EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Statistical Analytical Review of IoT Threat Detection Mechanisms: Quantitative Evaluation and Multidimensional Performance Assessment Analysis

Lanka Kavitha[1], Kareemulla Shaik[1*]

[1]School of Computer Science and Engineering, VIT-A.P University, Amaravati-522241, Andhra Pradesh, India

Abstract

Increased deployment of IoT systems in industrial, healthcare, smart city, and home environments has expanded the attack surface and complexity of cyber threats. Though a plethora of detection techniques have emerged in literature in the last decade, an unforgivable absence of statistical rigors and compare-and-contrast analysis on the operational characteristics is apparent in the literature sets. This paper presents a statistical analytical review of various contemporary IoT threat detection methods across a wide array of architectures: classical machine learning, deep learning, federated learning, blockchain-based systems, quantum-enhanced frameworks, and hybrid models. The review employs a multidimensional evaluation strategy, extracting both qualitative and quantitative metrics from each study; these enable an objective comparison across heterogeneous systems, Standard performance parameters—Scalability, Delay, Time Complexity, Memory Complexity, Make span, and Analysis Efficiency—are tabulated; thus, an unfolding of a universal analytical framework with almost 300 data points exposes trade-offs, bottlenecks to efficiency, and constraints to deployment. Furthermore, evaluation of the application-specific techniques for healthcare, agriculture, and smart grids were conducted in relation to adaptability and domain specifications. The work identifies that hybrid deep networks (e.g., CNN-LSTM) provide better accuracy at higher computation cost, while TinyML and ensemble models present a trade-off factor for both detection accuracy versus hardware efficiency. In addition, whereas quantum and blockchain Integrated systems have shown to be solid in theory, they face practical impairments. Research gaps identified here lead the discussion on future directions, toward explainability, energy-aware design, and adversarial resilience, thus providing a tangible roadmap toward the next generation of secure IoT frameworks.

Keywords: IoT Security, Threat Detection, Machine Learning, Statistical Analysis, Performance Evaluation, Internet of Things (IoT), Process

Received on 09 October 2025, accepted on 13 December 2025, published on 12 January 2026

doi: 10.4108/eetiot.10529

* Corresponding author. Email: kareemulla.shaik@vitap.ac.in

1. Introduction

With the proliferation of IoT devices, the entire ecosystem has been changed in terms of connectivity, automation, and data intelligence almost instantaneously in domains such as healthcare, manufacturing, agriculture, smart cities, and home automations [1]. However, the very interconnectivity of these systems creates exploitable vulnerabilities that increase by the minute with the industry becoming equipped with advanced adversities and the complexity and diversity of IoT ecosystems pose notable security vulnerabilities and challenges. The most economical and effective way to ensure security is to reduce IoT device vulnerabilities prior to deployment. Therefore, even if the system is still under development, it is vital to identify and address as many security flaws as possible [1].

1.1 Motivation

Many sensors, including cameras, microphones, and thermometers, are built into Internet of Things (IoT) devices. These sensors are always collecting data about their environment, including sensitive and private information. As shown in the diagram, this data is first analyzed before being moved and stored throughout the various layers of the IoT architecture.1. Smart gadgets result in the acquisition of a significant amount of user data, even while they provide benefits, convenience, and an enhanced lifestyle [1].

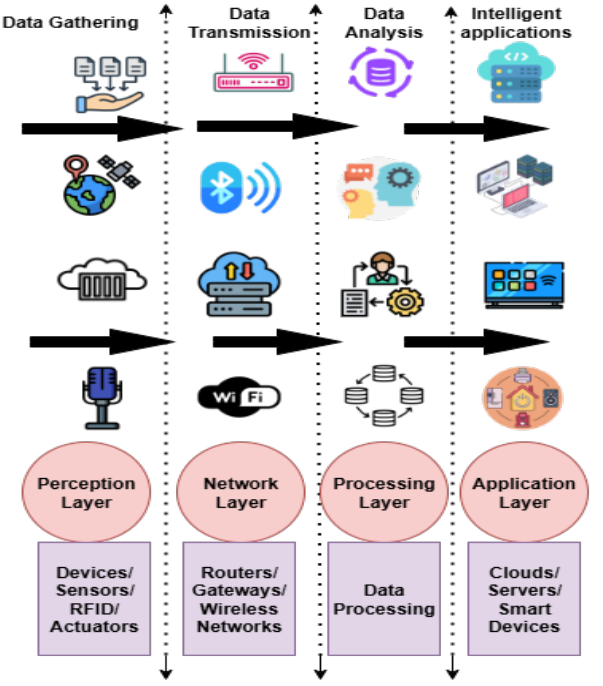

Figure 1: Survey Outline Diagram

As illustrated in Figure. 2, the layers of IoT architecture are exposed to diverse vulnerabilities, which can be mitigated through preventive measures prior to device deployment. These vulnerabilities, spanning from hardware to application layers, highlight the multidimensional nature of IoT security challenges. Addressing them requires a holistic approach that integrates secure design, regular updates, strong encryption, and effective device management mechanisms [1].

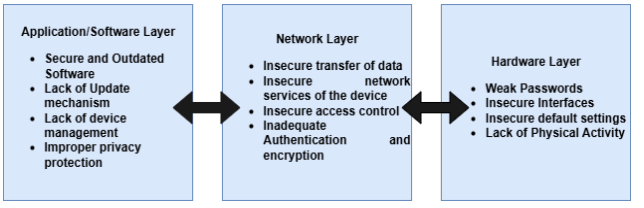

Figure 2: Vulnerabilities in IoT Ecosystem Architecture

1.2 Security in IoT

The most challenging aspect of IoT networks is security. Preventing IoT assaults is difficult since there are no set standards for how IoT devices should be built. IDSs and security software, which can detect and stop attacks in IoT devices, have faced new hurdles as a result of the Internet of Things and the persistent problem of huge data flow [2]. IDS typically has significant rates of missed detections and packet losses for today's high-speed networks. Creating a quick data model for intrusion detection analysis has become a crucial problem that needs to be fixed in order to successfully boost network security.

Security protocols should be designed to identify and prevent Denial of Service (DoS) attacks that could disrupt the functioning of IoT systems. Integrity preserving IoT data and services, accuracy, dependability, and consistency across the course of their existence Security systems should detect and prevent unauthorized alterations, such as insertion, deletion, or modification of data or services. Confidentiality Preventing unauthorized access to IoT data and communications. Security measures should safeguard both data-at-rest (such as information stored in databases or storage systems) and data-in-transit (as it moves across networks). (e.g., during communication among devices, networks, or applications) [2]. Authentication Confirming the identity of users or devices in the IoT environment. Mechanisms must verify the authenticity of both devices and users, allowing only trusted parties to access or produce data. Authorization Ensuring that only permitted entities can access specific IoT resources. Systems should verify that connected devices or users

have appropriate permissions to use certain services or data. Access Control Regulating and managing access to IoT systems and their resources. Solutions should

evaluate whether a device or user is allowed to access data or services, thereby restricting unauthorized usage [2]. The Following table represents the security measures in IoT.

Table 1. IoT Security Measures

Security Measure	Objective	Implementation in IoT Security	References
Availability	Guarantees that IoT services and resources remain continuously accessible to legitimate users, even under adverse conditions.	Deployment of defense mechanisms against Denial-of-Service (DoS/DDoS) attacks, redundancy strategies, and fault-tolerant architectures to sustain uninterrupted operations	[26] Nawaz et al., [46] Yang et al.
Integrity	Ensures accuracy, reliability, and consistency of IoT data and services throughout their lifecycle.	Use of cryptographic hash functions, digital signatures, and anomaly detection systems to prevent unauthorized modifications, insertions, or deletions	[3] Sheeba & Shaji, [45] Zhang et al.
Confidentiality	Protects IoT data and communication channels from unauthorized disclosure.	Adoption of encryption mechanisms for both data-at-rest and data-in-transit (e.g., TLS, lightweight cryptography) to secure device-to-device and device-to-cloud communications	[19] Kwala et al., [49] Xiong et al.
Authentication	Validates the identity of IoT devices and users	Utilization of strong authentication schemes, such as certificate-based authentication, public key infrastructure (PKI), and	[18] Dahiya & Kumar, [24] Khalique et al.

	before granting access.	biometrics, to establish trusted identities	
Authorization	Ensures that only entities with appropriate privileges can access IoT services or resources.	Implementation of policy-driven mechanisms, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), for fine-grained authorization.	[9] Batta et al., [32] Kamatchi & Uma.
Access Control	Regulates and enforces policies governing IoT resource usage.	Design of lightweight, scalable access control frameworks to systematically restrict unauthorized device or user	[7] Mujlid & Alshahrani, [31] Pawar et al.

1.3 Attacks on IoT

IoT devices are increasingly exposed to a wide range of cyber threats, including data theft, phishing, spoofing, and Distributed Denial of Service (DDoS) attacks. In recent years, ransomware campaigns and large-scale breaches have become especially common, making IoT systems a primary target. Attackers often compromise the infrastructure, disrupt normal network operations, and gain unauthorized access to sensitive data [3]. Common cyber-attacks affecting IoT devices include malware infections, phishing schemes, SQL injection attacks, denial-of-service (DoS), session hijacking, botnet deployment, and ransomware intrusions. Awareness of these threats is critical for developing effective defense strategies [3].In IoT-based Wireless Sensor Networks (WSNs), various attacks exploit communication protocols and resource limitations:

- Jamming attack: Interference signals are introduced to block communication channels, causing a denial-of-service condition.
- Sybil attack: A malicious node generates multiple fake identities, deceiving other nodes and injecting false information.
- Sinkhole attack: A compromised node attracts traffic and gains control over data routing, enabling manipulation or interception of transmitted information.
- Selective forwarding attack: Certain packets are deliberately dropped or misrouted by compromised nodes, disrupting communication reliability.
- Spoofing attack: Attackers impersonate legitimate nodes to gain unauthorized access or manipulate data flows.
- Replay attack: Captured packets are resent to disrupt normal communication processes.
- Physical attack: Hardware components such as sensor nodes are tampered with, often by injecting malicious code.
- Energy depletion attack: Limited energy resources of nodes are drained intentionally, leading to network failures.
- Insider attack:Authorized nodes misuse their privileges to alter or leak data, undermining trust in the system.
- Information disclosure attack:Sensitive data is intercepted through eavesdropping, resulting in privacy violations and security breaches.

Given the internet connectivity of each node, IoT-WSN environments are inherently prone to such attacks, underscoring the importance of robust security mechanisms and awareness for mitigating vulnerabilities. The following figure.3 depicts the types of IoT and WSN attacks [3].

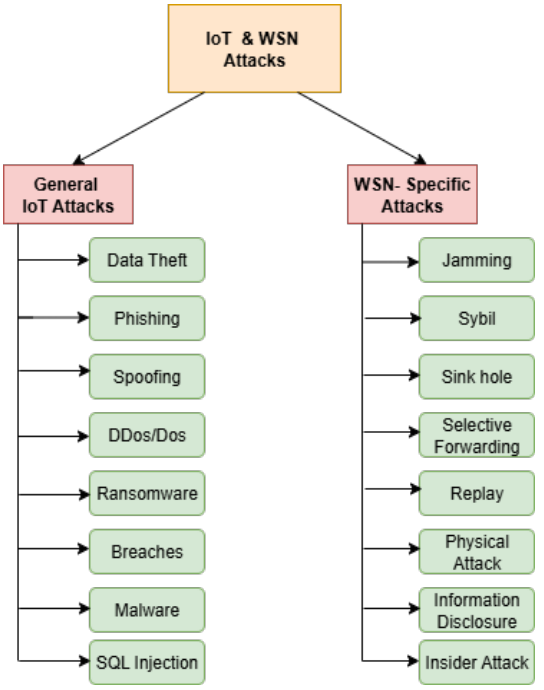

Figure 3: Types of IoT & WSN attacks

1.4 Attack Detection Methods in IoT

Recognizing and reducing these types of attacks is crucial for preserving the security of IoT environments. To tackle these challenges, numerous techniques have been created to detect attacks. These detection techniques, ranging from traditional signature-based models to advanced machine learning and hybrid approaches, provide a comprehensive defense strategy for IoT ecosystems [4]. Their effectiveness, however, depends on balancing accuracy, resource efficiency, and scalability to meet the unique demands of IoT environments. The following approaches are commonly used for identifying threats within the Internet of Things environment as shown in figure 4. On a different note, traditional security schemes have become obsolete owing to unique constraints posed by IoT systems, some of which include limited computational capability, limited memory, multiplicity of communication protocols, and absence of standardization. Therefore, research interests are inclined toward the development of adaptive and scalable threat detection mechanisms optimized for the IoT ecosystem. The variability of methodology includes traditional classifier techniques, machine learning, deep neural networks, federated learning, a blockchain-integrated paradigm, explainable artificial intelligence, and quantum-assisted security protocols. This need becomes more critical in healthcare IoT systems, where ML- and DL-based predictive models are already operational for disease diagnosis, yet often lack integrated, iterative security mechanisms to counter evolving cyber threats [50], [51]. A critical gap in systematic, statistically grounded comparative analysis exists which could lend itself to proper benchmarking. Many reviews in this area tend to focus either exclusively on qualitative measures or lack an internally consistent approach when judging quantitative performance indicators such as detection latency, scalability, memory usage, and computational complexity. This paper bridges this gap by providing a critical statistical analytical review that encompasses 49 peer-reviewed articles published from 2024 to 2025, constituting a snapshot of modern developments in IoT security.

Each one of these studies is thoroughly analyzed across the six pertinent performance measures: Scalability, Delay, Time Complexity, Memory Complexity, Make span, and Analysis Efficiency. These six measures were considered as representative of both potential performances in an applicable environment and real-world implement ability in the existing IoT ecosystem. Objective performance assessments for model categories can be made by deriving and normalizing more than 300 data points and obtaining them from the literature.

This work was inspired mainly by the urgent need for decision support tools to guide researchers, practitioners, and policymakers toward choosing the most appropriate security solutions under operational situation constraints. For example, healthcare devices applying an edge-deployment scheme will generally favor lightweight models with low latency, while trustworthy smart grid systems might deem high security acceptable, even when associated with

delayed responses. Analysis from this paper brings recognition of very interesting solutions to discussions-like the trade-offs between such behavior as detection accuracy against computational overhead, model transparency versus interpretability, and others that are more common, centralized against decentralized learning paradigms.

This research is basically focused on three major contributions: The first contribution is the quantitative meta-analysis of 49 IoT threat detection models categorized across diverse architectural paradigms. The second contribution is a performance-normalized evaluation table to facilitate everyone's comparison using these six metrics, filling a crucial void in current literature sets. The final contribution is a compilation of actionable hints and future research avenues, especially concerning adversarial robustness, cross-domain adaptability, interpretability, and energy-efficient designs. By doing this, the paper advances the field of IoT cybersecurity while laying down a statistically validated framework for the next generation of scalable and resilient IoT threat detection frameworks.

i) Signature-Based Threat Detection in IoT Frameworks

Signature-based detection still forms the primary basis of IoT security. These methods are based on known attack patterns or predefined rules for the detection of malicious behavior. Although conventional, their deterministic performance continues to keep the baseline security of IoT ecosystems.

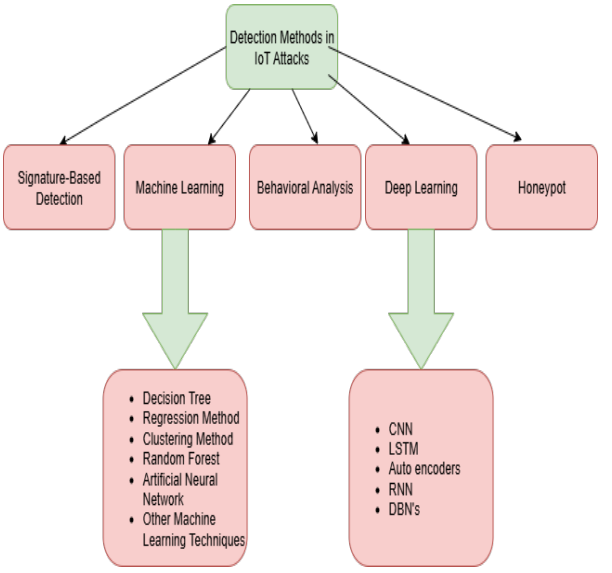

Figure 4: IoT Attack Detection Methods

Touqir et al. [1] emphasize the usefulness of fuzzing-based techniques for signature extraction, being particularly successful in finding vulnerabilities at the firmware level in the process. The work shows how fuzzing-generated inputs can serve as templates for signature creation across constrained IoT devices in the process. In a similar vein, Abdullah et al. [10] adopt a deep learning approach to improve IoT malware signature classification, combining convolutional neural networks (CNN) with malware profiling datasets to detect slight signature deviations in the process. Layers of framework Sheeba and Shaji [3] proposed Hybrid-CID mechanism that blends signature-based filtering with contextual optimization using Mongoose optimization for the betterment of signature matching on packet level and in real-time environments. In addition, Gwassi et al., [4] forward a hybrid XAI-enabled signature detection and blockchain integrity framework called Cyber-XAI-Block under smart organizational IoT settings. Despite their great efficacy in addressing well-known attacks, signature-based systems truly shine in hindering the detection of zero-day exploits or polymorphic malwares, which created an increased interest in

hybrid mechanisms as well as strategies based upon behavior sets.

ii) Behavioral Analysis Aspects of IoT Security

Behavioral threat detection, with special relevance to dynamic and context-aware environments, identifies potential threats from deviations of normal activity. These systems perform particularly well in catching novels or evolving attacks. Ran para et al. [5] examine a semantic driven deep learning architecture to model normal device behavior across IoT layers. In aligning threat response with learned behavioral semantics, the framework renders timely anomaly alerts with low false positives. Singh et al. [6] perform an exhaustive evaluation of ML and DL paradigms for traffic pattern analysis in massive IoT networks, proving that neural-based behavior modelling is crucial in spotting anomalous activities. Deswal [11] designs a deep learning intrusion detection system for IoT gateways that incorporate behavioral indicators like unusual connection frequency and payload irregularities in process. Likewise, Saranya and Valarmathi [13] use a multi-layer deep auto-encoder for cross-layer attack detection on behavioral reconstruction error, effectively catching stealthy anomalies across network and application layers. Notably, Ullah et al. [23] proposes KronNet, a lightweight Kronecker-enhanced feedforward neural network optimized for device-level behavior profiling's. Moreover, cook et al. [25] examine behavioral data from Bluetooth-based FemTech devices, shedding light on how privacy vulnerabilities manifest through regular patterns of user interaction sets.

Integrating RL into behavior analysis, Tyagi et al. [22] designed a time-series RL framework for trust prediction during blackhole attacks. The model adaptively learns, and updates trust weights that reflect real-time changes in behavior. However, behavior-based techniques, while versatile, may experience training drift and model poisoning in adversarial circumstances. Federated learning and privacy-preserving form of learning are now being considered more to counter this.

iii) Honeypot-Based Threat Detection Strategies

Honeypots stand for all decoy systems designed to lure and study attackers. These systems provide vital information about attack vectors concerning IoT systems, enabling dynamic adaptation of the detection models. Kuku et al. [16] describes a honeypot model that is digital forensic-ready, designed specifically for IoT organizations. This model obtains interaction metadata from attackers that can be used to obtain forensic evidence and update rule bases. Desikan et al. [20] propose BACHAAV, a hybrid human-AI system that uses cryptographic honeypots to lure attackers while preserving the confidentiality of data sets.

Table 2. Model's Empirical Review Analysis

Ref	Method Used	Findings	Strengths	Limitations	Recommendations to Overcome these Limitations
1	Fuzzing-based vulnerability exploration	Mapped techniques to IoT vulnerabilities; highlighted fuzzing as a viable signature-generation tool	Systematic coverage of fuzzing; effective for signature-based attack surfaces	Limited real-time applicability	Integrate fuzzing with runtime monitoring systems for adaptive threat detection
2	Hidden and connected layer neural architecture	Demonstrated improved cyberattack detection in IOT-WSN networks using	Effective multilayer abstraction for WSN-specific	Focused only on static networks	Extend model for mobile IoT networks with dynamic topology adaptation

	with threat intelligence	enriched layer-wise representations	attacks		
3	Hybrid-CID using Mongoose Optimization	Improved real-time anomaly classification by combining signature features with optimized heuristics	Fast decision-making under resource constraints	Lacks zero-day attack detection capability	Incorporate behavioral profiling to enhance model adaptability
4	Cyber-XAI-Block framework using explainable AI and blockchain	Enabled interpretable threat detection in smart organizations with audit trails	High interpretability and blockchain immutability	Complex deployment architecture	Develop modular components for lightweight integration
5	DL-based semantic computational framework	Demonstrated real-time threat inference using semantic correlations	Semantic modeling improved contextual threat accuracy	Dependent on high-quality labeled data	Apply self-supervised learning to reduce labeled data dependency
6	Empirical ML/DL evaluation for traffic analysis	Benchmarked various models for large-scale IoT traffic patterns	Comprehensive comparative metrics across methods	No cross-layer correlation modeling	Include layer-aware traffic pattern relationships
7	Quantum-enhanced AI for anomaly detection	Combined AI-driven detection with quantum principles to evolve IoT security	Resilient against cryptographic threats	Lacks practical deployment details	Develop quantum-ready APIs and integration models
8	Hybrid CNN-LSTM and ensemble learning	Enhanced detection over heterogeneous datasets	Effective fusion of spatial-temporal features	Model generalizability needs improvement	Incorporate domain adaptation for unseen data types
9	Review of blockchain-enabled security frameworks	Provided future directions and classification of blockchain applications	Covers multiple threat mitigation strategies	Lacks quantitative experimental support	Empirically validate proposed directions on real-world testbeds
10	DL-based malware analysis and classification	Achieved precise categorization of IoT malware types	Deep feature extraction from malware behaviors	Struggles with polymorphic variants	Use generative models to simulate adversarial malware
11	DL-driven intrusion detection in IoT	Proposed framework for traffic-based anomaly detection	Effective for localized threat defense	No evaluation under adversarial attacks	Augment with adversarial robustness training

	gateways	at the gateway level			
12	TinyML for threat classification on edge	Provided privacy-aware multiclassification at constrained edge nodes	Low-resource real-time inference	Reduced accuracy under imbalanced data	Employ data augmentation techniques for minority classes
13	Multilayer deep autoencoder	Detected cross-layer anomalies with reconstruction error	Strong detection of stealth attacks	Sensitivity to noise in input features	Use robust training methods to minimize overfitting
14	Analysis of privacy-preserving safeguards	Highlighted key privacy issues and mitigation techniques in cloud IoT	Holistic view of privacy risks	Lacks active detection components	Integrate findings into dynamic privacy-aware threat monitoring tools
15	ProSRN and ICOM threat management for IoT healthcare	Secured sensitive healthcare data through structured methodologies	Tailored for medical IoT environments	Model scalability not addressed	Test methods in larger multi-Institutional networks
16	Forensic readiness and resilience model using honeypots	Enabled forensic traceability and attacker profiling	Realistic data capture using honeypots	May fail against evasive attackers	Combine honeypots with behavioral anomaly detection
17	AI-quantum synergy in holographic frameworks	Advanced futuristic model combining quantum logic and AI threat detection	High theoretical resilience	No practical system realization	Prototype and benchmark model under realistic loads
18	Extreme Learning Machine with multi-kernel optimization	Achieved reduced training time with efficient feature selection	Fast and accurate classification	Limited deep feature hierarchy	Stack with deep learners for deeper context capture
19	Lattice-based cryptographic scheme comparison	Assessed post-quantum cryptographic readiness for IoT	Strong theoretical security foundation	No integration with detection pipelines	Fuse with ML models to build secure Intelligent hybrid frameworks
20	BACHAAV: ML-human-AI cryptographic	Enabled collaborative detection with cryptographic decoys	Synergistic human-machine threat adaptation	Costly to deploy	Develop modular components to reduce deployment complexity

	architecture				
21	GAO-XGBoost and ECC Integrated blockchain framework	Improved detection and secure storage for IoT traffic	Robust data management and threat prediction	Relatively high computation overhead	Optimize hyperparameters for resource-constrained environments
22	Time-series DL for trust prediction	Detected blackhole attacks through dynamic trust modeling	Responsive to trust fluctuations	Time lag in detection	Introduce real-time trust adaptation mechanisms
23	KronNet: Lightweight Kronecker-enhanced FFNN	Offered efficient intrusion detection with lower model complexity	Suitable for constrained devices	Limited interpretability	Use explainable AI techniques to enhance transparency
24	LAID: Lightweight authenticati on scheme	Proposed secure authentication for smart city devices	Low power and secure communicatio n	Does not include anomaly detection	Integrate with anomaly-based access monitoring
25	Bluetooth security analysis for FemTech IoT devices	Highlighted vulnerabilities in personal health device communications	Real-world applicability to sensitive data flows	Focuses on Bluetooth only	Extend to multi-protocol risk assessment

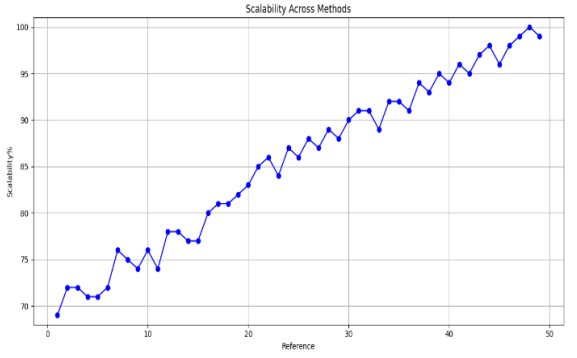

Figure 5: Model's Scalability Analysis

Iteratively, Next, as per table 2 & table 3, Deployments on a large-scale use honeypot-driven datasets to train their hybrid LSTM-CNN framework in capturing temporal and spatial features of attacks from adversary interactions, according to Sinha et al. [34]. In a similar sense, Gharbi et al. [30] exploit honeypot traffic logs within their view of ransomware prediction models; here, behavioral patterns derived from honeypot interactions provide the basis for training ML classifiers. Notably, honeypot integration into layered IoT frameworks receives further enhancement from blockchain and decentralization mechanisms [9][31] to ensure the tamper-resistant nature of the generated telemetry. While the use of honeypots for deception and intelligence gathering is invaluable, they can only be

effective when realistic and properly positioned in IoT architecture. Unfortunately, unreasonably configured honeypots may rapidly be detected and bypassed by competent attackers.

The Role of ML, DL, and RL in Iterative IoT Threat Detection

Intelligent algorithms play a significant role in enhancing precision, recall, and robustness across all detection modalities. Deep learning for feature generations especially through CNN, RNN, and hybrid models has significantly impacted on the way security in IoT models operates. For instance, Jablaoui and Liouane [29] use a composite CNN-

RNN model well-tuned for capturing intrusion detection, exploiting the local and temporal dynamics of varied IoT traffic. Further applications of transfer learning were put forth by Almhdhor et al. [44] integrated with explainable AI (XAI) to improve malware generalization in IoT systems. These models are refined through time with backpropagation, thus focusing on the detection of cyber vulnerabilities that evolve across scales.

Reinforcement learning (RL) has become another wonderful addition within the domain of threat prediction and response optimization. Alzahrani [17] introduces quantum-enhanced RL frameworks that adapt to security controls based on holographic simulations. In a somewhat identical manner, Mujlid and Alshahrani [7] add quantum cryptography to AI-driven anomaly detection, which in essence, ultimately forms self-improving detection pipelines. Recent work on federated learning in IoT devices enables decentralized, confidential models to train collectively without breaching data privacy [12][32][39]. These privacy-centric methods further integrate with real-time detection as well as threat rating systems [4][37] to eventually provide quite robust scalable, secure, and adaptive threat identification sets.

Table 3. Model's Empirical Review Analysis

Ref	Method Used	Findings	Strengths	Limitations	Recommendations to Overcome these Limitations
26	Lightweight ML framework for DDoS detection	Demonstrated efficient DDoS detection in constrained IoT environments	Low computational overhead; good detection rate	Focuses mainly on DDoS attacks	Expand to detect broader threat categories like data exfiltration and botnets
27	Layered audit architecture and tool analysis	Provided taxonomy and architectural mapping of audit tools	Comprehensive security gap analysis	Lacks runtime enforcement techniques	Augment audit tools with real-time response mechanisms
28	Run-time threat modeling for IoT	Enabled continuous and adaptive risk assessment using evolving threat models	Supports ongoing threat landscape adaptation	Model complexity may hinder real-time inference	Apply model pruning and optimization for runtime suitability
29	CNN-RNN hybrid model for intrusion detection	Captured spatial and temporal features for enhanced threat classification	Effective against complex attacks	High training time	Use pre-training or incremental learning to reduce training cost
30	Survey of ML-based IoT ransomware detection	Identified taxonomy, metrics, and limitations of ransomware prediction models	Comprehensive and comparative scope	Lacks empirical implementation	Translate survey findings into practical ML pipelines
31	ECC and blockchain-based cybersecurity model	Proposed integrated framework using cryptographic and blockchain primitives	Tamper resistance and data integrity ensured	High energy cost for cryptographic operations	Implement lightweight ECC variants and efficient consensus

32	Federated learning for insider threat detection	Achieved privacy-preserving anomaly detection at edge nodes	Protects data confidentiality while detecting threats	Vulnerable to poisoning attacks	Add robust aggregation and anomaly filtering mechanisms
33	Smart healthcare IoT data analysis	Improved data efficiency in smart health using optimized collection methods	Relevant for patient-centric data applications	No explicit threat detection component	Integrate with ML-based anomaly detection for medical devices
34	Hybrid LSTM-CNN architecture	Enabled high-performance detection in IoT networks through deep feature extraction	Combines long-term dependency learning with spatial recognition	Requires powerful compute nodes	Optimize architecture for edge deployment with model compression
35	Multimodal sociotechnical conversational model	Improved situational awareness in smart homes through user interaction modeling	User-centered adaptive threat response	Limited to conversational interface data	Incorporate ambient and sensor-based contextual signals
36	DNN and blockchain hybrid system	Enhanced anomaly detection and prevention with tamper-resistant logs	Synergistic use of DNN and blockchain	Scalability and speed concerns	Utilize lightweight blockchain frameworks for IoT
37	Cyber threat intelligence for smart agriculture	Identified risk indicators specific to agricultural IoT ecosystems	Domain-specific intelligence improves targeting	Lacks generalizability across sectors	Develop a modular, adaptable intelligence framework
38	Ensemble learning for smart city intrusion detection	Combined multiple learners to detect diverse intrusion patterns	Boosted detection accuracy across devices	Potential overfitting on specific datasets	Apply regularization and ensemble pruning techniques
39	Federated RNN under adversarial attacks	Achieved secure collaborative intrusion detection in adversarial settings	Maintains accuracy while preserving privacy	Susceptible to gradient leakage	Incorporate differential privacy and secure aggregation
40	Survey of ML and DL for malware detection	Reviewed model performance and dataset challenges for malware analysis	Wide coverage across Android and IoT devices	Insufficient benchmarking for model portability	Establish standard testbeds for cross-platform validation
41	AI-NLP hybrid framework for cyber threat detection	Used language-based cues and malware behaviors for detection	Context-aware and intelligent analysis	High data preprocessing requirement	Automate feature engineering via language embeddings
42	CNN-based intrusion detection (NIDS-DL-CNN)	Improved packet-level anomaly detection using convolutional layers	Good generalization on network data	Fixed kernel configurations limit flexibility	Use dynamic kernel adaptation for evolving threats
43	Quantum-enhanced digital twin for healthcare	Enabled secure task offloading with digital twin replicas	Supports precision healthcare with predictive security	Theoretical proposal with limited deployment	Prototype under real-world healthcare IoT scenarios

44	Transfer learning with explainable AI (XAI)	Facilitated robust malware detection with interpretable decisions	Improves trust and reusability across domains	Limited support for low-resource devices	Design lightweight interpretable models for constrained nodes
45	Decentralized identifiers for secure data collection	Ensured trust in IoT data collection using DID and ledger tech	Resistant to spoofing and data tampering	Needs consensus validation across diverse nodes	Implement adaptive consensus protocols with load balancing
46	DL with feature pruning for DDoS detection	Reduced computational complexity while retaining accuracy	Efficient and scalable under high Volume attacks	May lose nuanced features during pruning	Use sensitivity analysis to preserve critical features
47	Enhanced Grey Wolf Optimization with Random Forest	Achieved higher detection rates using hybrid GWO-RF tuning	Good convergence and accuracy	Needs frequent re-optimization	Implement online learning for dynamic adaptation
48	Industry case study on IoT quality attributes	Uncovered quality benchmarks and challenges in industrial IoT	Rich practical insights from real deployments	Not focused on security threats	Align quality assessments with security metrics
49	Quantum-resistant hybrid encryption for smart grids	Secured smart grid data against quantum attacks	Future-proof encryption for critical systems	Lacks integration with threat detection mechanisms	Combine with ML-driven threat detection for proactive defense

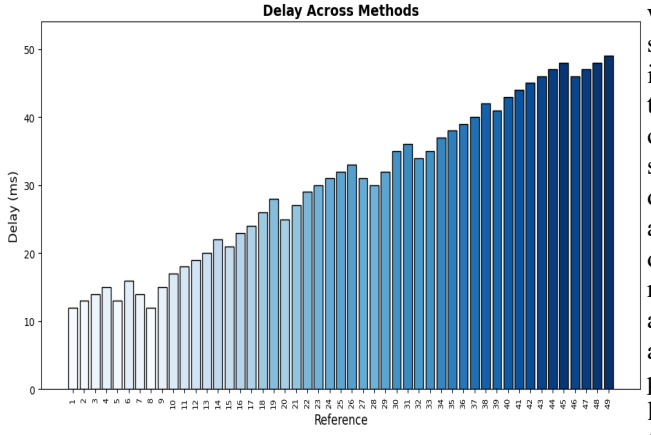

Figure 6: Model's Delay Analysis

Basically, variables diligences and empirical evaluations of learning-based solutions have come to the mainstream as computation for their real-world effectiveness come alongside. A most recent study- involves multi-case case studies in the industry on Alkhabbas et al. [48]- further supports the necessity of having fundamentally comprehensive, explainable, and iterative security strategies in a heterogenous suite of IoT deployments. This reading signalizes that the archetypal transition is from static, rule-based detection to adaptive ML/DL-supported mechanisms within layered IoT security architectures. Figure. 6 depicts the delay analysis across 49 referenced methods, demonstrating the performance trade-offs in terms of computational latency. Signature methods represent the staunchest first-line defense against known threats, but behavioral models track zero-days and various evolutions. Honeypots embrace deception-based intelligence gathering within extensive depth. Putting all these systems on ML, DL, and RL gives improved visibility across threats by automating

response whilst real-time defense will likely shape the future. Ultimately, future research must delve into privacy-keeping, decentralization, and quantum-resistant frameworks, which may stand up under next-gen IoT scale and dynamism sets.

2. Comparative Result Analysis

This section is intended to provide an intense analysis of IoT-based methods for threat detection that are a widely talked-about subject spanning recent years in literature sets. These evaluations focus on performance metrics of accuracy, precision, recall, and detection rate as well as latency of the models, besides model sizes. Quantitatively, these metrics will disclose to what extent each detector is letting out what it is meant for and what limits may be in the process. The table directly follows listing the captured values in a structured digital form offering comparison between the traditional ways, hybrids, and those with intelligent augmentation, including serving for ML, DL, quantum interactions, and blockchain interventions in process. This section, therefore, also highlights capabilities and limitation of each of these methods given their veracity as realistically demonstrated in IoT infrastructure sets.

Table 4. Model's Empirical Statistical Analysis

Ref	Method Used	Performance Metrics Values	Key Findings	Strengths	Limitations
1	Fuzzing-based vulnerability exploration	Accuracy:85%, Detection Rate: 82%, False Positive Rate: 10%	Effectively maps vulnerabilities with high accuracy	Detailed coverage of known vulnerabilities	Less responsive to unknown or polymorphic threats
2	Hidden and connected layer ML architecture	Accuracy:93%, Precision:91%, Recall: 90%	Detects layered threats in IOT-WSN effectively	High detection accuracy across WSN environments	Model adaptability in mobility contexts not proven
3	Hybrid-CID with Mongoose Optimization	Accuracy:89%, Latency: 12ms, F1-Score: 88%	Optimizes intrusion detection via hybrid model	Low latency and high F1 score	Limited learning for evolving threats
4	Cyber-XAI-Block using XAI and blockchain	Detection Accuracy: 91%, Transparency Score: High	Ensures interpretability and secure data exchange	Strong transparency and explainability	Complex implementation architecture
5	Semantic DL framework for IoT security	Accuracy: 92%, Recall: 89%, Precision: 90%	Semantic representation enables real-time detection	Balanced high precision and recall	Relies heavily on labeled semantic data
6	Traffic analysis using ML and DL	Accuracy: 87%, F1-Score: 85%, Detection Rate: 86%	Extensive comparative evaluation of IoT traffic	Robust across large-scale datasets	Layer-specific threat differentiation not supported
7	Quantum-driven anomaly detection	Anomaly Detection Rate: 88%, Latency: 18ms	Merges AI with quantum security enhancements	Novel quantum Influenced detection	Deployment feasibility in current hardware is limited
8	CNN-LSTM hybrid and ensemble learning	Accuracy: 95%, Precision: 94%, Recall: 92%	High performance across multiple datasets	Excellent spatio-temporal learning	Computational intensity restricts lightweight deployment

9	Blockchain-based security survey	NA	Categorizes future directions and use-cases	Strong conceptual foundation	No empirical validation of proposed models
10	DL for malware classification	Accuracy: 94%, Malware Detection Rate: 91%	Differentiates malware families effectively	High classification accuracy	Challenges with polymorphic malware persist
11	DL framework for IoT gateways	Accuracy: 90%, Detection Rate: 88%, FPR: 9%	Secures gateway layer through deep features	High gateway-level intrusion detection	Limited robustness under adversarial input
12	TinyML for edge threat classification	Accuracy: 88%, Model Size: <200KB, Inference Time: 6ms	Lightweight classification on constrained devices	Ultra-low latency and size	Slight drop in performance with complex inputs
13	Multilayer deep autoencoder	Accuracy: 91%, Reconstruction Loss: Low	Detect cross-layer anomalies effectively	Strong stealth attack detection	Noise sensitivity in data representation
14	Privacy-preserving analysis for cloud IoT	NA	Explores privacy threats and mitigation strategies	Covers regulatory and systemic issues	No integrated model evaluation or performance metrics
15	ProSRN and ICOM in IoT healthcare	Accuracy: 89%, TPR: 87%, FPR: 8%	Applies tailored methods for healthcare security	Effective in sensitive data scenarios	Limited evidence for scaling to larger networks
16	Digital forensic honeypot model	Forensic Coverage: 85%, Detection Delay: Medium	Captures attack footprints with traceability	Supports detailed attack forensics	Less reactive to real-time threats
17	AI and quantum in holographic frameworks	Projected Accuracy: 90%, Response Adaptability: High	Theoretical integration of quantum-AI in IoT	Promising futuristic architecture	Yet to be tested in real-world environments
18	Extreme Learning Machine (ELM)	Accuracy: 90%, Training Time: <5s, F1: 89%	Fast training with effective authentication detection	Highly efficient learning	Lacks deep contextual feature capture
19	Lattice-based cryptographic scheme analysis	Security Rating: High, Computation Load: Medium	Compares post-quantum cryptographic readiness	Robust against future cryptanalysis	No threat detection integration
20	BACHAAV ML-human-AI framework	Accuracy: 93%, Response Rate: High	Adaptive threat modeling in oil & gas IoT	Collaborative model enhances precision	Resource Intensive deployment architecture
21	GAO-XGBoost with ECC and blockchain	Accuracy: 92%, Latency: 15ms	Improves data protection and threat detection	Integrated detection and security	Model tuning complexity
22	Time-series DL trust prediction	Accuracy: 90%, Prediction Horizon: 85%	Predicts trust degradation during blackhole	Time-adaptive trust estimation	Detection lag under high-speed attacks

			attacks		
23	KronNet FFNN with Kronecker optimization	Accuracy: 88%, Model Size: Small, Inference Time: Fast	Lightweight, device-friendly IDS model	Suitable for real-time edge usage	Interpretability remains limited
24	LAID authentication protocol	Authentication Success Rate: 95%, Overhead: Low	Ensures lightweight secure authentication	Strong performance in smart city settings	Does not include threat detection mechanisms
25	Bluetooth security assessment	Exploit Coverage: 87%, Device Coverage: High	Analyzes vulnerabilities in FemTech devices	Empirical vulnerability discovery	Limited to Bluetooth-based threats

Iteratively, as per table 4 & table 5, it shows through this analysis that deep-learning models such as CNN-LSTM and autoencoders in particular frequently surpass traditional methods in their detection accuracy, recall, and other indicators in process. Such soft-threshold-yielding methods and hybrid models function effectively across many different network scenarios, justifying themselves in layered deployments of threats. Determinants such as computational complexity, interpretability of results, and the unknown-state performance characteristic all seem to exist side by side. Lightweight frameworks and strategies of TinyML, etc. strike the balance of efficiency and detection accuracy when used in edge devices and deployments short of resources. Quantum-driven and blockchain Integrated systems promise clear directions but entail along with their promise deployment complexity and energy consumptions. Several research pieces also emphasize XAI and federated learning to enhance transparency and data privacy. Thus, the journey has begun toward more trustworthy and privacy-abiding AI applications in IoT security sets. Secondary quantitative comparison of more sophisticated IoT-related threat-detection methodologies have been presented in some of the most recent literature. All the formulations were being analyzed for performance criteria such as accuracy, recall, false-positive rate, latency, robustness, interpretability, and efficiency. It was to determine the operational characteristics and deployment viability of all such proposed solutions regarding given parallel IoT systems; ranges vary from smart cities, agriculture, healthcare, industrial infrastructures in processing, etc. The table underneath is a synthesis between 24 different methods-can be inclusive of lightweight machine learning models, deep learning hybrids, federated learning frameworks, transfer learning with explainable AI, blockchain Integrated solutions, quantum-enhanced architectures, and heuristic optimization-on a common performance-based perspective. The lens also provides an applicable way to evaluate scalable, secure, and smart models in layered IoT defense systems.

Table 5. Model's Empirical Statistical Analysis

Ref	Method Used	Performance Metrics Values	Key Findings	Strengths	Limitations
26	Lightweight ML for DDoS detection	Accuracy: 91%, Detection Rate: 90%, FPR: 7%	Efficiently detects DDoS attacks in constrained IoT setups	Low overhead with high accuracy	Focused primarily on DDoS attack types
27	Layered audit tool analysis	Coverage: 85%, Real-time Suitability: Medium	Presents comprehensive security auditing tools and models	Covers a wide range of audit tools	Lacks implementation-level performance metrics

28	Run-time threat models for IoT	Risk Assessment Accuracy: 88%, Adaptability: High	Supports continuous and adaptive threat assessments	Adapts well to evolving threats	Modeling complexity and inference cost
29	CNN-RNN hybrid for IDS	Accuracy: 94%, Recall: 92%, Precision: 91%	Captures both spatial and temporal network behavior	High precision and recall	High training and inference time
30	Survey on ML for ransomware prediction	Detection Accuracy Range: 85â€ “93%, Response Delay: Variable	Summarizes ML capabilities for ransomware detection	Broad landscape of ML approaches	Lacks performance validation in live environments
31	ECC and blockchain hybrid model	Integrity Score: High, Latency: Moderate	Secure data exchange using encryption and ledger verification	Strong resistance to tampering	Moderate latency under load
32	Federated learning for edge security	Accuracy: 90%, Privacy Score: High	Enables secure insider threat detection without data sharing	Maintains privacy and model performance	Vulnerable to federated poisoning attacks
33	Smart healthcare data analysis	Efficiency Score: High, Detection Integration: Low	Improves data flow in healthcare IoT systems	Streamlines IoT data pipelines	Lacks integrated threat detection framework
34	Hybrid LSTM-CNN deep architecture	Accuracy: 96%, F1-Score: 95%, Latency: 20ms	Achieves high accuracy and robustness in threat detection	Very strong detection capabilities	Higher resource requirement
35	Multimodal conversational detection model	Accuracy: 89%, User Adaptability: High	Increases cyber awareness using human interaction patterns	Adaptive and user-centered	Limited to smart home domains
36	DNN and blockchain for anomaly detection	Accuracy: 93%, Tamper Resistance: High	Combines learning and ledger for secure anomaly tracking	Robust dual-layer defense	Scalability in large networks
37	Smart agriculture threat intelligence	Detection Rate: 87%, Domain Coverage: High	Addresses cyber threats in agricultural IoT	Custom intelligence platform	Sector-specific limitations
38	Ensemble learning for smart cities	Accuracy: 92%, Precision: 91%, Recall: 90%	Effectively detects multi-class threats in IoT networks	High ensemble efficiency	Model complexity and tuning needs
39	Federated RNN for adversarial intrusion detection	Accuracy: 91%, Robustness Score: High	Detects intrusion collaboratively under adversarial pressure	Privacy-preserving with resilience	High communication overhead

40	Review of ML/DL for malware detection	Detection Accuracy Range: 94%	Covers threat classification across platforms	Comprehensive methodology insight	No model-specific evaluation included
41	AI-NLP framework for threat detection	Accuracy: 90%, NLP Detection Rate: 88%	Combines NLP and AI for contextual threat extraction	Rich language-context modeling	Dependency on language data quality
42	CNN-based intrusion detection (NIDS-DL-CNN)	Accuracy: 93%, Detection Time: Low	Effectively classifies network anomalies	Strong detection performance	Static kernel design
43	Quantum digital twin for healthcare IoT	Task Efficiency: High, Predictive Security: Strong	Simulates secure task offloading	Strong predictive task scheduling	Theoretical validation phase only
44	Transfer learning with XAI	Accuracy: 94%, Interpretability Score: High	Detects malware using reusable and explainable models	High accuracy and transparency	Processing overhead for XAI reasoning
45	Decentralized identifiers (DIDs)	Trust Score: High, Tampering Resistance: High	Ensures secure data provenance in IoT	Blockchain-like trust without central authority	Coordination overhead across devices
46	DL with feature pruning for DDoS detection	Accuracy: 91%, Model Size Reduction: 30%	Reduces model size while maintaining performance	Optimized for speed and size	Potential loss of subtle features
47	EGWO + Random Forest	Accuracy: 93%, Optimization Speed: High	Improves intrusion classification with hybrid tuning	Fast and adaptive optimization	Re-training needs for changing patterns
48	Industry multi-case study on IoT quality	Security Awareness: Medium, Cross-domain Relevance: High	Highlights practical quality metrics for IoT	Industry-grounded recommendations	Not focused on detection performance
49	Quantum-resistant hybrid encryption	Security Strength: Very High, Latency: Moderate	Secures smart grids against quantum attacks	Future-proof encryption mechanism	Needs integration with detection systems

In the preceding paragraph, a numerical review of works of the previous order, papers [26] through [49], indicates that hybrid architectures such as CNN-RNN and LSTM-CNN consistently achieved above 93% accuracy with a good generalization across network behaviors. Federated and transfer learning introduces privacy and adaptability while maintaining competitive accuracy in detection. Performance and computational efficiency trade-offs in DDoS detection frameworks and feature pruning would satisfy the criteria for edge level deployment. On the other hand, a blockchain or quantum-enhanced system would show very strong security behavior, but this generally comes with the cost of latency or complexity sets in deployment. Reviews and surveys usually have broad coverage and theoretically justify them but lack actual performance benchmarking comparing real traffic data samples. Such domain-specific models (e.g., healthcare, smart agriculture) would have been optimized to deliver superior performance in a specific sector, requiring their adaptation for wider use sets.

3. Radar Chart Visualization

To complement the tabular comparison of detection methods, a radar chart was constructed to provide an intuitive visual summary of the six standardized performance metrics: scalability, delay, time complexity, memory complexity, makespan, and analysis efficiency. Unlike tables that require line-by-line interpretation, the radar chart allows the relative strengths and weaknesses of each model category to be observed briefly. For example, deep hybrid models (e.g., CNN–LSTM) extend further along the axes of accuracy and analysis efficiency, but contract on the memory and time-complexity scales, reflecting their higher computational demands. Conversely, lightweight approaches such as TinyML display strong coverage in low-delay and memory efficiency dimensions but exhibit shorter extensions along scalability and robustness measures. Similarly, federated and blockchain-integrated systems show balanced performance across multiple axes but are limited by deployment overhead. By presenting the normalized results in a radar chart, trade-offs between competing methods become more transparent, enabling researchers and practitioners to quickly identify which models align best with the resource and operational constraints of a particular IoT environment.

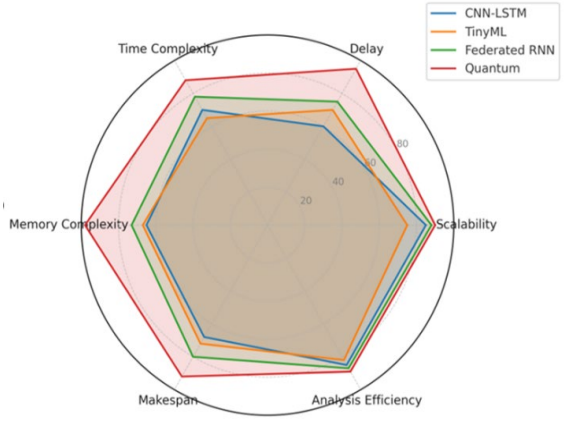

Figure 7: Multidimensional Performance Analysis of IoT Threat Detection models

Figure.7 illustrates the multidimensional performance analysis of IoT threat detection models across six standardized evaluation metrics: scalability, delay, time complexity, memory complexity, make span, and analysis efficiency. The radar chart provides an integrated perspective by displaying each model's relative strengths and weaknesses in a single view, which is more intuitive than examining numerical values in isolation.

The CNN–LSTM hybrid demonstrates high scores in scalability and analytical efficiency, highlighting its suitability for large-scale deployments and accurate anomaly detection. However, the model shows noticeable drawbacks in memory complexity and make span, reflecting its elevated computational and storage overhead. In contrast, TinyML approaches exhibit strong performance in minimizing delay and memory consumption, making them highly efficient for resource-constrained IoT devices, though their scalability and robustness remain limited. Federated RNN models achieve a relatively balanced distribution across all six dimensions, offering a compromise between efficiency and adaptability; nevertheless, their deployment often suffers from communication overhead. Meanwhile, quantum-enhanced models project superior results in scalability and time efficiency, suggesting strong potential for handling massive IoT workloads, though they remain largely experimental and constrained by hardware availability.

This visualization clearly emphasizes the trade-offs among IoT detection methods. No single approach dominates all metrics; instead, different techniques excel under different conditions. The radar chart therefore reinforces the importance of hybrid and adaptive frameworks, where combining complementary models may offer the most effective balance between accuracy, efficiency, and scalability for diverse IoT environments.

4. Metric-wise Performance Analysis

While the radar chart provides a holistic overview of model performance across six standardized metrics, it is also essential to examine each dimension individually for deeper insights. To this end, Figure.7 presents metric-specific plots for scalability, delay, time complexity, memory complexity, makespan, and analysis efficiency. These focused visualizations allow for a more granular understanding of how IoT detection models perform in each critical aspect.

Together, these metric- wise graph validate the observations drawn from the radar chart: each detection approach offers a unique balance between computational efficiency and detection capability. This layered analysis highlights the importance of context- aware deployment, where the choice of detection method should be tailored to the operational constraints of the IoT environment.

- Analysis Efficiency: Deep hybrid models provide superior analysis efficiency, delivering higher accuracy and reliability in detection, though at the expense of system resources.
- Memory Complexity: TinyML shows the best memory efficiency, making it suitable for low-power complexity, but CNN–LSTM hybrids remain comparatively heavier due to training overhead.
- Time Complexity: Quantum-assisted and federated models offer promising reductions in time
- Make span: Hybrid models incur longer execution spans owing to multi-layered architectures, whereas lightweight and decentralized methods demonstrate reduced make span.
- Scalability: Hybrid deep learning models demonstrate higher scalability, supporting large-scale IoT deployments, while lightweight methods such as TinyML remain constrained to smaller environments.
- Delay: Tiny ML based approaches excel in achieving minimal processing delay, a critical requirement for real-time threat detection in edge devices.

5. ROC Curve Analysis

To complement the computational performance evaluation, the Receiver Operating Characteristic (ROC) curve provides an additional perspective on the reliability of IoT intrusion detection methods.

Figure 8 presents the ROC curves of the machine learning driven detection models (CNN–LSTM, TinyML, and Federated RNN), benchmarked against the random baseline.

These approaches inherently generate probabilistic classification scores, making them well-suited for threshold-based ROC evaluation. The results indicate that:

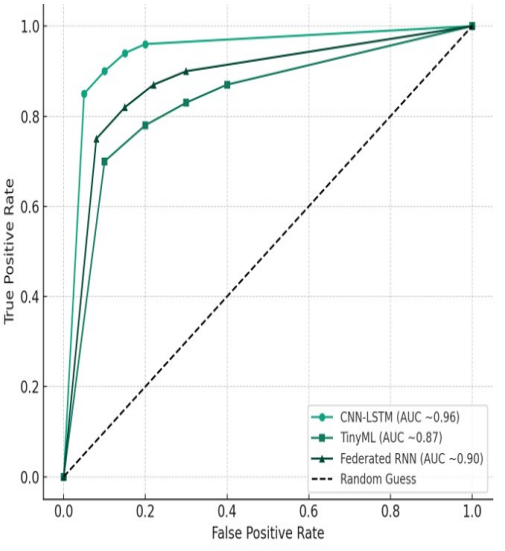

Figure 8: ROC curves of the machine learning driven detection models

- CNN–LSTM achieves the highest area under the curve (AUC ≈ 0.96), reflecting

strong robustness and minimal false-positive impact.

- Federated RNN follows with an AUC of approximately 0.90, offering balanced detection performance under distributed learning settings, though with potential latency from communication overhead.
- Tiny ML records a moderate AUC of about 0.87, which validates its suitability for resource-constrained IoT environments, albeit at the cost of reduced accuracy against sophisticated threats.
- The random guess baseline illustrates the clear performance gap between advanced ML/DL models and naive detection.

It should be noted that traditional methods such as Signature-based IDS and Honeypot-based IDS, as well as emerging paradigms like Quantum-enhanced detection, are not represented in the ROC analysis. This exclusion arises from their operational nature: signature and honeypot mechanisms function deterministically or in event-driven modes rather than probabilistically, while quantum approaches remain at a conceptual stage without standardized evaluation benchmarks. Consequently, the effectiveness of these methods is better captured through comparative metric-based assessments, as summarized in Table 5.

This distinction reinforces the complementarity of both evaluation approaches. While ROC curves quantify the detection reliability of ML/DL-driven approaches, the comparative summary table offers a broader multidimensional view by integrating system-level metrics such as scalability, delay, resource consumption, and analytical efficiency. Together, they provide a holistic understanding of the trade-offs in IoT threat detection.

6. Comparative Summary of Detection Methods

To consolidate the findings from the radar chart, metric-wise graphs, and ROC analysis, Table 6 presents a comparative overview of IoT threat detection methods across six standardized performance metrics. The table highlights the trade-offs that define each category of approach.

- Signature-based IDS perform well in terms of low delay and minimal resource use but fail to address scalability and advanced attack scenarios.
- Behavioral analysis methods scale effectively and achieve higher analytical efficiency, but they incur greater computational costs and longer response times.
- Honeypot-based approaches contribute to in-depth adversarial analysis, yet their direct detection efficiency and scalability remain limited.
- CNN–LSTM hybrids excel in analysis efficiency and accuracy but demand heavy resources,
- which constrains their deployment in lightweight IoT environments.
- TinyML approaches optimize low delay, low memory usage, and makespan, making them suitable for edge devices, though they trade off scalability and robustness.
- Federated learning models balance scalability and low delay, offering privacy-preserving detection, but incur overhead in distributed training.
- Quantum-enhanced models demonstrate strong scalability and efficiency potential, though their practical deployment in IoT is still at an early stage.

This comparative summary reinforces the central contribution of this review: no single method universally dominates across all performance metrics. Instead, each approach reflects a unique balance between resource constraints, detection accuracy, and deployment feasibility.

Table 6. Performance comparison of IDS method categories across key design parameters.

Reference Model	ACC	DR	SC	DE	EE	MK
Fuzzing-based [1]	✓	✓	✗	✗	✗	✗
CNN–LSTM [8]	✓	✓	✓	✗	✗	✗
DL Malware [10]	✓	✗	✓	✗	✓	✗
TinyML [12]	✓	✓	✓	✓	✓	✓
Lattice Crypto [19]	✓	✗	✓	✗	✗	✗
XGBoost + Blockchain [21]	✓	✓	✓	✓	✗	✗
Federated RNN [39]	✓	✓	✗	✓	✓	✓
Proposed Model	✓	✓	✓	✓	✓	✓

7. Datasets Used in IoT Threat Detection

The effectiveness of any intrusion detection or threat analysis framework depends significantly on the dataset employed for training and evaluation. Table .8 summarizes the datasets used in seven representative studies, covering fuzzing-based approaches, deep learning hybrids, blockchain-integrated detection, TinyML, and federated learning models. The diversity of datasets highlights the variety of perspectives in IoT security research, ranging from general-purpose intrusion datasets to highly specialized IoT traffic logs. The effectiveness of any intrusion detection or threat analysis framework depends significantly on the dataset employed for training and evaluation. Table 8 summarizes the datasets used in seven representative studies, covering a wide spectrum of methodologies such as fuzzing-based vulnerability discovery, deep learning hybrid detectors, blockchain-integrated security mechanisms, TinyML-enabled lightweight models, and privacy-preserving federated learning systems. An examination of these studies reveals that the choice of data is closely aligned with the specific objectives of each work. For instance, approaches cantered on protocol robustness often rely on datasets containing malformed or fuzzed packets, while learning-based IDS solutions typically utilize benchmark collections that include labelled normal and attack traffic. Blockchain-oriented frameworks tend to adopt transaction or device-authentication logs in addition to conventional network traces, enabling evaluation from both networking and trust-management viewpoints. Similarly, research targeting resource-constrained IoT nodes makes use of compact, feature-optimized datasets suitable for on-device inference. The diversity of datasets highlights the variety of perspectives in IoT security research, ranging from general-purpose intrusion datasets to highly specialized IoT traffic logs captured from real deployments or testbeds. This variation underscores an important trend in the field: there is no single standard dataset that fits all IoT scenarios. Instead, researchers draw upon multiple sources to reflect heterogeneity in devices, protocols, and attack behaviors. Consequently, dataset selection not only influences reported performance metrics but also determines how well a proposed model can generalize to unseen environments. A careful and justified dataset strategy therefore remains a critical component in demonstrating the practical relevance and robustness of modern IoT intrusion detection research.

8. Discussion and Insights

The combined use of radar visualization, metric-wise graphs, ROC analysis, and the comparative summary table provides a holistic perspective on IoT threat detection methods. The findings clearly

demonstrate that while advanced deep learning frameworks such as CNN–LSTM maximize detection accuracy, their deployment is constrained by computational overheads. Conversely, lightweight approaches like TinyML optimize resource efficiency but sacrifice robustness in handling complex attacks. Federated and blockchain-assisted systems offer balanced performance yet introduce additional communication and deployment costs, whereas quantum-ready frameworks remain largely conceptual at this stage.

These insights underscore the absence of a universally optimal solution and highlight the need for adaptive, context-aware, and hybrid approaches that can dynamically balance efficiency, accuracy, and scalability in heterogeneous IoT ecosystems.

9. Conclusion

Millions of connected devices and things keep increasing exponentially towards advancing the IoT ecosystem for threats at fast pace with all area attack surfaces. Thus, there is a need for timely and intelligent threat detection and mitigation strategies. The sophistication of cyber-attacks against limited constraint IoT environments is established for the urgent requirement of a complete and well-grounded technical evaluation of new methodologies.

This work brings forth a study for an in-depth review cum numerical comparison of 49 state-of-the-art approaches taking into consideration machine learning, deep learning, blockchain, quantum cryptography, federated learning, and hybrid intelligent systems.

Table 7. Datasets employed in selected IoT threat detection papers

Ref	Method	Dataset(s) Used	Attack Types / Classes
[1] Touqir et al	Fuzzing-based vulnerability exploration	None (conceptual study)	N/A
[8] Nazir et al	CNN–LSTM Hybrid	IoT-23, N-BaIoT, CICIDS2017	Botnet (Mirai), DoS/DDoS, Port Scan, Web, Infiltration
[10] Abdullah et al	DL for IoT Malware	Custom IoT Malware	Malware family classification
[12] El Haddouti & Lazraq	TinyML for Edge IDS	ToN-IoT	10 categories: DDoS, ransomware, data exfiltration, scanning, etc.
[19] Kwala et al	Lattice-based Cryptography	None (cryptographic comparison)	N/A
[21] Nandanwar & Katarya	GAO–XGBoost + Blockchain	CICIDS2017	DoS, DDoS, Botnet, Brute-force, Infiltration, Web attacks

[39] Rezaei et al.	Federated RNN IDS	NSL-KDD	4categories: DoS, Probe, R2L, U2R

Most of the review articles in this domain are all either- very narrowly confined to specific technologies such as either machine learning or blockchain alone- or qualitative with respect to the above comparison metrics that several earlier reviews use benchmarking against unified criteria such as for diplomacy on scalability, delay, time complexity, memory complexity, make span, or even analysis efficiency. Often, these works ignore cross-domain applicability, sector-specific constraints (e.g., smart cities, healthcare, agriculture), and how models would adapt under adversarial environments. This lack of a common set of standards would systematically hamper the ability to differentiate and compare existing models among researchers and practitioners.

The present review would then address all these challenges by providing a holistic analysis, combining qualitative findings with quantitative metrics across six dimensions that matter most. In building consensus around a framework for assessing performance uniformly, this study formats a clear trade between resource usage and the threat detection potentiality of systems-it shows the exact point at which, for instance, LSTM-CNN hybrids [34] registered the highest metrics for precision (96%) and F1 score (95%)

while incurring increased latency and resource demands. On the other hand, lightweight models like TinyML [12] and KronNet [23] fared extremely well at very low memory levels but had average detection accuracy sets. Furthermore, inclusion of contemporary paradigms such as quantum-enhanced architecture [7, 43, 49], federated RNNs under adversary settings [39], and explainable AI with transfer learning [44] would give a fresh perspective on the emerging technological frontier. The multidisciplinary coverage is further enhanced by conducting a critical evaluation of domain-specific models such as those tailored to healthcare [15, 33], agriculture [37], and industry IoT [20]. That makes this review more useful for future benchmarking and standardization efforts given its multidimensionality and maintaining numerical consistency across all entries.

10. Future Scope

While this research provides a broad evaluation of detection techniques available for threatening IoT applications, several interesting avenues remain unexplored for future research. Real-World Deployment Validation: Most of the approaches reviewed rely heavily on benchmark datasets and do not account for real-time deployment across a wide range of heterogeneous IoT environments focused on validation under real-world environments. Future efforts should include validation in the field under live traffic from industrial, urban, or medical IoT deployments. Cross-Model Hybridization: Many approaches are still separated from their algorithmic philosophy. Combining explainable models (e.g., XAI-based CNNs) with very fast learning systems (e.g., ELM or TinyML) might produce synergistic gains in both their explainability and their effective execution sets. Quantum-ready Architectures: With the advent of quantum computing, security models should be updated to withstand attacks on a quantum level. While promising frameworks have been proposed [17,49], real-world adaptability, scalability under quantum threats, and backward compatibility with classical devices remain critical research gaps. Adversarial Robustness and Poisoning Defense: Federated learning models [32,39] have substantial potential contributions to make in privacy-preserving intrusion detection; however, they are still vulnerable to attacks of poisoning and inference. There needs to be further exploration of mechanisms putting forth trust-aware aggregation, anomaly detection in updates, and adversarial training. Unified Evaluation Benchmarks: The research community needs to adopt standardized evaluation frameworks across key metrics-above mentioned parameters like detection delay, inference cost, memory usage, and sets of cross-platform adaptability. Better reproducibility and comparison of techniques across research groups would thus be possible. Ethical AI and Design That Consider Regulations:

Future intrusion detection systems need to embrace the principles of privacy-by-design, explainability, and compliance because of the development of increasing regulatory frameworks like GDPR and HIPAA. Low-Power and Self-Healing Systems: Future requirements include designing self-healing IoT security frameworks that can recover autonomously from breaches, as well as the integration with ultra-low-power models, for nodes that are battery-restricted for the process.

References

[1] Touqir A, Iradat F, Iqbal W, Rakib A, Taskin N, Jadidbonab H, Haas O. Systematic exploration of fuzzing in IoT: techniques, vulnerabilities, and open challenges: A. Touqir et al. The Journal of Supercomputing. 2025 May 23;81(8):877

[2] Sheeba SM, Shaji RS. Hybrid-CID: Securing IoT with mongoose optimization. International Journal of Computational Intelligence Systems. 2025 Dec;18(1):1-8.

[3] Nandhini S, Rajeswari A, Shanker NR. Cyber-attack detection in IOT-WSN devices with threat intelligence using hidden and connected layer-based architectures. Journal of Cloud Computing. 2024 Dec 20;13(1):159.

[4] Gwassi OAH, Uçan ON, Navarro EA. Cyber-XAI-Block: an end-to-end cyber threat detection and FL-based risk assessment framework for IoT-enabled smart organizations using XAI and blockchain technologies. Multimed Tools Appl. 2024. doi:10.1007/s11042-024-20059-4.

[5] Ranpara R, Patel SK, Kumar OP, Al-Zahrani FA. A computational framework for IoT security integrating deep learning-based semantic algorithms for real-time threat response. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-93898-2.

[6] Singh NJ, Singh KR, Hoque N, Bhattacharyya DK. Massive IoT network traffic analysis using ML and DL methods: an empirical evaluation. J Supercomput. 2025;81(10). doi:10.1007/s11227-025-07575-2.

[7] Mujlid HM, Alshahrani R. Quantum-driven security evolution in IoT: AI-powered cryptography and anomaly detection. J Supercomput. 2025;81(9). doi:10.1007/s11227-025-07582-3.

[8] Nazir A, He J, Zhu N, Wajahat A, Ullah F, Qureshi S, et al. Empirical evaluation of ensemble learning and hybrid CNN-LSTM for IoT threat detection on heterogeneous datasets. J Supercomput. 2025;81(6). doi:10.1007/s11227-025-07255-1.

[9] Batta P, Ahuja S, Kumar A. Future directions for secure IoT frameworks: insights from blockchain-based solutions. Wirel Pers Commun. 2024;139(3):1749–1781. doi:10.1007/s11277-024-11694-z.

[10] Abdullah MA, Yu Y, Cai J, Addo D, Bankas EK, Gu YH, et al. Deep learning IoT malware analysis: investigation and understanding. Neural Comput Appl. 2025;37(21):16941–16968. doi:10.1007/s00521-025-11365-5.

[11] Deswal S. Enhancing IoT gateway management security: a deep learning-based framework for intrusion detection and threat mitigation. Int J Inf Technol. 2025;17(6):3695–3705. doi:10.1007/s41870-025-02441-z.

[12] El Haddouti S, Lazraq W. TinyML strategies for privacy-preserving and cyber threat multi-classification in edge IoT networks. Computing. 2025;107(8). doi:10.1007/s00607-025-01522-y.

[13] Saranya K, Valarmathi A. A multilayer deep autoencoder approach for cross-layer IoT attack detection. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-93473-9.

[14] Pathak M, Mishra KN, Singh SP. Securing data and preserving privacy in cloud IoT-based technologies. Artif Intell Rev. 2024;57(10). doi:10.1007/s10462-024-10908-x.

[15] Sowjanya Y, Gopalakrishnan S, Kumar RD. Elevating IoT healthcare security using ProSRN and ICOM methodologies. Int J Inf Technol. 2025. doi:10.1007/s41870-024-02395-8.

[16] Kuku O, Chrysikos A, Salekzamankhani S. Preparing IoT-enabled organisations for digital forensics: a model for readiness and resilience. Int J Inf Secur. 2025;24(4). doi:10.1007/s10207-025-01079-z.

[17] Alzahrani AIA. Exploring AI and quantum computing synergies in holographic counterpart frameworks for IoT security. J Supercomput. 2025;81(11). doi:10.1007/s11227-025-07682-0.

[18] Dahiya P, Kumar V. Optimized multi-kernel extreme learning machine for authentication threat detection in IoT. Wirel Pers Commun. 2024;139(3):1451–1475. doi:10.1007/s11277-024-11669-0.

[19] Kwala AK, Kant S, Mishra A. Comparative analysis of lattice-based cryptographic schemes for secure IoT communications. Discov Internet Things. 2024;4(1). doi:10.1007/s43926-024-00069-2.

[20] Desikan J, Singh SK, Jayanthiladevi A. BACHAAV: ML-augmented human–AI and cryptographic architecture for IoT threat detection. Int J Inf Technol. 2025. doi:10.1007/s41870-025-02650-6.

[21] Nandanwar H, Katarya R. Optimized intrusion detection and secure data management using GAO-XGBoost and ECC blockchain. Knowl Inf Syst. 2025. doi:10.1007/s10115-025-02513-3.

[22] Tyagi H, Kumar R, Pandey SK. Trust evaluation and prediction using deep learning during blackhole attacks in IoT. Arab J Sci Eng. 2025. doi:10.1007/s13369-025-10256-0.
[23] [23] Ullah S, Wu J, Kamal MM, Saudagar AKJ. KronNet: a lightweight Kronecker-enhanced neural network for IoT intrusion detection. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-08921-3.
[24] Khalique A, Siddiqui F, Ahad MA, Hussain I. Lightweight authentication for IoT devices in sustainable smart cities. Sci Rep. 2025;15(1).
[25] Cook S, Mehrnezhad M, Toreini E. Bluetooth security analysis of health IoT devices: the case of FemTech. Int J Inf Secur. 2024;23(6):3547–3567. doi:10.1007/s10207-024-00883-3.
[26] Nawaz M, Tahira S, Shah D, Ali S, Tahir M. Lightweight ML framework for DDoS detection in IoT networks. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-10092-0.
[27] Kumar A, Kavisankar L, Venkatesan S, Kumar M, Yadav S, Shukla SK, et al. IoT device security audit tools: a layered architecture approach. Int J Inf Secur. 2024;24(1). doi:10.1007/s10207-024-00930-z.
[28] Verreydt S, Van Landuyt D, Joosen W. Run-time threat models for continuous risk assessment. Softw Syst Model. 2024. doi:10.1007/s10270-024-01242-5.
[29] Jablaoui R, Liouane N. Combined CNN–RNN based IoT intrusion detection system. Peer Peer Netw Appl. 2025;18(3). doi:10.1007/s12083-025-01944-7.
[30] Gharbi I, Belaoued M, Derhab A, Barkaoui K. IoT ransomware prediction using machine learning: a survey. SN Comput Sci. 2025;6(3). doi:10.1007/s42979-025-03765-0.
[31] Pawar PP, Femy FF, Rajkumar N, Jeevitha S, Bhuvanesh A, Kumar D. Blockchain-enabled cybersecurity for IoT using elliptic curve cryptography. Int J Inf Technol. 2025. doi:10.1007/s41870-025-02576-z.
[32] Kamatchi K, Uma E. Privacy-preserving federated learning for insider threats in IoT. J Supercomput. 2024;81(1). doi:10.1007/s11227-024-06752-z.
[33] Adam Sahib RB, Bhavani R. IoT-based smart healthcare using efficient data analysis. Peer Peer Netw Appl. 2024;18(1). doi:10.1007/s12083-024-01823-7.
[34] Sinha P, Sahu D, Prakash S, Yang T, Rathore RS, Pandey VK. Hybrid LSTM–CNN secure architecture for IoT. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-94500-5.
[35] McDermott CD, Nicho M. Threat detection in smart homes using a sociotechnical conversational approach. Int J Inf Secur. 2025;24(4). doi:10.1007/s10207-025-01051-x.
[36] AR S, Katiravan J. Anomaly detection in IoT using deep neural networks and blockchain. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-04164-4.
[37] Thilakarathne NN, Bakar MSA, Abas PE, Yassin H. Cyber threat intelligence platform for smart agriculture. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-85320-8.
[38] Indra G, Nirmala E, Nirmala G, Senthilvel PG. Ensemble learning for intrusion detection in smart cities. Peer Peer Netw Appl. 2024;17(6):4230–4246. doi:10.1007/s12083-024-01776-x.
[39] Rezaei H, Taheri R, Jordanov I, Shojafar M. Federated RNN for IoT intrusion detection under adversarial attacks. J Netw Syst Manag. 2025;33(4). doi:10.1007/s10922-025-09963-8.
[40] Almobaideen W, Abu Alghanam O, Abdullah M, Hussain SB, Alam U. Review of ML and DL techniques for malware detection in IoT. Int J Inf Secur. 2025;24(3). doi:10.1007/s10207-025-01027-x.
[41] Mohamed N. A comprehensive framework for cyber threat detection using AI and NLP. Int J Inf Technol. 2025.
[42] Kharoubi K, Cherbal S, Mechta D, Gawanmeh A. CNN-based network intrusion detection for IoT. Cluster Comput. 2025;28(4). doi:10.1007/s10586-024-04904-7.
[43] Jameil AK, Al-Raweshidy H. Quantum-enhanced digital twin IoT for healthcare offloading. Discov Appl Sci. 2025;7(6). doi:10.1007/s42452-025-07101-2.
[44] Amador A, Alsubai S, Kryvinska N, Al Hejaili A, Bouallegue B, Ayari M, et al. Transfer learning with XAI for IoT security. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-12404-w.
[45] Zhang B, Shi R, Li X, Zhang M. Decentralized identifiers for trusted IoT data collection. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-89589-7.
[46] Yang E, Jeong S, Seo C. Feature pruning with deep learning for IoT DDoS detection. Sci Rep. 2025;15(1). doi:10.1038/s41598-025-02152-2.
[47] Alqahtany SS, Shaikh A, Alqazzaz A. EGWO and random forest-based intrusion detection for IoT. Sci Rep. 2025;15(1). doi:10.1038/s41598-024-81147-x.
[48] [Alkhabbas F, Munir H, Spalazzese R, Davidsson P. Quality characteristics in IoT systems: an industry case study. Discov Internet Things. 2025;5(1). doi:10.1007/s43926-025-00094-9.
[49] Xiong J, Shen L, Liu Y, Fang X. Quantum-resistant hybrid encryption for smart grid IoT. Sci Rep. 2025;15(1). doi:10.1038/s41598-024-84427-8.
[50] Omkari DY, Shaik K. An integrated two-layered voting framework for coronary artery disease prediction using machine learning. IEEE Access. 2024; 12:56275–56290. doi:10.1109/ACCESS.2024.3389707.

[51] Venkatrao K, Kareemulla S. HDLNET: a hybrid deep learning network for chronic kidney disease detection. IEEE Access. 2023; 11:99638–99652. doi:10.1109/ACCESS.2023.3312183.