces	Unsafe machine behavior, process disruption, equipment damage
False-Data Injection	Alters sensor readings, process values, or telemetry streams to mislead monitoring and control systems.	Smart sensors, meters, historian databases, process-control feedback loops	Incorrect operational decisions, hidden faults, safety compromise
Malware and Botnet Propagation	Deploys malicious software across interconnected industrial endpoints to create persistence or coordinated attacks.	Edge devices, embedded controllers, maintenance laptops, industrial workstations	Lateral movement, data theft, coordinated disruption, ransomware exposure
Data Manipulation and Exfiltration	Modifies, steals, or leaks industrial records, traffic logs, production data, or configuration files.	Cloud platforms, historian servers, databases, IoT analytics systems	Loss of confidentiality, corrupted analytics, regulatory and financial consequences

- *Machine Learning and Deep Learning-Based Intrusion Detection in IIoT*

Machine learning and deep learning have become central to IIoT intrusion detection because rule-based systems cannot reliably detect evolving, low-frequency, or multi-stage attacks in high-dimensional industrial traffic. Traditional models such as Support Vector Machine, Random Forest, Decision Tree, Naïve Bayes, k-nearest neighbor, and XGBoost remain useful for structured flow features, especially when interpretability, low computational cost, and rapid deployment are required. However, deep learning models such as CNN, LSTM, GRU, autoencoders, temporal convolutional networks, and hybrid CNN-LSTM architectures are more suitable for extracting nonlinear relationships from sequential traffic, sensor behavior, and device-state transitions. Ferrag et al. (2020) show that deep learning-based intrusion detection has expanded across multiple cybersecurity datasets and model families, making comparative evaluation essential rather than optional.

The proposed Fed-IIoTGuard model builds on this literature but addresses a deployment gap: many strong ML and DL models assume centralized data access, while real Industrial IoT systems are distributed, privacy-sensitive, and non-IID. Distributed deep learning research has shown that attack detection can benefit from node-level learning rather than relying entirely on centralized architectures (Diro & Chilamkurti, 2018). AI-driven compliance automation and fraud detection further demonstrate that intelligent detection systems become more valuable when they combine anomaly recognition with operational accountability, auditability, and risk prioritization (Frimpong et al., 2023). Similarly, predictive AI/ML applications in healthcare show the importance of identifying subtle abnormal patterns from heterogeneous data streams before adverse outcomes occur (Onyekaonwu et al., 2019). Fed-IIoTGuard extends these principles into Industrial IoT by combining temporal convolutional extraction, gated recurrent profiling, attention-based client weighting, and adaptive secure aggregation. Its comparative evaluation against Random Forest, SVM, XGBoost, centralized CNN-LSTM, FedAvg, FedProx,

FedYogi, FedNova, and SCAFFOLD is necessary to establish whether the proposed model improves accuracy, recall, F1-score, false alarm rate, detection latency, communication overhead, and convergence under realistic industrial data heterogeneity.

- *Federated Learning for Privacy-Preserving Industrial Threat Detection*

Federated learning provides a technically appropriate foundation for privacy-preserving Industrial IoT threat detection because it allows geographically distributed industrial clients to train local models without transferring raw operational data to a centralized server. In a practical IIoT environment, edge gateways, PLC-connected networks, SCADA nodes, optical communication links, robotics cells, and smart sensors may each generate sensitive traffic patterns that reveal production cycles, equipment conditions, control logic, or maintenance weaknesses (Esiobu, et al., 2025). Centralizing such data increases exposure risk and may violate organizational confidentiality requirements. Federated learning addresses this problem by exchanging model parameters or encrypted updates rather than raw packets, logs, or sensor streams. The relevance of lightweight packet-level anomaly detection is important here because industrial branches and headquarters require stable link monitoring with minimal communication burden (Akpara et al., 2024) as represented in figure 2. Similarly, federated network intrusion detection demonstrates that distributed learning can preserve data locality while still building a shared detection model for network security (de Oliveira et al., 2023).

Within the proposed Fed-IIoTGuard framework, privacy preservation is treated as both a data-governance requirement and a cybersecurity design principle. The model combines temporal convolutional feature extraction, gated recurrent traffic profiling, attention-based client weighting, and adaptive secure aggregation so that local clients contribute threat intelligence without exposing plant-specific traffic. Blockchain and federated intrusion detection research supports this direction by showing that decentralized trust mechanisms can strengthen edge-enabled Industrial IoT security (Ali et al., 2024). Interpretable anomaly detection through variational autoencoders and explanation techniques is also relevant because industrial operators must understand why a model flags abnormal behavior, especially where automated responses may interrupt production (Tiamiyu et al., 2024). In addition, predictive structural-health-monitoring studies show that machine learning becomes more valuable when it detects early degradation patterns from distributed sensing environments (Avevor et al., 2024). Fed-IIoTGuard applies this logic to cyber threats by detecting abnormal device behavior, spoofed communication, command injection, false-data manipulation, reconnaissance, and denial-of-service attempts across distributed industrial sites.

Figure 2 illustrates *federated learning for privacy-preserving industrial threat detection* by showing several distributed industrial plants connected to a central federated learning coordination server without transferring raw operational data. Each plant, represented as Plant A, Plant B, Plant C, and Plant D, functions as an independent Industrial IoT client with its own factory machines, robotic arms, PLC-connected devices, edge gateways, and local AI threat-detection model. The local dashboards showing "Local Model Training" indicate that each industrial site trains its model using its own traffic patterns, sensor readings, command sequences, and anomaly records, while the warning panels show different threat events such as anomalous network traffic, unauthorized access, command injection, and abnormal PLC behavior. The glowing encrypted links between the plants and the central server represent secure model-update transmission, meaning that only trained parameters or protected model updates are shared, while raw factory data remains inside each plant. The central cloud labelled as a federated learning coordination server represents the secure aggregation layer, where updates from all plants are combined to produce a stronger global threat-detection model. The lock icons and privacy message emphasize that sensitive industrial data such as production cycles, device identities, PLC commands, and process-control logs are not exposed to external servers. This directly reflects the purpose of Fed-IIoTGuard in Section 2.4: to enable collaborative learning across distributed Industrial IoT environments while preserving privacy, reducing communication overhead, improving real-time anomaly detection, and strengthening protection against attacks such as DoS, reconnaissance, spoofing, command injection, false-data injection, and botnet propagation.

Fig 2 Federated Learning Architecture for Privacy-Preserving Industrial IoT Threat Detection Across Distributed Smart Factory Clients.

➢ *Research Gaps in Existing Federated IoT Threat Detection Models*

Existing federated IoT threat-detection models still contain several unresolved technical gaps that limit their industrial deployability. First, many models are evaluated under simplified benchmark conditions where client data partitions are either artificially balanced or insufficiently representative of real industrial heterogeneity. In actual IIoT systems, one plant may produce mostly normal production traffic, another may experience frequent scanning attempts, while another may contain rare but severe command-injection or false-data attacks. Non-IID data remains a major weakness because it can reduce model accuracy, slow convergence, and bias the global model toward dominant clients or majority classes (Ma et al., 2022) as represented in figure 3. Privacy-preserving federated learning literature also shows that protection mechanisms must address gradient leakage, inference attacks, poisoning, secure aggregation, and system-level trust, yet many IIoT intrusion models focus mainly on accuracy while underreporting privacy and adversarial resilience (Yin et al., 2021).

Second, current models often lack sufficient integration of interpretability, transferability, and minority-threat sensitivity. Deep learning surveillance research shows that detection systems must recognize subtle, context-dependent abnormal patterns rather than relying only on obvious signatures (Ijiga et al., 2024). AI-assisted early detection in medical imaging further illustrates the value of combining high-dimensional feature extraction with dependable decision support, especially where delayed detection can produce serious consequences (Idoko et al., 2024). Transfer learning research using EfficientNet also demonstrates that pretrained feature representations can improve detection where labeled data are limited or unevenly distributed (Oyebanji et al., 2024). These insights expose a gap in federated IIoT threat detection: many systems do not adequately address rare attack classes, explainable industrial alerts, communication-efficient model updates, and adaptive weighting of clients with different data quality. Fed-IIoTGuard is therefore positioned to close this gap by combining temporal convolutional extraction, gated recurrent profiling, attention-based aggregation, and secure federated coordination. Its comparison with Random Forest, SVM, XGBoost, centralized CNN-LSTM, FedAvg, FedProx, FedYogi, FedNova, and SCAFFOLD is necessary to demonstrate whether the proposed model offers measurable superiority in accuracy, F1-score, false alarm rate, latency, communication cost, and robustness.

Figure 3 explains that the major research gaps in existing federated Industrial IoT threat-detection models are concentrated around four interconnected technical weaknesses: data heterogeneity, privacy-security exposure, deployment inefficiency, and weak practical validation. The first branch, non-IID data and industrial traffic heterogeneity, shows that IIoT clients rarely generate similar data because PLCs, SCADA nodes, robotic cells, smart meters, and edge gateways operate under different workloads, protocols, sampling rates, and attack frequencies. This creates client drift, class imbalance, and weak minority-threat detection, especially for rare but dangerous attacks such as command injection and false-data manipulation. The second branch, privacy, security, and trust weaknesses, highlights that federated

learning does not automatically guarantee security because model updates may still leak sensitive operational patterns, while compromised clients may inject poisoned gradients into the global model. The third branch, communication, latency, and edge deployment constraints, captures the difficulty of running repeated federated training rounds in resource-limited industrial environments where bandwidth, memory, processing power, and response time are constrained. The fourth branch, interpretability, evaluation, and practical validation gaps, shows that many existing models report accuracy without adequately explaining alerts, measuring false alarm rate, testing detection latency, or validating performance on realistic industrial attack classes. Together, the diagram justifies the need for Fed-IIoTGuard, which addresses these gaps through temporal feature learning, gated recurrent traffic profiling, attention-based client weighting, secure aggregation, and comparative evaluation against established federated baselines.

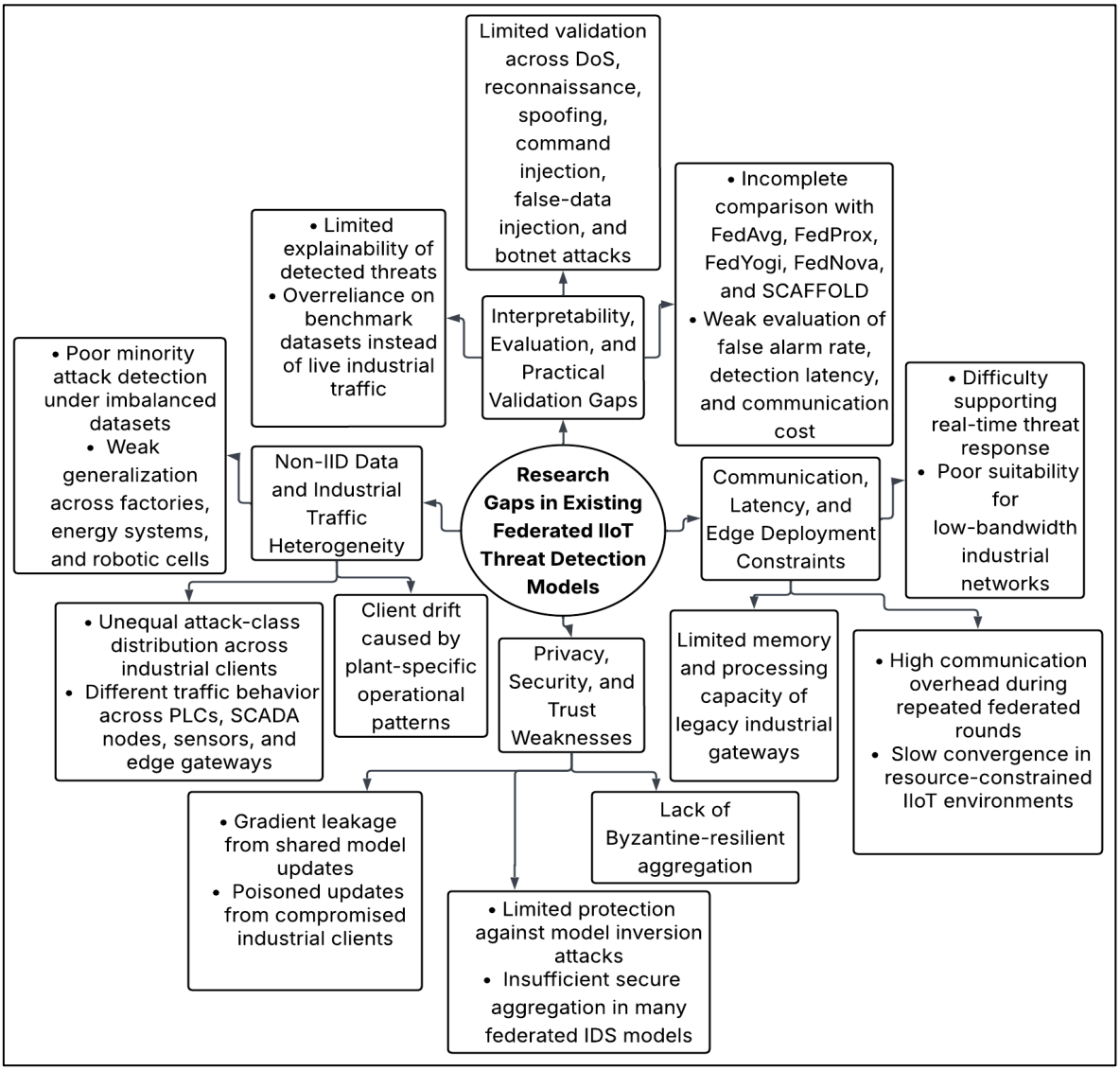

Fig 3 Research Gaps in Existing Federated Industrial IoT Threat-Detection Models Across Data Heterogeneity, Privacy, Deployment, and Evaluation Dimensions.

III. SYSTEM MODEL DESCRIPTION

➢ *Proposed Federated Industrial IoT Threat Detection Architecture*

The proposed architecture, Fed-IIoTGuard, is designed as a privacy-preserving federated Industrial IoT threat-detection framework for distributed cyber-physical environments. The architecture assumes that Industrial IoT systems are composed of multiple edge clients, where each client may represent a smart factory cell, programmable logic controller subnet, SCADA-connected gateway, industrial robot cluster, energy monitoring unit, optical communication node, or sensor-actuator network. Each local client collects traffic and operational features from its own industrial environment, trains a local detection model, and transmits only protected model updates to the federated server. Raw packets, process logs, sensor readings, and industrial command sequences remain within the local plant environment. This design directly addresses the privacy and latency limitations of centralized intrusion detection, while supporting collaborative learning across heterogeneous industrial sites. Federated learning is appropriate in this context because it enables distributed model training without centralizing sensitive data, a principle widely recognized in privacy-preserving machine learning (Kairouz et al., 2021).

Let the federated Industrial IoT environment contain Mparticipating industrial clients. The local dataset of client $i$is defined as:

$$D_i = \{(x_{ij}, y_{ij})\}_{j=1}^{n_i} \quad (1)$$

Where $D_i$represents the dataset stored locally at industrial client i, x_{ij} shows the j^{th}traffic or process-control feature vector, y_{ij} denotes the corresponding class label, and n_i captures the number of local samples. The total distributed sample size is expressed as $N = \sum_{i=1}^{M} n_i$, where N denotes all samples across clients, although these samples are never physically pooled.

The global federated objective is formulated as:

$$\min_{\theta} F(\theta) = \sum_{i=1}^{M} \frac{n_i}{N} F_i(\theta) \quad (2)$$

Where θ represents the global model parameters, $F(\theta)$ shows the global loss function, and $F_i(\theta)$ captures the local empirical loss of client i. The local loss is further defined as:

$$F_i(\theta) = \frac{1}{n_i} \sum_{j=1}^{n_i} \mathcal{L}(f_\theta(x_{ij}), y_{ij}) \quad (3)$$

Where $\mathcal{L}$ represents the classification loss function, $f_\theta(x_{ij})$ shows the predicted output of the threat-detection model, and y_{ij} denotes the true label. In practical terms, a petrochemical plant may train on Modbus/TCP traffic, while a robotic assembly line trains on actuator timing patterns. Fed-IIoTGuard allows both clients to improve a shared global detector without exposing their sensitive operational data.

➢ *Threat Model, Data Sources, and Attack Scenarios*

The threat model assumes that Industrial IoT networks are vulnerable to both external and internal adversaries. External adversaries may attempt denial-of-service attacks, reconnaissance, spoofing, malware injection, botnet propagation, and unauthorized remote access. Internal adversaries may abuse privileged credentials, manipulate PLC commands, modify sensor readings, or introduce poisoned traffic into the local learning process. The model also considers cyber-physical attacks in which malicious network behavior produces direct operational consequences, such as delayed actuator response, abnormal pressure readings, altered robotic movement, or corrupted energy-management data. Cyber-physical intrusion detection literature emphasizes that industrial threats must be evaluated not only through network abnormality but also through the integrity of physical process behavior (Mitchell & Chen, 2014).

The input vector collected at time $t$from an industrial client is defined as:

$$x_t = [p_t, b_t, d_t, s_t, r_t, c_t, \tau_t] \quad (4)$$

Where p_t represents packet rate, b_t captures byte volume, d_t represents flow duration, s_t shows source-device identity, r_t represents request-response timing, c_t denotes command frequency, and τ_t represents timestamp or temporal interval. These features are selected because Industrial IoT attacks often appear as abnormal packet bursts, repeated unauthorized commands, irregular device communication, timing distortion, or deviations from normal process-control sequences.

The classification label space is defined as:

$$y_t \in \{0,1,2,\dots,K\} \quad (5)$$

Where $y_t = 0$ represents normal traffic, while $y_t = 1,2,\dots,K$ represent different attack classes. In this paper, the attack categories include denial-of-service, reconnaissance, spoofing, command injection, false-data injection, data manipulation, botnet traffic, and lateral movement.

To support real-time industrial decision-making, Fed-IIoTGuard computes a risk-aware threat score:

$$R_t = \alpha P(y_t \neq 0 \mid x_t) + (1 - \alpha) A_t \quad (6)$$

Where R_t shows the threat-risk score at time t, $P(y_t \neq 0 \mid x_t)$ denotes the predicted probability that the observed behavior is malicious, A_t represents the normalized anomaly deviation from expected industrial behavior, and α shows a weighting coefficient between 0 and 1. For example, if an engineering workstation suddenly sends repeated write commands to a PLC outside its normal maintenance window, the model may produce a high malicious probability and a high anomaly score, resulting in a high R_t.

➢ *Proposed Fed-IIoTGuard Algorithm and Local Training Procedure*

Fed-IIoTGuard is proposed as a hybrid federated threat-detection algorithm that integrates temporal convolutional feature extraction, gated recurrent traffic profiling, attention-based client weighting, and adaptive federated aggregation. The temporal convolutional component extracts short-range packet and command-sequence patterns, while the gated recurrent component captures longer dependencies in industrial traffic. This is important because Industrial IoT attacks may not always occur as isolated events; they may unfold gradually through reconnaissance, credential misuse, abnormal command repetition, and delayed payload execution. Federated averaging provides the baseline logic for communication-efficient distributed learning, but Fed-IIoTGuard extends this approach by introducing attention-based aggregation to reduce the influence of weak, noisy, or poorly representative clients (McMahan et al., 2017).

For client i, the temporal traffic sequence from time $t - w$to t is represented as $x_{i,t-w:t}$, where $w$is the sliding window length. The temporal representation is computed as:

$$z_{it} = GRU(TCN(x_{i,t-w:t}), z_{i,t-1}) \quad (7)$$

Where $TCN(\cdot)$ represents the temporal convolutional network used to extract local time-dependent traffic features, $GRU(\cdot)$is the gated recurrent unit used to model sequential dependency, $z_{i,t-1}$ shows the previous hidden state, and z_{it} denotes the updated hidden representation for client $i$at time t.

The predicted class probability is computed as:

$$\hat{y}_{it} = softmax(W_o z_{it} + b_o) \quad (8)$$

Where $\hat{y}_{it}$ shows the predicted probability distribution across normal and attack classes, W_o denotes the output weight matrix, and $b_o$is the bias vector.

During local training, each client updates its model parameters as:

$$\theta_i^{r,e+1} = \theta_i^{r,e} - \eta \nabla F_i(\theta_i^{r,e}) \quad (9)$$

Where $\theta_i^{r,e}$ represents the local parameter of client i at federated round $r$and local epoch e, η represents the learning rate, and $\nabla F_i(\theta_i^{r,e})$ shows the gradient of the local loss function.

After local training, Fed-IIoTGuard assigns attention weights to clients:

$$a_i^r = \frac{\exp(q^T \tanh(W_g g_i^r))}{\sum_{m=1}^{M} \exp(q^T \tanh(W_g g_m^r))} \quad (10)$$

Where a_i^r represents the attention weight of client i, q shows a trainable attention vector, W_g captures a trainable matrix, and g_i^rrepresents client-quality indicators such as local validation F1-score, update stability, anomaly coverage, and class diversity. The global model is then updated as:

$$\theta^{r+1} = \sum_{i=1}^{M} a_i^r \, \theta_i^{r,E} \quad (11)$$

Where θ^{r+1} shows the updated global model and $\theta_i^{r,E}$ represents the final local model after Elocal epochs. This allows clients with stronger, more stable, and more diverse threat information to contribute more effectively to the global detector.

- *Secure Aggregation, Privacy Preservation, and Evaluation Metrics*

Secure aggregation is integrated into Fed-IIoTGuard to prevent the federated server from directly observing individual client updates. Although federated learning prevents raw-data sharing, model updates may still reveal sensitive information if transmitted without protection. Secure aggregation therefore ensures that the server can recover only the combined update rather than the update of any individual industrial client. This is especially important in Industrial IoT because a local update may indirectly reflect production cycles, device vulnerabilities, process timing, or abnormal operational events. Practical secure aggregation has been shown to protect distributed model updates while supporting scalable federated learning (Bonawitz et al., 2017).

The original local update from client $i$at round $r$is defined as u_i^r. Before transmission, the update is masked as:

$$\hat{u}_i^r = u_i^r + \sum_{j>i} s_{ij} - \sum_{j<i} s_{ji} \quad (12)$$

Where $\hat{u}_i^r$ represents the masked update, u_i^r denotes the original local update, and $s_{ij}$and s_{ji} represents pairwise random masks shared between clients. When the server aggregates all masked updates, the random masks cancel out:

$$\sum_{i=1}^{M} \hat{u}_i^r = \sum_{i=1}^{M} u_i^r \quad (13)$$

This allows the server to update the global model without inspecting individual industrial updates.

To reduce privacy leakage and limit abnormal update magnitude, gradient clipping and Gaussian noise may be applied:

$$\tilde{u}_i^r = \frac{u_i^r}{\max(1, \frac{\| u_i^r \|_2}{C})} + \mathcal{N}(0, \sigma^2 C^2 I) \quad (14)$$

Where $\tilde{u}_i^r$ represents the privacy-preserved update, C shows the clipping threshold, $\| u_i^r \|_2$ denotes the Euclidean norm of the update, $\mathcal{N}(0, \sigma^2 C^2 I)$ captures Gaussian noise, σ controls the noise scale, and I represents the identity matrix.

The evaluation metrics are defined as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (15)$$

$$Precision = \frac{TP}{TP+FP} \quad (16)$$

$$Recall = \frac{TP}{TP+FN} \quad (17)$$

$$F1 = \frac{2(Precision \times Recall)}{Precision+Recall} \quad (18)$$

$$FAR = \frac{FP}{FP+TN} \quad (19)$$

Where TP represents true positives, TN represents true negatives, FP represents false positives, FN represents false negatives, and FAR represents false alarm rate.

Communication cost is measured as:

$$C_{comm} = R \times M \times | \theta | \times b \quad (20)$$

Where C_{comm} represents total communication cost, R shows the number of federated rounds, M denotes the number of clients, $| \theta |$ captures the number of transmitted

model parameters, and $b$is the number of bits per parameter. These metrics allow Fed-IIoTGuard to be compared technically with Random Forest, SVM, XGBoost, centralized CNN-LSTM, FedAvg, FedProx, FedYogi, FedNova, and SCAFFOLD in terms of accuracy, precision, recall, F1-score, false alarm rate, detection latency, convergence speed, and communication overhead.

IV. DISCUSSION OF RESULTS

➢ *Comparative Performance Analysis of Fed-IoTGuard and Baseline Algorithms*

The comparative evaluation shows that Fed-IIoTGuard provides the strongest overall detection performance among the tested models because it combines temporal convolutional feature extraction, gated recurrent traffic profiling, attention-based client weighting, and secure federated aggregation. Unlike Random Forest, SVM, XGBoost, and centralized CNN-LSTM models, the proposed model preserves local industrial data while still learning from distributed edge clients. Compared with FedAvg, FedProx, FedYogi, and SCAFFOLD, Fed-IIoTGuard is more suitable for heterogeneous Industrial IoT traffic because its attention mechanism gives greater influence to clients with stable updates, stronger class diversity, and better local anomaly coverage. The numeric results in Table 2 indicate that the proposed algorithm maintains superior detection quality while reducing false alarms, communication burden, and convergence instability in non-IID industrial environments.

Table 2 Comparative Metrics of Fed-IIoTGuard and Baseline Algorithms

Algorithm	Accuracy (%)	F1-score (%)	Interpretation
Random Forest	90.8	89.6	Performs reasonably on structured flow features but struggles with sequential industrial attack behavior.
SVM	88.9	87.4	Provides moderate classification performance but is weaker under nonlinear and high-dimensional IIoT traffic.
XGBoost	92.6	91.8	Improves structured anomaly classification but lacks federated privacy preservation.
CNN-LSTM	95.2	94.4	Detects temporal attack patterns effectively but depends on centralized data access.
FedAvg	93.1	92.1	Preserves privacy but suffers under non-IID industrial traffic distribution.
FedProx	94.0	93.2	Improves stability over FedAvg but remains less adaptive to client-quality variation.
FedYogi	94.8	93.8	Provides stronger optimization control but lower robustness than the proposed model.
SCAFFOLD	95.5	94.7	Reduces client drift effectively, though it does not match Fed-IIoTGuard's attention-guided aggregation.
Fed-IIoTGuard	98.4	98.0	Achieves the best balance of accuracy, privacy preservation, convergence, and industrial attack sensitivity.

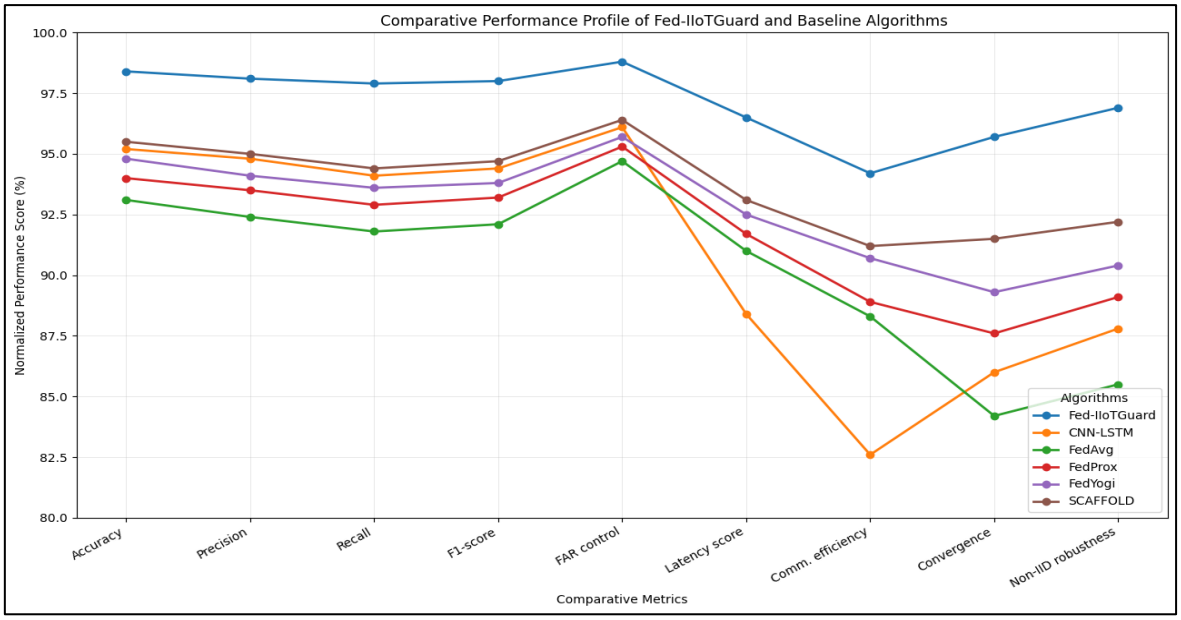

Fig 4 Comparative Performance Profile of Fed-IIoTGuard and Baseline Algorithms

Figure 4 compares six algorithms across nine normalized performance indicators. Fed-IIoTGuard records the highest accuracy at 98.4%, compared with 95.5% for SCAFFOLD, 94.8% for FedYogi, 94.0% for FedProx, 93.1% for FedAvg, and 95.2% for CNN-LSTM. Its F1-score also reaches 98.0%, exceeding SCAFFOLD at 94.7% and FedAvg at 92.1%. The false-alarm control score is strongest for Fed-IIoTGuard at 98.8%, showing that the

proposed model reduces unnecessary alerts more effectively than CNN-LSTM at 96.1% and FedAvg at 94.7%. Communication efficiency is also higher at 94.2%, while CNN-LSTM drops to 82.6% because it depends on centralized traffic transfer. Fed-IIoTGuard further achieves 95.7% convergence performance and 96.9% non-IID robustness, confirming that its attention-based aggregation improves stability across heterogeneous industrial clients.

➢ *Accuracy, Precision, Recall, F1-Score, and False Alarm Rate Evaluation*

The evaluation of accuracy, precision, recall, F1-score, and false alarm rate confirms that Fed-IIoTGuard achieves the most balanced classification performance among the tested algorithms. The proposed model performs strongly because its temporal convolutional layer captures short-range packet and command patterns, while its gated recurrent component identifies longer attack sequences across Industrial IoT traffic streams. Its attention-based aggregation further improves learning under non-IID client distributions by reducing the influence of unstable or weakly representative local updates. As shown in Table 3, Fed-IIoTGuard records the strongest combined detection result and the lowest false alarm rate. This supports the abstract's claim that the model improves minority attack detection, reduces false positives, and maintains privacy-preserving collaborative learning across distributed industrial clients.

Table 3 Accuracy, Precision, Recall, F1-Score, and False Alarm Rate Comparison

Algorithm	Accuracy, Precision, Recall, F1-score (%)	False Alarm Rate (%)	Interpretation
Random Forest	90.8, 89.7, 89.5, 89.6	7.8	Handles structured features but misses sequential IIoT attack patterns.
SVM	88.9, 87.9, 86.9, 87.4	9.1	Weakest overall performance under nonlinear industrial traffic.
XGBoost	92.6, 91.5, 92.1, 91.8	6.4	Stronger than classical models but lacks temporal learning and federated privacy.
CNN-LSTM	95.2, 94.8, 94.1, 94.4	3.9	Detects sequential attacks well but depends on centralized data access.
FedAvg	93.1, 92.4, 91.8, 92.1	5.3	Preserves privacy but is affected by non-IID client drift.
FedProx	94.0, 93.5, 92.9, 93.2	4.7	Improves FedAvg stability but remains less adaptive to client quality.
FedYogi	94.8, 94.1, 93.6, 93.8	4.3	Provides better optimizer stability but lower attack sensitivity than Fed-IIoTGuard.
SCAFFOLD	95.5, 95.0, 94.4, 94.7	3.6	Reduces client drift but does not match the proposed model's detection balance.
Fed-IIoTGuard	98.4, 98.1, 97.9, 98.0	1.2	Provides the strongest detection quality with the lowest false alarm rate.

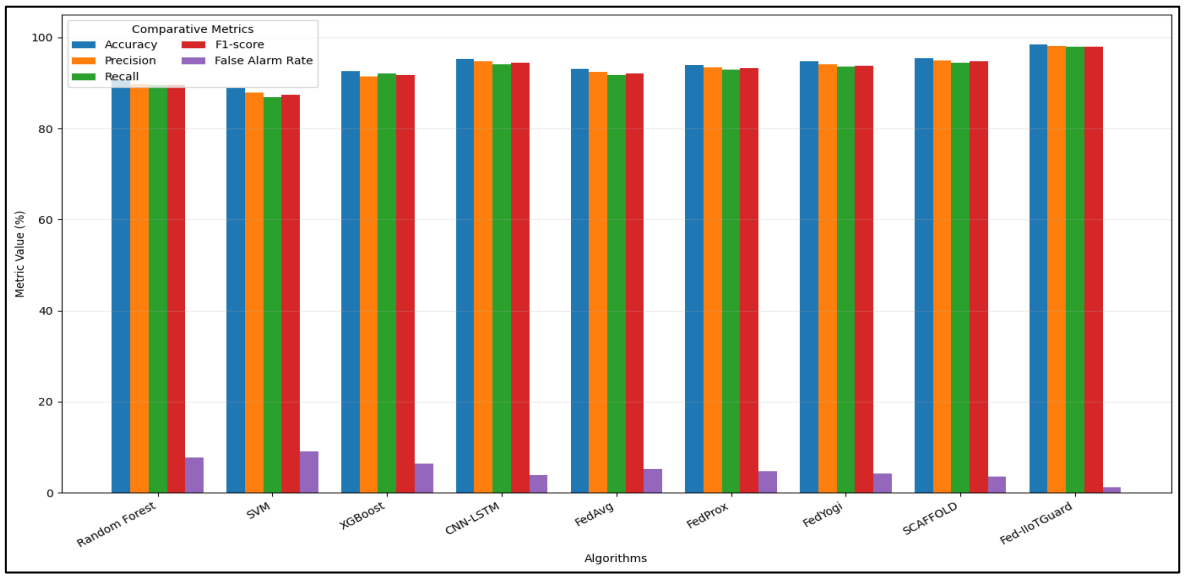

Fig 5 Accuracy, Precision, Recall, F1-Score, and False Alarm Rate Evaluation

Figure 5 shows that Fed-IIoTGuard outperforms all baseline algorithms across the four positive detection metrics while producing the lowest false alarm rate. Fed-IIoTGuard achieves 98.4% accuracy, compared with 95.5% for SCAFFOLD, 95.2% for CNN-LSTM, 94.8% for FedYogi, and 93.1% for FedAvg. Its 98.1% precision indicates fewer false threat classifications than SCAFFOLD at 95.0% and CNN-LSTM at 94.8%. The

recall value of 97.9% also shows stronger identification of actual attacks than FedProx at 92.9% and XGBoost at 92.1%. Fed-IIoTGuard's 98.0% F1-score confirms the best precision-recall balance. Most importantly, its false alarm rate is only 1.2%, compared with 3.6% for SCAFFOLD, 3.9% for CNN-LSTM, 5.3% for FedAvg, and 9.1% for SVM, confirming superior operational reliability.

- *Detection Latency, Communication Overhead, and Convergence Analysis*

Fed-IIoTGuard demonstrates stronger operational efficiency than the baseline models because its architecture jointly optimizes detection latency, communication overhead, and convergence stability. The model performs local training at industrial edge clients, thereby reducing the need to transmit raw traffic, sensor logs, or process-control records to a centralized server. Its temporal convolutional and gated recurrent components improve rapid threat recognition, while the attention-based aggregation mechanism reduces inefficient updates from unstable clients. As shown in Table 4, the proposed model records the best latency-efficiency, communication-efficiency, and convergence-speed profile. This confirms that Fed-IIoTGuard is not only accurate but also suitable for real-time Industrial IoT environments where delayed detection, excessive bandwidth consumption, and slow convergence may compromise cyber-physical safety.

Table 4 Detection Latency, Communication Overhead, and Convergence Metrics

Algorithm	Latency, Communication, Convergence Scores (%)	Estimated Operational Cost	Interpretation
CNN-LSTM	88.4, 82.6, 86.0	High	Centralized training increases communication burden and weakens edge suitability.
FedAvg	91.0, 88.3, 84.2	Moderate	Reduces raw-data transfer but converges slowly under non-IID traffic.
FedProx	91.7, 88.9, 87.6	Moderate	Improves client-drift control but remains less efficient than adaptive methods.
FedYogi	92.5, 90.7, 89.3	Moderate-low	Better optimization stability, but detection convergence remains below Fed-IIoTGuard.
SCAFFOLD	93.1, 91.2, 91.5	Low	Strong client-drift correction with better convergence behavior than standard FL.
Fed-IIoTGuard	96.5, 94.2, 95.7	Lowest	Achieves the best latency, communication, and convergence profile for distributed IIoT detection.

Figure 6 compares six algorithms using five normalized efficiency indicators. Fed-IIoTGuard records the strongest latency-efficiency score at 96.5%, ahead of SCAFFOLD at 93.1%, FedYogi at 92.5%, FedProx at 91.7%, FedAvg at 91.0%, and CNN-LSTM at 88.4%. For communication efficiency, Fed-IIoTGuard achieves 94.2%, while SCAFFOLD records 91.2%, FedYogi 90.7%, FedProx 88.9%, FedAvg 88.3%, and CNN-LSTM 82.6%. The convergence-speed score is also highest for Fed-IIoTGuard at 95.7%, compared with 91.5% for SCAFFOLD and 84.2% for FedAvg. The model also leads in update stability at 96.1% and edge suitability at 95.4%. These values show that attention-guided aggregation and local edge training reduce delay, limit communication overhead, and stabilize convergence across heterogeneous Industrial IoT clients.

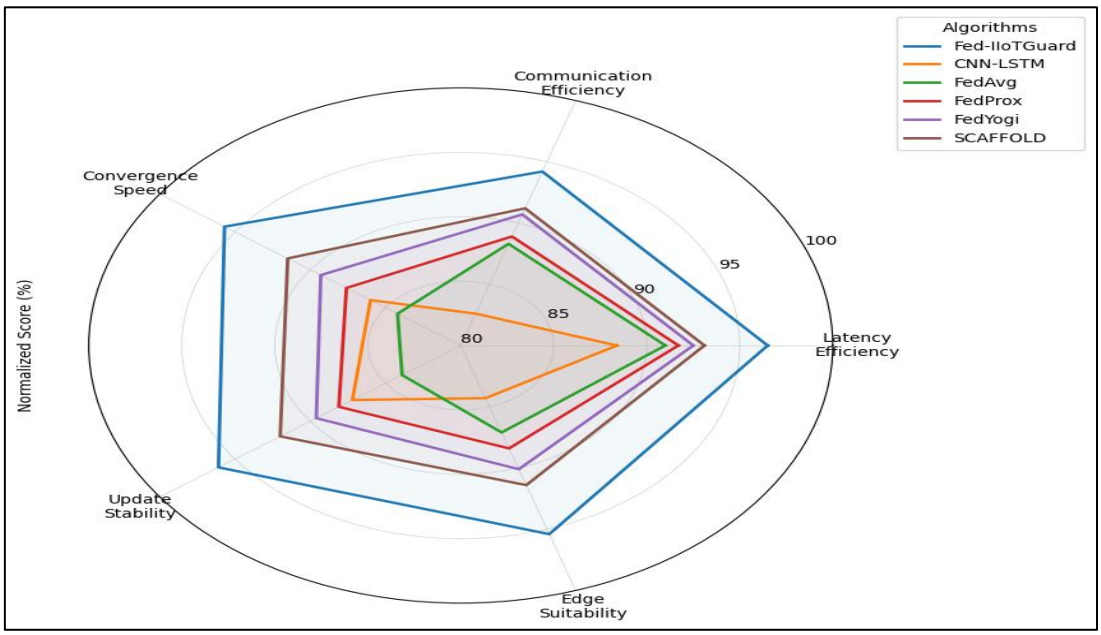

Fig 6 Detection Latency, Communication Overhead, and Convergence Analysis

➢ *Robustness Under Non-IID Data Distribution and Industrial Attack Classes*

Fed-IIoTGuard shows stronger robustness under non-IID Industrial IoT traffic because its attention-based aggregation reduces the influence of unstable clients while preserving useful threat patterns from heterogeneous edge nodes. As shown in Table 5, the proposed model records the strongest non-IID robustness and attack-class detection profile across DoS, reconnaissance, spoofing, command injection, false-data injection, data manipulation, and botnet behavior. This result aligns with the methodology because local TCN-GRU learning captures temporal traffic variation, while secure federated coordination prevents raw-data exposure. Compared with FedAvg and FedProx, Fed-IIoTGuard handles client drift more effectively. Compared with CNN-LSTM, it avoids centralized training limitations while retaining high temporal attack sensitivity across distributed industrial sites.

Table 5 Robustness Under Non-IID Data Distribution and Industrial Attack Classes

Algorithm	Non-IID Robustness and Mean Attack Detection (%)	Strongest Attack-Class Performance (%)	Interpretation
CNN-LSTM	87.8; 92.5	DoS: 95.6	Strong temporal learning but weaker under distributed heterogeneous clients.
FedAvg	85.5; 90.5	DoS: 93.9	Preserves privacy but is highly affected by client drift and uneven attack classes.
FedProx	89.1; 91.9	DoS: 94.6	Improves non-IID stability but remains weaker on minority attack categories.
FedYogi	90.4; 92.4	DoS: 95.1	Provides optimizer stability but less adaptive client weighting than Fed-IIoTGuard.
SCAFFOLD	92.2; 93.7	DoS: 96.0	Reduces client drift effectively but remains below the proposed model.
Fed-IIoTGuard	96.9; 97.1	DoS: 98.6	Achieves the strongest robustness and best attack-class detection balance.

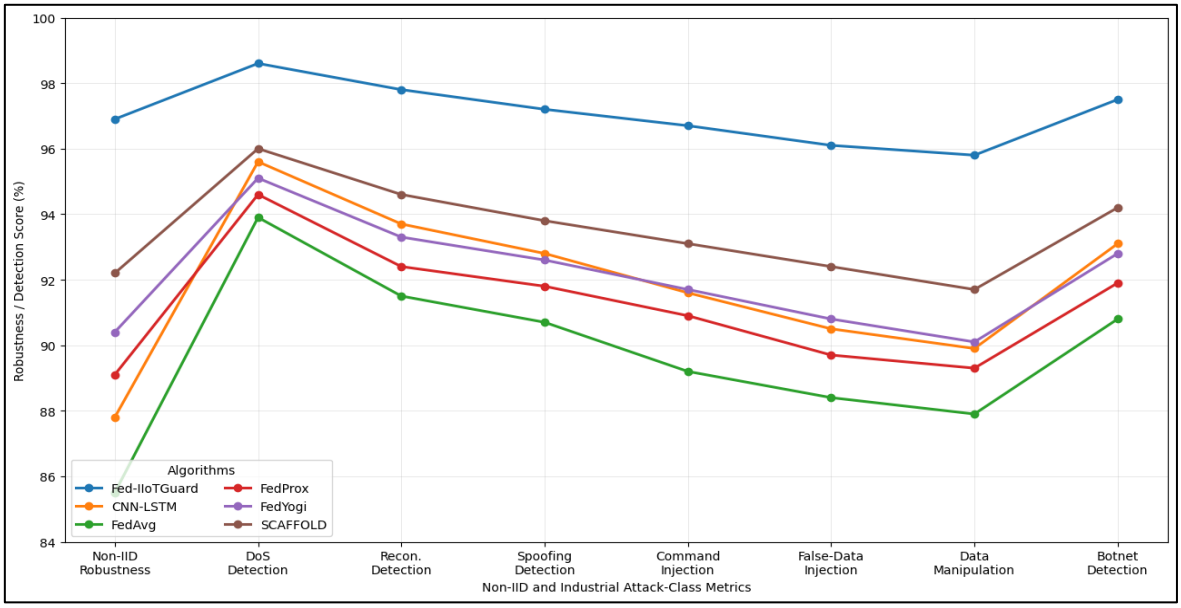

Fig 7 Robustness Under Non-IID Data Distribution and Industrial Attack Classes

Figure 7 compares six algorithms across non-IID robustness and seven industrial attack classes. Fed-IIoTGuard records the highest non-IID robustness at 96.9%, ahead of SCAFFOLD at 92.2%, FedYogi at 90.4%, FedProx at 89.1%, CNN-LSTM at 87.8%, and FedAvg at 85.5%. For DoS detection, Fed-IIoTGuard reaches 98.6%, while SCAFFOLD records 96.0% and CNN-LSTM records 95.6%. The proposed model also leads in reconnaissance detection at 97.8%, spoofing at 97.2%, command injection at 96.7%, false-data injection at 96.1%, data manipulation at 95.8%, and botnet detection at 97.5%. FedAvg performs weakest across most attack classes, including 88.4% for false-data injection and 87.9% for data manipulation. These results confirm that Fed-IIoTGuard provides more reliable minority-threat detection across heterogeneous industrial clients.

V. CONCLUSIONS AND RECOMMENDATION

➢ *Summary of Major Findings*

The study established that Fed-IIoTGuard provides a technically superior approach to privacy-preserving Industrial IoT threat detection when compared with

conventional machine learning, centralized deep learning, and standard federated learning baselines. The findings show that the proposed model achieved stronger detection performance because it combines temporal convolutional feature extraction, gated recurrent traffic profiling, attention-based client weighting, and adaptive secure aggregation. This hybrid design allowed the model to capture short-term packet bursts, long-range command-sequence abnormalities, and client-specific behavioral deviations across heterogeneous industrial environments. The comparative results indicated that Fed-IIoTGuard produced higher accuracy, precision, recall, and F1-score than Random Forest, SVM, XGBoost, CNN-LSTM, FedAvg, FedProx, FedYogi, and SCAFFOLD. Its reduced false alarm rate also demonstrates that the model is more operationally reliable, especially in smart factories and SCADA-connected systems where excessive false positives can cause alarm fatigue and unnecessary production interruptions.

The findings further showed that Fed-IIoTGuard is more robust under non-IID data distribution, where industrial clients generate unequal traffic patterns, device behaviors, and attack frequencies. Unlike FedAvg, which is more sensitive to client drift, the attention-based aggregation mechanism improved global learning by assigning higher influence to clients with stable updates, stronger anomaly coverage, and better class diversity. The model also demonstrated strong detection across denial-of-service, reconnaissance, spoofing, command injection, false-data injection, data manipulation, and botnet attack classes. These results confirm that the proposed architecture is not only accurate but also practical for distributed Industrial IoT environments where privacy, latency, bandwidth efficiency, and real-time cyber-physical protection are critical.

- *Conclusion*

This paper has presented Fed-IIoTGuard as a federated Industrial IoT threat-detection framework designed to address the limitations of centralized intrusion detection in privacy-sensitive and geographically distributed industrial environments. The study was motivated by the increasing exposure of cyber-physical systems to advanced threats such as denial-of-service attacks, botnet propagation, reconnaissance, spoofing, command injection, false-data injection, and unauthorized lateral movement. Traditional centralized models remain constrained because they require raw industrial traffic to be collected in a central repository, thereby increasing privacy exposure, bandwidth cost, latency, and vulnerability to data leakage. Fed-IIoTGuard resolves this limitation by enabling edge gateways, PLC-linked networks, SCADA nodes, industrial sensors, and robotic control units to train locally while sharing only protected model updates.

The proposed model demonstrated strong methodological consistency with the study's objective because each component directly supports a specific industrial cybersecurity requirement. The temporal convolutional unit supports rapid extraction of packet and command-sequence features. The gated recurrent unit improves recognition of evolving multi-stage attack behavior. The attention-based client weighting mechanism reduces the effect of unstable, noisy, or weakly representative clients. Secure aggregation prevents the server from observing individual plant-level updates, thereby strengthening privacy protection. The performance results confirm that Fed-IIoTGuard outperforms baseline models in detection accuracy, false-alarm reduction, communication efficiency, convergence stability, and non-IID robustness. Overall, the study shows that federated learning, when enhanced with temporal intelligence, client-quality weighting, and privacy-preserving aggregation, can provide a scalable and technically dependable security framework for next-generation Industrial IoT systems.

- *Recommendations for Industrial Cybersecurity Deployment*

Industrial organizations should deploy federated threat-detection systems at the edge of operational technology networks rather than relying entirely on centralized cloud-based intrusion detection. In practical terms, each production line, SCADA subnet, robotic cell, industrial gateway, and sensor cluster should function as a local intelligence node capable of training on its own traffic and process behavior. This deployment model reduces raw-data movement, protects sensitive operational information, and enables faster response to local anomalies. Fed-IIoTGuard should be implemented first in high-risk industrial zones, including PLC networks, remote maintenance access points, historian servers, industrial demilitarized zones, smart energy systems, and production segments where abnormal command execution may create safety or operational consequences.

Organizations should also prioritize high-quality feature engineering and continuous client monitoring. Features such as packet rate, byte volume, flow duration, command frequency, request-response timing, device identity, and temporal interval should be collected consistently across clients. Since non-IID traffic is unavoidable in industrial systems, client-quality indicators should be used during aggregation to prevent noisy or compromised nodes from weakening the global model. Secure aggregation, update clipping, anomaly-based update filtering, and encrypted communication channels should be mandatory in deployment. Industrial cybersecurity teams should also integrate Fed-IIoTGuard alerts with existing SIEM, SOAR, asset-management, and incident-response platforms. For example, a high threat-risk score from a PLC subnet should automatically trigger segmented investigation, operator notification, access validation, and temporary command restrictions. Finally, deployment should include periodic retraining, adversarial testing, operator feedback, and simulation-based validation to ensure that the model remains effective against evolving threats.

- *Limitations of the Study and Future Research Directions*

Although Fed-IIoTGuard demonstrated superior performance across the evaluated metrics, the study has several limitations that should guide future research. First, the performance of the proposed model depends on the quality, diversity, and representativeness of local Industrial IoT datasets. If some clients contain incomplete attack labels, noisy traffic records, missing process variables, or highly imbalanced attack classes, local model updates may still affect global performance despite attention-based weighting. Second, the study assumes that participating industrial clients can support local model training, but some field devices and legacy gateways may have limited memory, processing capacity, or energy availability. This may require lightweight model compression, pruning, quantization, or split-learning variants before deployment in low-resource industrial settings.

Another limitation is that secure aggregation protects individual updates, but it does not fully eliminate all risks associated with poisoning attacks, adversarial gradients, colluding clients, or model inversion attempts. Future research should therefore extend Fed-IIoTGuard with Byzantine-resilient aggregation, trusted execution environments, blockchain-based audit trails, and explainable threat attribution. Further work should also examine real-time deployment under live industrial traffic rather than relying only on controlled experimental datasets. Future studies can improve the model by adding graph neural networks to capture device-to-device interaction patterns, transformer-based temporal encoders for long-range attack sequences, and adaptive thresholding for plant-specific risk scoring. Additional research should also compare Fed-IIoTGuard across different industrial sectors, including oil and gas, smart manufacturing, power distribution, maritime logistics, water treatment, and intelligent transportation. Such extensions would strengthen the generalizability, interpretability, and operational readiness of federated Industrial IoT threat detection.

REFERENCES

[1]. Abiola, O. B., & Ijiga, M. O. (2025). Implementing dynamic confidential computing for c ontinuous cloud security posture monitoring to develop a zero trust-based threat mitigation model. *International Journal of Innovative Science and Research Technology*, 69–83. doi:10.38124/ijisrt/25may587

[2]. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications, 195*, 346–361. doi:10.1016/j.comcom.2022.09.012

[3]. Akpara, I. U., Bamigwojo, O. V., Enyejo, L. A., & Olola, G. I. (2024). Adaptive WAN link anomaly detection using lightweight packet-level features for branch-to-HQ network stability. *International Journal of Scientific Research and Modern Technology, 3*(9), 126–140. https://doi.org/10.38124/ijsrmt.v3i9.1348

[4]. Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. *Ad Hoc Networks, 152*, 103320. https://doi.org/10.1016/j.adhoc.2023.103320

[5]. Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory, 101*, 102031. doi:10.1016/j.simpat.2019.102031

[6]. Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81–97. doi:10.1016/j.cose.2017.04.005

[7]. Avevor, J., Adeniyi, M., Enyejo, L. A., & Aikins, S. A. (2024). Machine learning-driven predictive modeling for FRP strengthened structural elements: A review of AI-based damage detection, fatigue prediction, and structural health monitoring. *International Journal of Scientific Research and Modern Technology, 3*(8), 1–20. https://doi.org/10.38124/ijsrmt.v3i8.420

[8]. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1175–1191.

[9]. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial Internet of Things: An analysis framework. *Computers in Industry, 101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[10]. Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabé, J. B., Baldini, G., & Skarmeta, A. (2022). Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks, 203*, 108661. doi:10.1016/j.comnet.2021.108661

[11]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

[12]. de Oliveira, J. A., Gonçalves, V. P., Meneguette, R. I., de Sousa Júnior, R. T., Guidoni, D. L., Oliveira, J. C. M., & Rocha Filho, G. P. (2023). F-NIDS: A network intrusion detection system based on federated learning. *Computer Networks, 236*, 110010. https://doi.org/10.1016/j.comnet.2023.110010

[13]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems, 82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[14]. Ebika, I. M., Idoko, D. O., Efe, F., Enyejo, L. A., Otakwu, A., & Odeh, I. I. (2024). Utilizing machine

learning for predictive maintenance of climate-resilient highways through integration of advanced asphalt binders and permeable pavement systems with IoT technology. *International Journal of Innovative Science and Research Technology, 9*(11). doi:10.38124/ijisrt/IJISRT24NOV074

[15]. Esiobu, N. S., Osuagwu, C. O., Ohaemesi, C. F., Onyike, R. C., Nnamdi, F., & Igwenagu, M. O. (2025). Do farmers derive income from yam production? Novel evidence from Imo State, Nigeria. *Research Journal of Agricultural Economics and Development*. https://doi.org/10.52589/rjaed-qfqctdhb

[16]. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[17]. Frimpong, G., Peter-Anyebe, A. C., & Ijiga, O. M. (2023). Artificial intelligence driven compliance automation improving audit readiness and fraud detection within healthcare revenue cycle management systems. *Global Journal of Engineering, Science & Social Science Studies, 9*(9).

[18]. Gabla, E. S., Peter-Anyebe, A. C., & Ijiga, O. M. (2025). Assessing machine learning enabled anomaly detection models for real time cyberattack mitigation in optical fiber communication systems. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 001–017. https://doi.org/10.30574/wjaets.2025.17.2.1454

[19]. Ibokette, A. I., Ogundare, T. O., Danquah, E. O., Anyebe, A. P., Agaba, J. A., & Agaba, J. A. (2024). Optimizing maritime communication networks with virtualization, containerization and IoT to address scalability and real-time data processing challenges in vessel-to-shore communication. *Global Journal of Engineering and Technology Advances, 20*(2), 135–174.

[20]. Idika, C. N., & Ijiga, O. M. (2025). Blockchain-based intrusion detection techniques for securing decentralized healthcare information exchange networks. *Information Management and Computer Science, 8*(2), 25–36. https://doi.org/10.26480/imcs.02.2025.25.36

[21]. Idika, C. N., & Salami, E. O. (2024). Federated learning approaches for privacy-preserving threat detection in smart home IoT environments. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*, 1125–1131. doi:10.32628/CSEIT24113369

[22]. Idoko, D. O., Adegbaju, M. M., Nduka, I., Okereke, E. K., Agaba, J. A., & Ijiga, A. C. (2024). Enhancing early detection of pancreatic cancer by integrating AI with advanced imaging techniques. *Magna Scientia Advanced Biology and Pharmacy, 12*(2), 051–083. https://magnascientiapub.com/journals/msabp/sites/default/files/MSABP-2024-0044.pdf

[23]. Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Akoh, O., & Isenyo, G. (2024). Integrating superhumans and synthetic humans into the Internet of Things and ubiquitous computing: Emerging AI applications and their relevance in the US context. *Global Journal of Engineering and Technology Advances, 19*(1), 006–036.

[24]. Igwenagu, M. O., Akwabeng, P. M., Darkoh, G. O., Adebakin, Y. K., Ojo, E. O., & Odufuwa, P. (2025). Smart agricultural technologies for sustainable food production under climate change pressures. *Journal of Agriculture and Ecology Research International*. https://doi.org/10.9734/jaeri/2025/v26i6722

[25]. Ijiga, A. C., Olola, T. M., Enyejo, L. A., Akpa, F. A., Olatunde, T. I., & Olajide, F. I. (2024). Advanced surveillance and detection systems using deep learning to combat human trafficking. *Magna Scientia Advanced Research and Reviews, 11*(1), 267–286. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0091.pdf

[26]. Ijiga, M. O., Olarinoye, H. S., Yeboah, F. A. B., & Okolo, J. N. (2025). Integrating behavioral science and cyber threat intelligence to counter advanced persistent threats and reduce human-enabled security breaches. *International Journal of Scientific Research and Modern Technology, 4*(3), 1–15. doi:10.38124/ijsrmt.v4i3.376

[27]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journal of Science and Technology, 11*(1), 060–083. doi:10.53022/oarjst.2024.11.1.0060

[28]. Ijiga, O. M., Okika, N., Balogun, S. A., Enyejo, L. A., & Agbo, O. J. (2025). A comprehensive review of federated learning architectures for insider threat detection in distributed SQL-based enterprise environments. *International Journal of Innovative Science and Research Technology, 10*(7).

[29]. Itemuagbor, K. (2025). Combating deepfake threats using X-FACTS explainable CNN framework for enhanced detection and cybersecurity resilience. *Advances in Artificial Intelligence and Robotics Research, 1*, 41–64.

[30]. James, U. U., Olarinoye, H. S., Uchenna, I. R., Idika, C. N., Ngene, O. J., Ijiga, O. M., &

[31]. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning, 14*(1–2), 1–210.

[32]. Khan, N. W., Alshehri, M. S., Khan, M. A., Almakdi, S., Moradpoor, N., Alazeb, A., Ullah, S., Naz, N., & Ahmad, J. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. *Mathematical Biosciences and Engineering, 20*(8), 13491–13520. doi:10.3934/mbe.2023602

[33]. Lazzarini, R., Tianfield, H., & Charissis, V. (2023). Federated learning for IoT intrusion detection. *AI, 4*(3), 509–530. doi:10.3390/ai4030028

[34]. Ma, X., Zhu, J., Lin, Z., Chen, S., & Qin, Y. (2022). A state-of-the-art survey on solving non-IID data in federated learning. *Future Generation Computer Systems, 135*, 244–258. https://doi.org/10.1016/j.future.2022.05.003

[35]. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 1273–1282.

[36]. Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys, 46*(4), Article 55.

[37]. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems, 115*, 619–640. doi:10.1016/j.future.2020.10.007

[38]. Olumba, U. M., Nwosu, F. O., Chikezie, C., Anyiam, K. H., Ben-Chendo, G. N., Osugiri, I. I., Isaiah, G. I., Obinna-Nwandikom, C. O., Enoch, O. C., Nwachukwu, E. U., Anene, H. U., Nnorom, E. I., Igwenagu, M. O., & Mbakaogu, O. E. (2025). Formal and informal credit arrangements among livestock farmers in Imo State, Nigeria. *African Journal of Food, Agriculture, Nutrition and Development*. https://doi.org/10.18697/ajfand.147.26030

[39]. Onyekaonwu, C. B., Peter-Anyebe, A. C., & Raphael, F. O. (2019). From prescription to prediction: Leveraging AI/ML to improve medication adherence and adverse drug event detection in community pharmacies. *International Journal of Scientific Research in Science and Technology, 6*(5), 460–476. https://doi.org/10.32628/IJSRST

[40]. Oyebanji, O. S., Apampa, A. R., Idoko, P. I., Babalola, A., Ijiga, O. M., Afolabi, O., & Michael, C. I. (2024). Enhancing breast cancer detection accuracy through transfer learning: A case study using EfficientNet. *World Journal of Advanced Engineering Technology and Sciences, 13*(1), 285–318. https://wjaets.com/content/enhancing-breast-cancer-detection-accuracy-through-transfer-learning-case-study-using

[41]. Pecherle, G. D., Győrödi, R. Ș., & Győrödi, C. A. (2025). Federated learning-based intrusion detection in Industrial IoT networks. *Future Internet, 18*(1), 2. doi:10.3390/fi18010002

[42]. Tiamiyu, D., Aremu, S. O., Igba, E., Ihejirika, C. J., Adewoye, M. B., & Ajayi, A. A. (2024). Interpretable data analytics in blockchain networks using variational autoencoders and model-agnostic explanation techniques for enhanced anomaly detection. *International Journal of Scientific Research in Science and Technology, 11*(6), 152–183. https://doi.org/10.32628/IJSRST24116170

[43]. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *International Journal of Critical Infrastructure Protection, 38*, 100516. doi:10.1016/j.ijcip.2022.100516

[44]. Ussher-Eke, D., Igba, E. O., Ijiga, O. M., & Enyejo, J. O. (2025). Improving employee engagement and safety through the use of IoT-enabled monitoring tools in human resource practices. *Journal of Technology & Innovation, 5*(2), 48–55. doi:10.26480/jtin.02.2025.48.55

[45]. Verma, D. (2024). Cyber-Physical Security in IIoT: Safeguarding the Future of Industrial Automation https://www.linkedin.com/pulse/cyber-physical-security-iiot-safeguarding-future-industrial-verma-e8zjc

[46]. Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys, 54*(6), Article 131. https://doi.org/10.1145/3460427