Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

AI-Driven Security Frameworks for IoT Devices in 5G Edge Environments: A Survey

Research Article **https://stem.techspherejournal.com**

Article Info
Received: June 21, 2025
Revised: July 26, 2025
Accepted: August 25, 2025

Keywords
IoT Security
5G Edge Computing
Artificial Intelligence
Intrusion Detection
Federated Learning

Author Details
Akinsiku Ayokunle Michael[1]*, Akin-Olayemi Titilope Helen[2], Idris-Tajudeen Rashidat[3]
1, 2, 3 Computer Science Department, Federal Polytechnic Ado-Ekiti, Ekiti State.

**Corresponding author's email*: akinsiku_am@fedpolyado.edu.ng
DOI: **https://doi.org/10.5281/zenodo.16972423**

ABSTRACT

The convergence of the Internet of Things (IoT), fifth-generation (5G) networks, and edge computing is revolutionising connectivity, enabling massive device integration, ultra-low latency, and real-time applications. However, this paradigm shift introduces an expanded attack surface, exposing IoT ecosystems to diverse and sophisticated cyber threats across device, network, and edge levels. Traditional security mechanisms are often inadequate due to scalability constraints, resource limitations, and the need for adaptive responses in dynamic environments. Artificial Intelligence (AI), encompassing machine learning (ML), deep learning (DL), reinforcement learning, and federated learning, offers promising solutions by enabling intelligent, adaptive, and decentralised defence mechanisms. This survey provides a comprehensive analysis of AI-driven security frameworks for IoT in 5G edge environments. We develop a taxonomy of AI-enabled approaches, including intrusion detection and prevention, malware and botnet detection, privacy-preserving learning, intelligent access control, and blockchain-AI hybrid models. A comparative analysis of recent frameworks (2021–2025) highlights their AI techniques, threat target, datasets, latency suitability, key metrics reported and scalability notes, while underscoring the gaps in scalability, real-time detection, and privacy assurance. Furthermore, we discuss benchmark datasets, emerging evaluation metrics, and identify pressing research challenges such as lightweight AI models, explainable AI, and quantum-era security considerations. Finally, the paper envisions the future of adaptive, self-healing IoT security in 6G and beyond, emphasising the integration of blockchain, neuromorphic computing, and edge AI.

1 Introduction

The rapid proliferation of the Internet of Things (IoT) has transformed how devices, services, and infrastructures interact in modern society [1], [2]. Billions of heterogeneous devices, including sensors, actuators, wearables, smart appliances, and industrial systems, are now interconnected, generating massive volumes of data in real time. To support this data-intensive ecosystem, 5G networks have emerged as a critical enabler, offering ultra-low latency, high bandwidth, and massive machine-type communications (mMTC) [3]. Complementing this connectivity is edge computing, which shifts computational and storage resources closer to end devices, thereby reducing response times and alleviating the reliance on centralized cloud infrastructures. The convergence of IoT, edge computing, and 5G is laying the foundation for next-generation applications such as smart cities, autonomous vehicles, telemedicine, and industrial automation [4].

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

However, this convergence also expands the attack surface of IoT ecosystems. The sheer scale of IoT device deployments, coupled with their resource-constrained nature and diverse communication protocols, creates vulnerabilities across multiple layers, device, network, and application. Attackers exploit these weaknesses to launch Distributed Denial-of-Service (DDoS) attacks, inject malware, manipulate edge nodes, and compromise data privacy [5]. The decentralized architecture of edge-enabled 5G IoT networks further complicates security management, as traditional centralized defense mechanisms struggle to meet the stringent requirements of scalability, latency, and reliability [6]. Consequently, ensuring robust, adaptive, and intelligent security mechanisms is paramount for safeguarding IoT deployments in 5G-enabled edge environments.

One promising solution lies in the application of Artificial Intelligence (AI) techniques, particularly Machine Learning (ML), Deep Learning (DL), and Federated Learning (FL) [1], [2], [7]. Unlike static rule-based methods, AI-driven approaches can learn patterns from massive IoT traffic data, detect novel attacks, and adapt to evolving threat landscapes in real time. For instance, ML and DL models have been effectively applied to intrusion detection, malware classification, and anomaly detection, while FL enables collaborative model training across distributed edge devices without compromising user privacy [2], [8]. These capabilities make AI an attractive paradigm for building dynamic and autonomous security frameworks suited for the unique characteristics of IoT in 5G edge ecosystems.

This survey makes the following contributions:

i. It presents a comprehensive overview of the convergence between IoT, 5G, and edge computing, highlighting the unique security challenges that arise in this context.
ii. It develops a taxonomy of AI-driven security frameworks, categorizing them based on target threats, AI techniques employed, and deployment architecture.
iii. It conducts a comparative analysis of state-of-the-art AI-based frameworks, focusing on their performance, scalability, and applicability to real-world IoT use cases.
iv. It discusses evaluation metrics and benchmark datasets commonly used in this domain, identifying limitations and opportunities for improvement.
v. It identifies open challenges and future research directions, including lightweight AI models for constrained devices, explainable AI for transparent decision-making, and integration of blockchain for trust management.

The remainder of this paper is structured as follows: Section 2 provides background on IoT, 5G, and edge computing, alongside AI techniques relevant to security. Section 3 outlines the major security threats and challenges in 5G-enabled IoT systems. Section 4 introduces the proposed taxonomy of AI-driven security frameworks. Section 5 reviews and compares state-of-the-art frameworks, while Section 6 discusses evaluation metrics and benchmark datasets. Section 7 highlights open research challenges and potential directions, and Section 8 provides a forward-looking outlook. Finally, Section 9 concludes the survey.

2 Background and Fundamentals

2.1 Internet of Things (IoT) Ecosystem

The Internet of Things (IoT) refers to the interconnection of physical devices, sensors, actuators, and embedded systems that exchange data over the Internet to enable intelligent decision-making [9]. A typical IoT ecosystem is structured into three main layers:

a. **Perception Layer:** This is the physical sensing layer that collects data from the environment using sensors, Radio-Frequency Identification (RFID), cameras, and actuators. It is responsible for object identification, data acquisition, and interaction with the physical world [10].

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

b. **Network Layer:** This layer ensures the reliable transmission of collected data through various communication technologies such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and, more recently, 5G. It connects devices to edge nodes, gateways, or cloud servers [11].
c. **Application Layer:** This layer provides user-oriented services and applications across domains like healthcare, transportation, smart cities, and industrial automation. It translates IoT data into actionable insights for end-users [12].

Despite its transformative potential, IoT faces significant security vulnerabilities:

a. Device-level vulnerabilities: IoT devices are often resource-constrained, making them difficult to secure with strong encryption or authentication mechanisms. Attackers exploit this through malware injection, firmware **manipulation, and physical tampering.**
b. **Network-level vulnerabilities:** IoT data in transit can be intercepted, altered, or jammed. Attacks such as Man-in-the-Middle (MitM), Distributed Denial-of-Service (DDoS), and routing manipulation threaten communication reliability [13].
c. **Application-level vulnerabilities:** Weak access control, insecure APIs, and poor software design can expose sensitive user data, enabling unauthorized access or data leakage.

2.2 5G and Edge Computing Integration

The 5th Generation (5G) of mobile communication networks introduces significant advancements over previous generations, making it an ideal enabler for large-scale IoT deployments [14]. Its core features include:

a. Ultra-Low Latency: End-to-end latency in the range of 1 ms, crucial for real-time applications such as autonomous driving and remote surgery.
b. Massive Device Connectivity: Support for billions of IoT devices in dense networks through massive Machine-Type Communication (mMTC) [15].
c. High Bandwidth and Speed: Data rates up to 10 Gbps, enabling high-throughput applications such as video analytics and augmented reality in IoT systems.

To complement 5G, edge computing pushes computational resources closer to IoT devices, reducing dependency on centralized cloud servers. This decentralization improves responsiveness, minimizes bandwidth consumption, and enhances privacy by processing sensitive data locally. For example, real-time video surveillance in smart cities can be analyzed at the edge to detect anomalies before transmitting aggregated results to the cloud.

While 5G and edge computing improve IoT efficiency, they also introduce new security implications:

a. Expanded attack surface: Edge nodes become new points of vulnerability, susceptible to data tampering, poisoning, and denial-of-service attacks.
b. Heterogeneity in security: Diverse devices, protocols, and service providers create inconsistencies in implementing security policies.
c. Distributed trust management: Unlike cloud-centric models, edge-centric systems require distributed authentication, identity management, and intrusion detection mechanisms that can operate in near real time.

2.3 Artificial Intelligence in Security

Traditional static security mechanisms are insufficient to protect the dynamic and complex nature of 5G-enabled IoT networks. Artificial Intelligence (AI) provides adaptive, data-driven approaches to detect, predict, and mitigate security threats in real time [16].

i. **Machine Learning (ML):** Supervised and unsupervised ML algorithms are widely used in intrusion detection, anomaly detection, and traffic classification. For example, Support Vector Machines (SVM) and k-Nearest Neighbors (k-NN) can classify malicious versus benign traffic [17].

ii. **Deep Learning (DL):** [18], such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), learn complex traffic patterns and outperform traditional ML in detecting sophisticated cyberattacks like botnets or zero-day exploits.

iii. **Reinforcement Learning (RL):** RL agents can dynamically adapt security policies (e.g., intrusion prevention, routing decisions) by learning from interactions with the environment. This is particularly relevant for resource allocation in edge networks [19].

iv. **Federated Learning (FL):** FL enables collaborative training of security models across distributed IoT and edge devices without transferring raw data, thereby preserving privacy while improving the robustness of AI models against localized attacks [1], [20].

Applications of AI in IoT security include:

a. Anomaly Detection: Identifying unusual patterns in IoT traffic that may indicate intrusions, malware propagation, or sensor manipulation.
b. Intrusion Detection Systems (IDS): Leveraging ML/DL to detect both known and unknown attacks in real time [21], [22].
c. Malware and Botnet Detection: Using neural networks to identify malicious code and botnet behaviors in IoT devices with high accuracy.

By leveraging AI, IoT security in 5G edge environments can move toward proactive, intelligent, and self-healing systems, capable of countering rapidly evolving threats with minimal human intervention.

3 Security Threats and Challenges in IoT with 5G Edge

The integration of IoT, 5G, and edge computing introduces a highly dynamic and interconnected ecosystem that supports real-time applications across domains such as healthcare, transportation, and industrial automation [23]. However, this convergence also amplifies the attack surface, exposing IoT systems to a wide range of security threats at different architectural layers. This section categorizes the threats into device-level, network-level, and edge-level vulnerabilities, and further discusses the unique challenges that arise in securing such systems.

3.1 Blockchain Architecture

IoT devices are often lightweight, low-cost, and resource-constrained, which makes them attractive targets for attackers.

a. **Spoofing Attacks:** Attackers can impersonate legitimate IoT devices to gain unauthorized access, inject false data, or disrupt normal operations [24]. For example, a spoofed medical sensor could transmit fabricated readings, leading to incorrect clinical decisions.
b. **Side-Channel Attacks:** Adversaries exploit physical leakages such as power consumption, electromagnetic emissions, or timing information to extract cryptographic keys or sensitive information from IoT devices [25].
c. **Malware Infections:** IoT devices, especially those with weak update mechanisms, can be compromised with malware or ransomware. The infamous Mirai botnet demonstrated how insecure IoT devices could be hijacked to launch massive DDoS attacks [26].

3.2 Security Features

Given their reliance on 5G connectivity and heterogeneous communication protocols, IoT networks face several threats during data transmission.

a. **Distributed Denial-of-Service (DDoS) Attacks:** Attacker's flood IoT networks with malicious traffic, exhausting bandwidth and computational resources, thereby disrupting legitimate services [27].
b. **Jamming Attacks:** Wireless channels used by IoT devices can be deliberately jammed, causing communication failures in critical applications such as autonomous vehicles or industrial robotics [4].

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

c. **Eavesdropping and Man-in-the-Middle (MitM) Attacks:** Adversaries intercept communication between devices and edge nodes to steal sensitive data, manipulate commands, or inject malicious payloads. In 5G IoT, the vast number of connections increases opportunities for such intrusions [26].

3.3 Edge-Level Threats

The decentralization of computation in edge computing introduces vulnerabilities unique to edge servers and gateways.

i. **Data Poisoning Attacks:** Attackers inject malicious or misleading data into training datasets used by AI-driven security frameworks at the edge. This can degrade detection accuracy or cause models to misclassify attacks as benign [28].
ii. **Privacy Leakage:** Sensitive user or device data processed at the edge can be exposed if storage or computation is inadequately secured. This is particularly critical in applications such as telemedicine or smart home systems.
iii. **Data Tampering:** Compromised edge nodes can alter or manipulate IoT data before forwarding it to cloud servers or decision-making applications, leading to incorrect outcomes in real-time systems.

3.4 Unique Security Challenges in 5G-Enabled Edge IoT Systems

Beyond individual threats, the convergence of IoT, 5G, and edge computing presents systemic challenges that complicate security solutions:

i. **Scalability:** With billions of IoT devices expected to connect to 5G networks, traditional security mechanisms struggle to scale while maintaining performance. Security frameworks must handle massive volumes of heterogeneous data in real time.
ii. **Heterogeneity:** IoT ecosystems involve diverse devices, protocols, and vendors, making it difficult to establish unified security policies and standards across the network.
iii. **Real-Time Detection:** Mission-critical applications such as autonomous driving or industrial automation require sub-second threat detection and mitigation. Security mechanisms must operate at line speed without introducing latency.
iv. **Resource Constraints:** Many IoT devices have limited computational power, memory, and energy resources, restricting the deployment of resource-intensive cryptographic or AI-based solutions. Lightweight yet effective approaches are necessary.

The integration of IoT, 5G, and edge computing enhances connectivity and performance but also introduces multi-layered threats and systemic challenges. Addressing these vulnerabilities requires adaptive, intelligent, and decentralized security solutions that can evolve alongside the rapidly growing IoT ecosystem.
A visual taxonomy diagram illustrating security threats and challenges in IoT with 5G Edge across device, network, edge, and systemic levels is presented in Figure 1.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

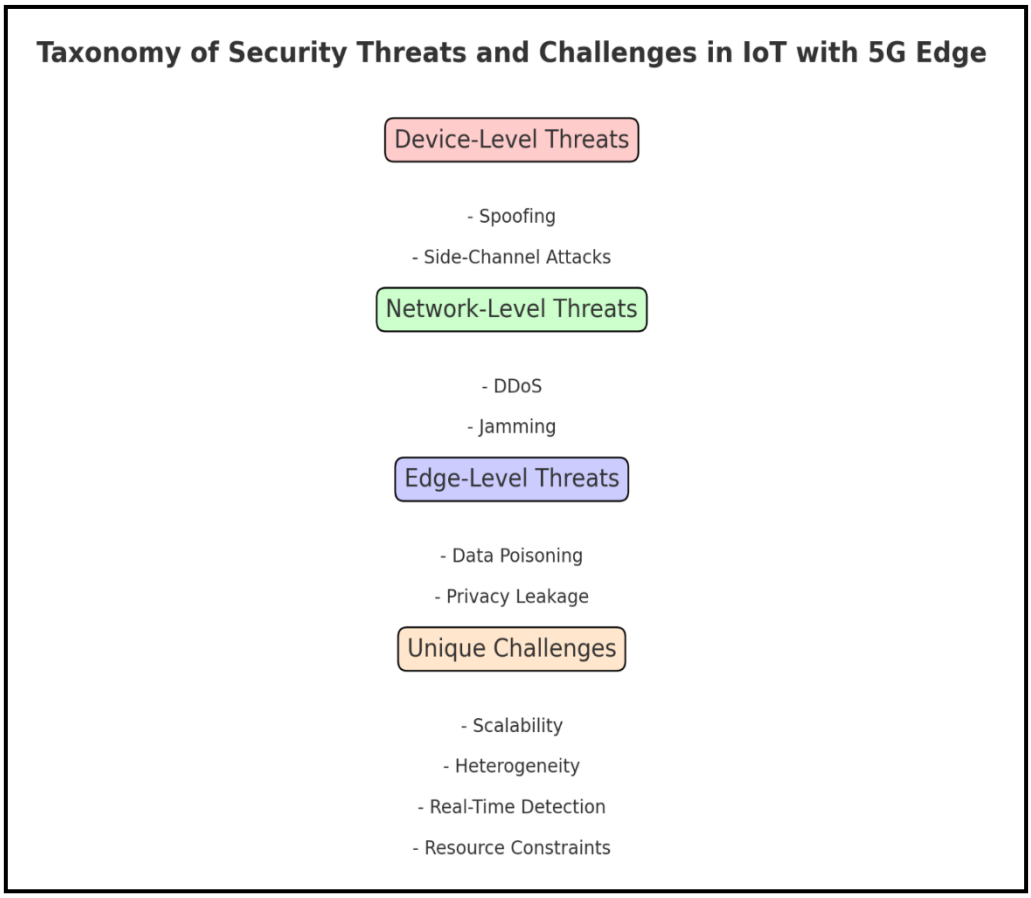

Figure 1: Taxonomy of security Threats and Challenges in IOT 5G Edge

4 AI-Driven Security Frameworks: A Taxonomy

The convergence of IoT, edge computing, and 5G necessitates a new paradigm of adaptive security. Traditional rule-based approaches often fail to address the dynamic and heterogeneous nature of IoT ecosystems, particularly under the constraints of ultra-low latency and massive device connectivity introduced by 5G. Artificial Intelligence (AI), through techniques such as machine learning (ML), deep learning (DL), reinforcement learning (RL), and federated learning (FL), provides the ability to detect, predict, and mitigate threats in real time [2], [5], [20]. This section presents a taxonomy of AI-driven security frameworks for IoT devices operating in 5G edge environments, categorizing them into five major areas: intrusion detection and prevention, malware and botnet detection, privacy-preserving AI, intelligent access control and authentication, and blockchain–AI hybrid systems.

4.1 Intrusion Detection and Prevention Systems (IDS/IPS) using AI

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) have evolved significantly with the integration of AI. In the IoT and 5G edge ecosystem, massive volumes of heterogeneous traffic make anomaly detection highly challenging [1], [20]. AI models trained on network traffic features enable systems to differentiate between benign and malicious activities with high accuracy. Machine learning approaches such as support vector machines, random forests, and ensemble methods have been widely adopted, while deep learning techniques, including recurrent neural networks (RNNs) and convolutional neural networks (CNNs), allow the extraction of temporal and spatial features from traffic

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

streams. Reinforcement learning has also been explored to develop adaptive IDS/IPS that can dynamically respond to evolving attack patterns.

4.2 Malware and Botnet Detection with ML/DL

IoT devices are particularly vulnerable to malware and botnet infections, often exploited in large-scale distributed denial-of-service (DDoS) attacks. AI-driven malware detection focuses on analyzing device behaviors, traffic patterns, and binary executables to identify anomalies [29], [30]. Deep learning methods, particularly autoencoders and graph neural networks (GNNs), have been applied to detect abnormal device-to-device communications indicative of botnet activities. Furthermore, hybrid detection approaches, combining static and dynamic malware analysis with AI models, have demonstrated effectiveness in real-time detection of evolving threats. The ability of deep models to generalize across unseen malware variants makes them particularly suitable for 5G-enabled IoT systems, where the scale of connected devices significantly expands the attack surface.

4.3 Privacy-Preserving AI

One of the major challenges in adopting AI for security in IoT systems is the handling of sensitive user data. Privacy-preserving techniques such as federated learning (FL) and differential privacy have gained significant attention. FL enables the training of AI models collaboratively across multiple IoT and edge devices without centralizing raw data, thereby reducing privacy risks. Differential privacy ensures that model updates do not inadvertently reveal individual user data. These approaches are particularly relevant in healthcare IoT, smart homes, and industrial IoT applications, where sensitive data must be protected while still benefiting from intelligent security models. The integration of FL with edge computing reduces communication overhead and latency, further making it a practical solution in 5G environments.

4.4 AI for Access Control and Authentication

Traditional static authentication mechanisms, such as passwords and pre-shared keys, are insufficient for IoT devices in 5G environments due to device heterogeneity and resource constraints. AI-driven access control systems provide dynamic, context-aware authentication based on behavioral biometrics, device usage patterns, and environmental contexts. Reinforcement learning can adaptively adjust access policies in response to threat levels, while deep learning models can enable continuous authentication through multimodal data such as voice, motion, and device interaction patterns [19]. Moreover, AI-based authentication mechanisms significantly enhance scalability, making them well-suited to environments with billions of connected IoT devices.

4.5 Evaluation Criteria – Performance, Scalability, Energy Efficiency, Security

Blockchain technology provides decentralization, immutability, and transparency, which are crucial for ensuring trust in distributed IoT environments [31]. However, blockchain alone is insufficient to address dynamic threats and scalability issues. The combination of blockchain with AI has emerged as a promising hybrid framework. AI models can detect intrusions, malware, and anomalous activities, while blockchain ensures secure data sharing, auditability, and tamper-proof logging of security events. Edge devices can leverage lightweight blockchain frameworks combined with federated learning to achieve decentralized yet intelligent threat mitigation. Such hybrid solutions are increasingly gaining attention in domains like smart cities, supply chain management, and intelligent transportation systems, where data authenticity and real-time responsiveness are critical.
Figure 2 presents the taxonomy mapping the discussed AI-driven security categories.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

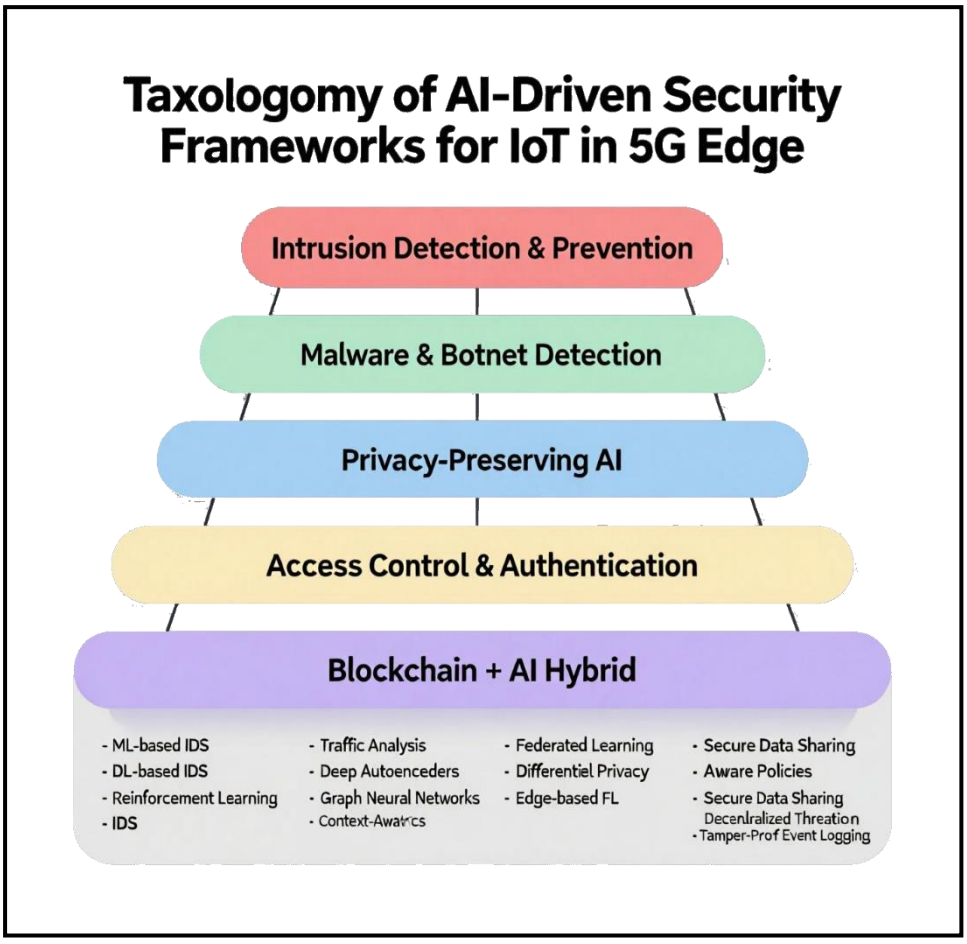

Figure 2: Taxonomy od AI-Driven Security frameworks for IoT in 5G Edge

5 Comparative Analysis of Existing Frameworks

This section synthesizes representative studies (2021–2025) on AI-driven security for IoT in 5G/edge environments and compares them across the dimensions most relevant to survey readers and reviewers: AI technique, target threat, latency (suitability for real-time use), accuracy (or detection efficacy), scalability (how well the approach grows with devices/data), datasets used for evaluation, and practical strengths/weaknesses. The selection emphasizes recent, peer-reviewed work and well-cited public datasets so readers can reproduce results or build on prior art. Federated learning (FL) and edge-deployed ML/DL have emerged as dominant paradigms for privacy-aware, low-latency defenses, while ensemble and hybrid approaches (e.g., combining DL with graph models or blockchain) are common routes to improve robustness and trustworthiness.

5.1 Overview of the literature sample and evaluation conventions

The comparative tables below report the key technical choices and the evaluation outcomes the original authors used. Where authors reported latency, we reproduce their classification as "real-time" (sub-second / edge-feasible) or "near-real-time" (seconds) when available; otherwise, we mark latency as "not reported." Accuracy/F1/other metrics are

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

shown as reported by the study; note that direct numeric comparison across papers is imperfect because experiments use different datasets, preprocessing, balancing techniques (SMOTE, ADASYN, etc.), and threat models. Popular benchmark datasets used by the community include TON_IoT, BOT-IoT, CICIDS (2017/2018), NSL-KDD, and IoT-specific collections such as IoT23; TON_IoT in particular was introduced to capture telemetry from heterogeneous IoT/IIoT sensors and is widely used in recent IDS evaluations.

5.2 Comparative table — Representative frameworks (2021–2025)

SN	Paper (year)	AI technique	Target threat	Dataset(s)	Latency suitability	Key metric(s) reported	Scalability / notes
1	"Smart Deep Learning Model for Enhanced IoT IDS" (2025)	DL ensemble	Generic IDS / anomalies	(The paper evaluates multiple IoT IDS corpora)	Near-real-time (edge-adapted)	Accuracy >95% on several sets	Ensemble boosts accuracy; higher compute at edge [5].
2	"FL-Based Intrusion Detection in IoT Networks" (2024)	Federated DL (client models + aggregation)	Intrusions (DoS/scan/etc.)	TON_IoT, others	Real/near-real-time (rounds dependent)	Competitive to centralized (≈85–98%)	Focus on IoT hardware feasibility and local model sizing [1].
3	"Deep Graph Embedding for IoT Botnet Detection" (2023)	GNN + graph features	Botnets / coordinated traffic	IoT botnet traces (incl. IoT-23 variants)	Near-real-time at gateway	>90% F1 (reported)	Captures device-relation context; more compute [32].
4	"IoT Intrusion Detection with Deep Learning" (2024)	ANN / DL	Botnet / IDS	BoTNeT-IoT-L01	Real-time (compact nets)	High acc. on BoTNeT-IoT-L01	Lab dataset; generalization caveat [22].
5	"FL-based IDS for the Internet of Things" (2024)	Supervised + unsupervised DL under FL	IDS (multi-class)	Common IoT IDS sets	Near-real-time	Gains in privacy with similar accuracy	Communication rounds overhead analyzed [20].

6	"Botnet Detection for IoT at the Edge (SDN-aided)" (2023)	Graph features + anomaly DL	Botnets	Custom/IoT traffic	Edge-real-time	High detection (paper)	SDN controller assists feature collection [29].
7	"Hybrid AI–Blockchain Security for Smart Grids" (2025)	AI + blockchain	Integrity, tamper, cyber-attacks	Smart-grid test data	Near-real-time (ledger-optimized)	Improved detection & auditability	DLT adds trust; latency/storage trade-offs [31].
8	"BoT-EnsIDS: Detecting IoT Botnet Attacks" (2025)	Hybrid ML/DL	Botnet / IDS	BoT-IoT, others	Near-real-time	F1 and FAR improvements reported	Focus on false-alarm reduction for edge [21].
9	"Optimal FL-Based IDS for IoT" (2025)	FL with DL clients	Multi-attack IDS	Mixed IoT corpora	Near-real-time	Accuracy gains vs single-site	Addresses novel-pattern generalization [33].
10	"CNN+SVM IoT Botnet Detection" (2024)	CNN features + SVM	Botnet	IoT botnet traces	Real-time	High acc. (paper)	Lightweight classifier head for gateways [34].
11	"Intelligent IDS for IoT (21 NN models on BoT-IoT)" (2025)	Multiple DL + ensemble	IDS	BoT-IoT	Near-real-time	Accuracy/Precision/Recall/F1 high	Systematic model comparison for IoT [30].
12	"Trust-Centric FL with TabTransformer	FL + TabTransformer	IDS	TON_IoT / tabular IDS	Near-real-time	Improved F1 vs baselines	Trust weighting of clients; tabular DL [2].

	(TTF)" (2025)						
13	"Quantile-Uniform + Hybrid DL/ML IDS" (2025)	Feature engineering + DL/ML ensemble	IDS / botnet	BOT-IoT, CICIOT-2023, IOT-23	Near-real-time	Acc: 100/99.2/91.5% respectively	Shows dataset-sensitivity of metrics [7].
14	"EC-IoT + AI Security Strategies" (2024)	Edge AI patterns	IDS/Privacy (design)	Surveyed sets	Real/near-real-time	(design study)	Practical edge placement guidance [35].
15	"Cosine-Similarity-Based IDS (LSTM)" (2025)	LSTM + feature selection	IDS	UNSW-BoT-IoT & BoT-IoT	Real/near-real-time	High Acc/Prec/Rec/F1	Compact features for edge devices [36].
16	"FL for IoT IDS (evaluation study)" (2024)	Federated ML	IDS	Mixed (incl. IoT)	Near-real-time	Acc improvements reported	Highlights privacy & transfer costs [37].
17	"GNN-IDS on CIC-IoT-2023" (2025)	Graph Neural Networks	IDS / robustness	CIC-IoT-2023	Near-real-time	Strong effectiveness reported	GNN handles uncertainty; explanations [18].
18	"Hybrid Blockchain for IoT Identity Mgmt." (2024)	Blockchain + AI hooks	Identity / access	Prototype	Near-real-time (PoC)	Security & efficiency gains (design)	Identity-centric; ledger overhead noted [38].
19	"Real-Time IoT NIDS (Applied Sci.)" (2025)	DL-based NIDS	IDS	BoT-IoT	Real-time focus	Critiques feature selection; proposes improvements	Emphasis on deployment realism [39].
20	"Botnet Detection & Mitigation	ML at edge + mitigation	DDoS/botnet	Corporate/IoT traces	Near-real-time	Effective mitigation shown	Moves detection closer to source [27].

	at Source (Sensors)" (2023)						

Notes on datasets and pre-processing. Studies frequently apply sampling and balancing techniques (SMOTE (Synthetic Minority Over-sampling Technique), ADASYN (Adaptive Synthetic Sampling), ROS (Random Over-Sampling)) and feature selection/engineering that strongly influence reported metrics; recent work highlights how different balancing strategies can push reported accuracy from high-80s to near-100% on some datasets, underscoring the need for standardized evaluation protocols [7][40].

5.3 Comparative table — Strengths, weaknesses, and reproducibility

Framework class	Strengths	Weaknesses	Typical reproducibility concerns
Centralized DL IDS (cloud training, edge inference)	Strong pattern learning, high detection rates with large labeled corpora	High communication cost, privacy concerns, single point of failure	Dataset mismatch (lab vs real traffic), hyperparameter sensitivity
Federated Learning NIDS	Preserves data locality/privacy; naturally distributed for edge	Susceptible to poisoning/label-flips; aggregation overhead; heterogeneity of client data	Need access to client update logs and aggregation code; studies differ in robust aggregation methods used [41].
Lightweight edge DL (autoencoders, 1D-CNN)	Low latency, deployable on gateways/edge nodes, energy-aware	May underperform on unseen attacks; limited contextual awareness	Hardware/firmware differences affect runtime; often evaluated only in simulation or constrained testbeds
Ensemble approaches	Better robustness and often higher accuracy across multiple datasets	Increased computational footprint; complex deployment	Reproducibility depends on exact model stacking and preprocessing pipelines
Blockchain + AI hybrids	Tamper-evident logs, decentralized trust, auditable model updates	Blockchain overhead (latency, storage); scalability challenges for high-frequency events	Many proofs-of-concept lack end-to-end measured latency in real deployments

5.4 Key observations from the comparative analysis

First, federated learning is repeatedly proposed as the most practical privacy-aware paradigm for distributed IoT security because it avoids centralizing raw telemetry while allowing collaborative model improvement; however, FL brings its own attack surface (poisoning, model inversion) and communication tradeoffs that many papers explicitly address. Representative surveys and framework papers document both the promise and the vulnerabilities of FL in IoT settings. Second, hybrid architectures, ensembling classical ML with DL modules, or combining GNNs to model device relations with autoencoder anomaly detectors, improve detection of coordinated and stealthy threats such as botnets, but they also increase deployment complexity and compute needs. Recent ensemble studies show state-of-the-art detection on benchmark datasets but often omit measured end-to-end latency on constrained edge hardware, which is critical for mission-critical use cases [42].

Third, the choice and preparation of datasets heavily influence reported performance. Studies using BOT-IoT, TON_IoT, and CICIDS variants often achieve high detection metrics after careful feature selection and balancing. This has motivated recent work calling for standardized, heterogeneous, and realistic datasets and benchmarks to avoid over-optimistic claims [43].

Finally, defenses that explicitly consider adversarial behavior against the learning pipeline (e.g., label-flipping, model poisoning) are increasing. Several works propose detection or robust aggregation strategies for FL, and others propose hybrid solutions that couple blockchain immutability with federated updates to improve trust. Nonetheless, these solutions are at different maturity levels; many are still validated in simulation or small testbeds rather than longitudinal real-world deployments [40].

5.5 Recommendations for evaluation best practices (for future research)

Authors should report:

i. exact preprocessing and balancing steps (SMOTE/ADASYN parameters),
ii. the complete feature set and selection method,
iii. per-class metrics (precision/recall/F1),
iv. latency measured on target edge hardware (inference time and end-to-end detection delay), and
v. robustness tests against poisoning/poisoned clients for FL methods.

Using a combination of public IoT datasets (TON_IoT, BOT-IoT, CICIDS) and at least one realistic network capture strengthens claims of generality. Several recent works and reviews outline these gaps and call for standardized benchmarks and reproducibility artifacts (code, seeds, configs)[5], [17].

6 Evaluation Metrics and Benchmark Datasets

Evaluating AI-driven security frameworks for IoT in 5G edge environments requires moving beyond traditional classification scores to a multidimensional assessment that captures detection quality, operational cost, and suitability for real-time, resource-constrained deployments. This section first defines and contextualizes the most commonly used metrics, then reviews widely adopted public datasets for IoT security research, and finally argues for, and outlines the design of, new, realistic datasets tailored to 5G edge IoT scenarios.

6.1 Common evaluation metrics (what to measure and why)

Classification-oriented metrics remain essential for quantifying detector performance, but they must be reported together and interpreted in context. Accuracy is the fraction of correctly classified instances, but it can be misleading for imbalanced attack/benign distributions typical of security datasets. Precision (the fraction of reported positives that are true positives) and recall (the fraction of true positives detected) together give a clearer picture; the harmonic mean of precision and recall, the F1-score, summarizes the tradeoff between false alarms and missed detections. These can be expressed mathematically as:

$$\text{Precision} = TP / (TP + FP)$$
$$\text{Recall} = TP / (TP + FN)$$
$$F1 = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$$

where TP, FP, and FN denote true positives, false positives, and false negatives respectively. Complementary measures such as the false alarm rate (FAR = FP / (FP + TN)) and specificity (TN / (TN + FP)) are critical because excessive false alarms can overwhelm operators and automated mitigation systems at the edge.

For operational deployment in 5G/edge settings, additional metrics must be considered alongside classification performance. Latency measures the time from when suspicious activity occurs to when a detection decision (and any

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Akinsiku et al. Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3092-9598

countermeasure) is executed; for many IoT applications "real-time" implies end-to-end detection and mitigation within milliseconds to low seconds depending on the use case. Energy efficiency quantifies the power cost of on-device inference and communications; for battery-powered sensors and gateways this can be the limiting factor for continuous monitoring. Model footprint (memory and storage required), CPU and accelerator utilization, and network overhead (bytes exchanged during model updates or telemetry transmission) determine whether a model is feasible on constrained edge hardware.

Robustness metrics are increasingly important. These include performance under adversarial conditions (model accuracy when a certain percentage of training or client updates are poisoned), resilience to distribution shift (performance when deployed on traffic distributions different from training), and explainability metrics (how interpretable model decisions are, often quantified indirectly via human-in-the-loop studies or proxy measures such as sparsity and rule extraction fidelity). Finally, reproducibility indicators, such as reporting of preprocessing steps, class imbalance handling, evaluation splits, random seeds, and hardware used for latency/energy measurements—are themselves practical metrics of research quality and usefulness.

6.2 Popular benchmark datasets for IoT security

Over the past decade several public datasets have become de facto standards for evaluating IoT intrusion detection and malware/botnet detection systems. CICIDS2017 (and subsequent CICIDS variants) provide a wide range of labeled attack scenarios and are frequently used for IDS benchmarking [5]. BOT-IoT focuses on IoT botnet and volumetric attack traffic and is useful for evaluating detection of coordinated network attacks. TON_IoT collects telemetry from heterogeneous IoT and IIoT devices, combining sensor logs, flow records, and system telemetry, which makes it attractive for experiments that span device and network layers. IoT-23 and N-BaIoT provide malware-infected IoT device captures and allow testing of device-level detection methods. Legacy datasets such as NSL-KDD and UNSW-NB15 continue to be used as baseline comparisons but do not reflect the traffic characteristics or device heterogeneity of modern IoT/5G edge ecosystems [5].

While these datasets support controlled experimentation and reproducibility, they have limitations when assessing solutions intended for 5G edge deployment. Many were collected in laboratory or emulated environments, lack 5G signalling and mobility traces, are imbalanced in ways that do not reflect real deployment ratios, or omit hardware and power measurements required for edge feasibility studies. Nevertheless, for comparative studies where authors clearly document preprocessing and limitations, these datasets remain useful starting points.

6.3 The need for new real-world datasets for 5G edge IoT and recommended design principles

The arrival of 5G and the decentralization introduced by edge computing change both traffic patterns and threat surfaces, making it necessary to supplement existing benchmarks with new datasets that capture those characteristics. A dataset intended for rigorous evaluation of AI-driven security at the 5G edge should include several key elements.

First, multi-modal telemetry is essential. Raw network flows (including 5G specific metadata such as RAN and core KPIs where permissible), device system logs, sensor readings, and edge platform metrics (CPU, memory, accelerator usage, power draw) should be collected in synchronized form. This enables cross-layer feature engineering and evaluation of detectors that fuse device, network, and edge signals.

Second, mobility and handover events should be represented because 5G mobility can change routing, latency, and session continuity, factors that influence both benign behaviour and attack impact. Third, the dataset should include realistic background (benign) traffic from diverse applications, video, telemetry, periodic sensor updates, firmware updates, and intermittent user-driven traffic, so that models are not overfitted to narrow lab traffic patterns.

Fourth, labeled attack scenarios must be diverse and clearly documented. Beyond classic DDoS and scanning, datasets should include poisoning attacks against learning pipelines, model update tampering (for federated settings), coordinated botnet campaigns that exploit device-to-device channels, side-channel leakage traces where feasible, and privacy-breach

vectors. Labels should include both coarse attack types and fine-grained annotations (start/stop timestamps, affected devices, and attack vectors) to enable temporal evaluation and detection-time metrics.

Fifth, the dataset should provide hardware metadata and energy traces to allow evaluation of model footprint and energy efficiency. Including representative edge hardware (commercial gateways, small servers, and common MCU classes) in the testbed or providing hardware-in-the-loop logs enables end-to-end latency and power measurements rather than relying on simulated cost models.

Sixth, datasets must consider privacy, consent, and legal constraints. Where user data is involved, privacy-preserving collection techniques, strong anonymization, and clear data sharing agreements are required. Synthetic augmentation techniques can supplement real captures when privacy prevents raw data release; however, any synthetic data should be clearly marked and validated for realism.

Standardization of evaluation protocols is crucial. Dataset releases should include recommended train/test splits, time-based cross-validation protocols to emulate concept drift, adversarial evaluation suites (e.g., a set of poisoning or evasion attacks with configurable strength), and baseline implementations with scripts for preprocessing and feature extraction. Providing Dockerized or virtualized testbeds and sample notebooks that reproduce key results dramatically improves reproducibility.

6.4 Practical checklist for authors reporting evaluations

Authors should report classification metrics per class (precision, recall, F1), confusion matrices, ROC/AUC and Precision–Recall curves for imbalanced scenarios, false alarm rates, and detection latency measured end-to-end on representative hardware. They should include model size, peak memory, average inference time, communication overhead (bytes per update and number of rounds for federated schemes), and energy cost where applicable. Robustness tests should demonstrate performance under distribution shift and quantify the impact of adversarial manipulations or poisoned clients in federated settings. Finally, authors should publish preprocessing code, feature extraction pipelines, and, where permitted, dataset splits and seeds to enable reproducibility.

In sum, while established benchmark datasets enable valuable comparative work, the unique combination of 5G, edge computing, and heterogeneous IoT demands richer, multi-modal, privacy-respecting datasets and standardized evaluation protocols so that claimed advances translate into practical, deployable security for real-world systems.

7 Future Outlook

As wireless generations advance and computation moves ever closer to the edge, the security landscape for IoT will evolve from reactive defenses to proactive, adaptive systems that think and act across network, device, and application boundaries. By the time 6G technologies begin to mature, the combination of pervasive connectivity, pervasive sensing, and abundant distributed compute will enable security architectures that are not merely detectors but autonomous, self-healing controllers that prevent, mitigate, and learn from attacks with minimal human intervention.

In this envisioned future, AI-driven security operates as a continuous control loop that senses anomalies, reasons about risk, plans mitigations, and executes countermeasures across device, edge, and cloud tiers. Models will increasingly be agentic: they will coordinate across multiple nodes to isolate compromised devices, reconfigure network slices to contain attacks, and re-deploy lightweight models or policies to affected segments in real time. These agents will rely on continual learning pipelines that incorporate on-device adaptation, federated updates, and secure model provenance, enabling defenses to evolve as threat tactics change while limiting exposure of raw telemetry and private data.

Blockchain and distributed ledger technologies will play a complementary role by providing auditable, tamper-evident records of security events, model updates, and policy changes. In practice, lightweight ledger primitives—or hybrid ledgers optimized for latency-sensitive edge environments—will be used to establish trust among heterogeneous

stakeholders (device manufacturers, service providers, and users), to notarize model weights and provenance, and to enforce decentralized access policies without central points of failure. The synergy between AI and ledger systems will enable verifiable, auditable, and accountable security workflows that are necessary for regulated sectors such as healthcare and critical infrastructure.

In brief, the future outlook for IoT security in 6G and beyond is one of intelligent, distributed, and energy-efficient defenses that combine agentic AI, trustworthy ledgers, and neuromorphic efficiency. Realizing this vision will require multidisciplinary advances in learning algorithms, hardware design, distributed systems, and governance. The ultimate success metric will not only be superior detection rates but demonstrable resilience: systems that sustain critical services, preserve privacy, and enable rapid, transparent recovery from incidents in a globally connected world.

8 Conclusion

This survey has explored the evolving landscape of AI-driven security frameworks for IoT within the context of 5G and edge computing ecosystems. Beginning with an overview of the exponential growth of IoT and the resulting attack surface, the study highlighted the insufficiency of traditional security paradigms in meeting the low-latency, high-scalability, and energy-efficient requirements of modern networks. A taxonomy of AI-based frameworks was presented, spanning intrusion detection and prevention, malware and botnet detection, privacy-preserving techniques, AI-enhanced access control, and blockchain–AI hybrids for decentralized trust. Comparative analysis of recent studies between 2019 and 2025 revealed that while AI techniques such as deep learning, reinforcement learning, and federated learning demonstrate impressive detection accuracies, they face persistent challenges in scalability, interpretability, and real-world deployment. Key evaluation metrics—including accuracy, precision, recall, F1-score, false alarm rate, and energy efficiency, were contextualized alongside widely used benchmark datasets such as CICIDS2017, Bot-IoT, and TON_IoT. However, the survey also underscored the pressing need for new datasets that accurately capture the heterogeneity and dynamics of 5G edge-enabled IoT environments. Emerging challenges, from the scalability of AI to quantum-era security considerations, highlight the necessity of research that balances performance with transparency, privacy, and resource constraints.

For academia, this survey provides a consolidated taxonomy, comparative mapping, and critical discussion of open problems, serving as a roadmap for future research. For industry, it underscores practical considerations for deploying AI-based security in ultra-dense IoT ecosystems, drawing attention to trade-offs in performance, privacy, and energy use. In closing, AI is not merely a tool but a transformative force shaping the trajectory of IoT security. In 5G and beyond, its integration with distributed edge intelligence, blockchain-based trust models, and neuromorphic computing points toward adaptive, autonomous, and resilient defenses. The path forward lies in building systems that are not only accurate but explainable, not only reactive but proactive, and not only secure but privacy-preserving—ultimately enabling trust in the interconnected fabric of future digital societies.

References

[1] N. Albanbay *et al.*, "Federated Learning-Based Intrusion Detection in IoT Networks: Performance Evaluation and Data Scaling Study," *J. Sens. Actuator Networks*, vol. 14, no. 4, 2025, doi: 10.3390/jsan14040078.

[2] M. Abd Elaziz, I. A. Fares, A. Dahou, and M. Shrahili, "Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimization.," *Front. big data*, vol. 8, p. 1526480, 2025, doi: 10.3389/fdata.2025.1526480.

[3] V. Mahesh and S. Bhargava, "Integration of IoT and 5G: A comprehensive review of opportunities and challenges," in *AIP Conference Proceedings*, AIP Publishing LLC, 2025, p. 20026.

[4] A. Biswas and H.-C. Wang, "Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain," *Sensors*, vol. 23, no. 4, p. 1963, 2023.

[5] F. S. Alsubaei, "Smart deep learning model for enhanced IoT intrusion detection," *Sci. Rep.*, vol. 15, no. 1, p. 20577, 2025, doi: 10.1038/s41598-025-06363-5.

[6] V. Veeramachaneni, "Edge Computing: Architecture, Applications, and Future Challenges in a Decentralized Era," *Recent Trends Comput. Graph. Multimed. Technol.*, vol. 7, no. 1, pp. 8–23, 2025.

[7] S. Ullah *et al.*, "Comparative analysis of deep learning and traditional methods for IoT botnet detection using a multi-model framework across diverse datasets," *Sci. Rep.*, vol. 15, no. 1, p. 31072, 2025, doi: 10.1038/s41598-025-16553-w.

[8] S. A. A. Hakeem and H. Kim, "Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security," *IEEE Trans. Intell. Transp. Syst.*, 2025.

[9] R. A. R. Ait Mouha, "Internet of things (IoT)," *J. Data Anal. Inf. Process.*, vol. 9, no. 02, p. 77, 2021.

[10] S. Khunteta, P. Saikrishna, A. Agrawal, A. Kumar, and A. K. R. Chavva, "RF-sensing: a new way to observe surroundings," *IEEE Access*, vol. 10, pp. 129653–129665, 2022.

[11] Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, "Wireless communication technologies for IoT in 5G: Vision, applications, and challenges," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, p. 3229294, 2022.

[12] M. T. Masud, M. Keshk, N. Moustafa, I. Linkov, and D. K. Emge, "Explainable artificial intelligence for resilient security applications in the Internet of Things," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 2877–2906, 2024.

[13] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "IoT and man-in-the-middle attacks," *Secur. Priv.*, vol. 8, no. 2, p. e70016, 2025.

[14] M. Kiruthiga Devi and M. Padma Priya, "Evolution of next generation networks and its contribution towards industry 5.0," *Resour. Manag. Adv. Wirel. networks*, pp. 45–80, 2025.

[15] A. Rathore, S. Mishra, V. Kaushik, S. S. Kolaventi, and V. J. K. K. Sonti, "Energy–Efficient Communication Protocols For Massive Machine-Type Communications (MMTC)," *Natl. J. Antennas Propag.*, vol. 7, no. 1, pp. 62–69, 2025.

[16] O. J. Adeyeye, I. Akanbi, I. Emeteveke, and O. Emehin, "Leveraging secured AI-driven data analytics for cybersecurity: Safeguarding information and enhancing threat detection," *Int. J. Res. Publ. Rev.*, vol. 5, no. 10, pp. 3208–3223, 2024.

[17] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset," *IEEE access*, vol. 9, pp. 22351–22370, 2021.

[18] S. Saxena, J. Grover, and S. Singhal, "Exploring Graph Neural Networks for Robust Network Intrusion Detection," *Procedia Comput. Sci.*, vol. 258, pp. 3630–3639, 2025, doi: https://doi.org/10.1016/j.procs.2025.04.618.

[19] F. Louati, F. B. Ktata, and I. Amous, "Enhancing Intrusion Detection Systems with Reinforcement Learning: A Comprehensive Survey of RL-based Approaches and Techniques," *SN Comput. Sci.*, vol. 5, no. 6, p. 665, 2024.

[20] B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models," *Cyber Secur. Appl.*, vol. 3, p. 100068, 2025, doi: https://doi.org/10.1016/j.csa.2024.100068.

[21] T. Al-Shurbaji *et al.*, "BoT-EnsIDS: Approach for detecting IoT Botnet attacks leveraging bio-inspired based ensemble feature selection and hybrid deep learning model," *Alexandria Eng. J.*, vol. 129, pp. 744–767, 2025, doi: https://doi.org/10.1016/j.aej.2025.06.030.

[22] M. Z. Qureshi, M. A. Sarwar, M. M. S. Missen, Haseeb Ur Rehman, and N. Umer, "IoT Intrusion Detection with Deep Learning Techniques," *VFAST Trans. Softw. Eng.*, vol. 12, no. 4 SE-Articles, pp. 145–157, Dec. 2024, doi: 10.21015/vtse.v12i4.1918.

[23] M. Sharma, A. Tomar, and A. Hazra, "Edge computing for industry 5.0: Fundamental, applications, and research challenges," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19070–19093, 2024.

[24] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, p. 8669348, 2022.

[25] M. Kaleem *et al.*, "Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities," *J. Comput. Biomed. Informatics*, vol. 7, no. 02, 2024.

[26] P. Victor, A. H. Lashkari, R. Lu, T. Sasi, P. Xiong, and S. Iqbal, "IoT malware: An attribute-based taxonomy, detection

mechanisms and challenges," *Peer-to-peer Netw. Appl.*, vol. 16, no. 3, pp. 1380–1431, 2023.

[27] F. L. de Caldas Filho *et al.*, "Botnet Detection and Mitigation Model for IoT Networks Using Federated Learning," *Sensors*, vol. 23, no. 14. 2023. doi: 10.3390/s23146305.

[28] A. N. Kalejaiye, "Adversarial Machine Learning for Robust Cybersecurity: Strengthening Deep Neural Architectures against Evasion, Poisoning, and Model-Inference Attacks".

[29] D. C. Muñoz and A. del-C. Valiente, "A novel botnet attack detection for IoT networks based on communication graphs," *Cybersecurity*, vol. 6, no. 1, p. 33, 2023, doi: 10.1186/s42400-023-00169-6.

[30] H. Zhang, "Development of an intelligent intrusion detection system for IoT networks using deep learning," *Discov. Internet Things*, vol. 5, no. 1, p. 74, 2025, doi: 10.1007/s43926-025-00177-7.

[31] Y. Y. Ghadi *et al.*, "A hybrid AI-Blockchain security framework for smart grids," *Sci. Rep.*, vol. 15, no. 1, p. 20882, 2025, doi: 10.1038/s41598-025-05257-w.

[32] B. Zhang, J. Li, L. Ward, Y. Zhang, C. Chen, and J. Zhang, "Deep Graph Embedding for IoT Botnet Traffic Detection," *Secur. Commun. Networks*, vol. 2023, no. 1, p. 9796912, 2023, doi: https://doi.org/10.1155/2023/9796912.

[33] A. Karunamurthy, K. Vijayan, P. R. Kshirsagar, and K. T. Tan, "An optimal federated learning-based intrusion detection for IoT environment," *Sci. Rep.*, vol. 15, no. 1, p. 8696, 2025, doi: 10.1038/s41598-025-93501-8.

[34] C. Lai, Y. Yao, Y. Chen, X. Liang, T. Cai, and Y. Shi, "Detection of IoT Botnet Based on Convolutional Neural Network and Linear Support Vector Machine," in *Proceedings of the 2023 13th International Conference on Communication and Network Security*, in ICCNS '23. New York, NY, USA: Association for Computing Machinery, 2024, pp. 222–226. doi: 10.1145/3638782.3638816.

[35] D. Rupanetti and N. Kaabouch, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities," *Applied Sciences*, vol. 14, no. 16. 2024. doi: 10.3390/app14167104.

[36] A. Prasad, W. Mohammad Alenazy, N. Ahmad, G. Ali, H. A. Abdallah, and S. Ahmad, "Optimizing IoT intrusion detection with cosine similarity based dataset balancing and hybrid deep learning," *Sci. Rep.*, vol. 15, no. 1, p. 30939, 2025, doi: 10.1038/s41598-025-15631-3.

[37] R. Lazzarini, H. Tianfield, and V. Charissis, "Federated Learning for IoT Intrusion Detection," *AI*, vol. 4, pp. 509–530, Jul. 2023, doi: 10.3390/ai4030028.

[38] S. S. Golder, S. Mondal, S. Das, R. Bose, S. Sutradhar, and H. Mondal, "Hybrid Blockchain Framework for Secure and Scalable Internet of Things (IoT) Networks (HB-IoT): A Novel Approach," in *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA)*, IEEE, 2024, pp. 1–7.

[39] J. Ashraf, G. M. Raza, B.-S. Kim, A. Wahid, and H.-Y. Kim, "Making a Real-Time IoT Network Intrusion-Detection System (INIDS) Using a Realistic BoT–IoT Dataset with Multiple Machine-Learning Classifiers," *Applied Sciences*, vol. 15, no. 4. 2025. doi: 10.3390/app15042043.

[40] E. M. Maseno, Z. Wang, and Y. Sun, "Performance Evaluation of Intrusion Detection Systems on the TON_IoT Datasets Using a Feature Selection Method," in *Proceedings of the 2024 8th International Conference on Computer Science and Artificial Intelligence*, in CSAI '24. New York, NY, USA: Association for Computing Machinery, 2025, pp. 607–613. doi: 10.1145/3709026.3709048.

[41] J.-P. A. Yaacoub, H. N. Noura, and O. Salman, "Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 155–179, 2023, doi: https://doi.org/10.1016/j.iotcps.2023.04.001.

[42] E. Dritsas and M. Trigka, "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1. 2025. doi: 10.3390/jsan14010009.

[43] T. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. den Hartog, "ToN_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets," *IEEE Internet Things J.*, vol. PP, p. 1, May 2021, doi: 10.1109/JIOT.2021.3085194.