Volume 10, Issue 3, July 2023 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

# Advancements in AI for IoT Security: Review of Intrusion Detection Methods

**Rohan Rajoriya**
*Lecturer (IT),*
*Kalaniketan Polytechnic College*
*Jabalpur (M.P.), India*
*Email: rohanrajoriya@gmail.com*

**Rupesh Kumar Dharne**
*Lecturer (IT),*
*Kalaniketan Polytechnic College*
*Jabalpur (M.P.), India*
*Email: rk.dharne@gmail.com*

## ABSTRACT

*The rapid proliferation of IoT devices has introduced significant cybersecurity challenges, necessitating advanced intrusion detection systems (IDS) powered by artificial intelligence (AI). This review paper systematically examines AI-driven IDS for IoT, focusing on machine learning (ML) and deep learning (DL) techniques. We analyze various peer-reviewed studies to identify trends, datasets, and performance metrics. Key findings reveal that ensemble methods (e.g., XGBoost) and lightweight DL models (e.g., autoencoders, TinyML) achieve high detection accuracy (>95%) while addressing IoT resource constraints. However, challenges such as adversarial attacks, data imbalance, and scalability gaps persist. Emerging solutions like federated learning (FL) and edge AI show promise for privacy-preserving, real-time threat detection. This paper also highlights the lack of standardized IoT-specific datasets and calls for explainable AI (XAI) to enhance trust in autonomous IDS. Future research directions include quantum ML, blockchain-integrated IDS, and self-learning systems for adaptive security. By synthesizing current advancements and open issues even with industrial perception of IoT , this review provides a roadmap for next-generation AI-powered IoT security.*

***Keywords:—*** *AI, ML, IoT Security, IDS, IEEE Standards*

## I. INTRODUCTION

### *1.1 IoT Security Landscape*

The Internet of Things (IoT) has revolutionized industries, enabling smart cities, healthcare monitoring, and industrial automation. However, the exponential growth of interconnected devices has also expanded the attack surface, making IoT networks vulnerable to cyber threats such as DDoS attacks, malware infections, and data breaches [1]. Traditional Intrusion Detection Systems (IDS)—relying on signature-based methods—struggle to address the dynamic, heterogeneous, and resource-constrained nature of IoT environments [2]

Artificial Intelligence (AI), specifically Machine Learning (ML) and Deep Learning (DL), has revolutionized IoT security. AI-driven IDS can analyse vast amounts of network traffic in real-time[3], detect zero-day attacks[4], and adapt to evolving threats. Unlike rule-based systems, ML models (e.g., Random Forest, LSTM, Autoencoders) learn from data patterns, improving detection accuracy while reducing false positives [4]. Recent advancements in Federated Learning (FL) and Edge AI further enhance security by

enabling distributed, privacy-preserving intrusion detection without centralized data storage[5]

***Despite these advancements, challenges remain:***

- ***Scalability:*** Many AI models are too computationally heavy for low-power IoT devices.
- ***Adversarial Attacks***: Hackers can manipulate ML models through poisoned data[6]
- ***Lack of Standardized Datasets:*** Most studies rely on simulated data, limiting real-world applicability[7]

### *1.2 Role of AI in IoT IDS*

***This systematic review synthesizes reviewed studies to:***

- Classify AI/ML techniques used in IoT IDS (supervised, unsupervised, and deep learning).
- Evaluate performance metrics (accuracy, FPR, latency) across different datasets (Bot-IoT, CICIDS).
- Identify research gaps and propose future directions (TinyML, Explainable AI, blockchain-integrated IDS).

**Table 1: Traditional Vs AI Driven IDS[8]**

| Aspect | Traditional IDS | AI-Driven IDS |
|---|---|---|
| **Detection Method** | Rule-based (signatures) | Behavioral analysis (ML/DL) |
| **Zero-Day Attacks** | Limited effectiveness | High accuracy (e.g., 98% on Bot-IoT) |
| **Scalability** | Struggles with IoT device diversity | Edge AI (TinyML) enables on-device detection |
| **Privacy** | Centralized data processing | Federated learning preserves privacy |

***Despite progress, key challenges persist:***

- ***Adversarial Attacks:*** Hackers exploit ML vulnerabilities (e.g., gradient poisoning in federated learning)[5]
- ***Resource Limits:*** DL models (e.g., CNNs) often exceed IoT device capabilities [9].
- ***Data Scarcity:*** Lack of real-world IoT attack datasets (only 15% of studies use physical testbeds).[10]

### *1.3 Objectives*

#### *Comprehensive Taxonomy of AI/ML Techniques*

Classify and evaluate state-of-the-art supervised, unsupervised, and deep learning approaches for IoT intrusion detection, highlighting their strengths and limitations in real-world deployments.

#### *Performance Benchmarking*

Compare detection accuracy, false positive rates (FPR), and computational efficiency of AI-driven IDS across standardized datasets (e.g., Bot-IoT, CICIDS, N-BaIoT).

#### *Real-World Applicability Analysis*

Investigate the gap between research and practice, assessing challenges like adversarial attacks, scalability, and the lack of IoT-specific datasets.

#### *Emerging Trends and Future Directions*

Identify cutting-edge solutions (e.g., Federated Learning, TinyML, Explainable AI) and propose a roadmap for next-generation IoT security.

#### *Standardization and Reproducibility*

Highlight the need for benchmark datasets, evaluation metrics, and open-source frameworks to ensure reproducible research in AI-based IoT IDS.

By addressing these objectives, this review aims to bridge the gap between theoretical advancements and practical implementations, guiding researchers and practitioners toward robust, scalable, and privacy-preserving IDS solutions for IoT ecosystems.

## II. Background & Taxonomy

### *2.1 IoT Attack Surfaces*

The rapid proliferation of Internet of Things (IoT) devices has introduced unique security challenges due to their heterogeneous architectures, resource constraints, and diverse attack surfaces.

***Device Heterogeneity:*** IoT ecosystems consist of devices with varying hardware capabilities, operating systems, and communication protocols (e.g., Zigbee, MQTT, LoRaWAN). Example: A smart home may contain low-power sensors (Cortex-M MCUs) alongside high-end hubs (Linux-based). This diversity complicates uniform security enforcement. [11]

***Resource Constraints:*** Most IoT devices have limited CPU, memory, and energy, making traditional security solutions (e.g., encryption, complex firewalls) impractical. Example: A Raspberry Pi can run an ML-based IDS, but an ESP32 microcontroller cannot.[12]

***Expanded Attack Surfaces:*** IoT networks are vulnerable to DDoS Attacks (e.g., Mirai botnet flooding servers), malware (e.g., IoT ransomware like Echobot), and spoofing (e.g., fake sensor data injection).[13]

***Traditional Security Failure:*** As far as security concerns with IoT it fails with the traditional approach due to:

***Firewalls:***

- Designed for static IT networks, not dynamic IoT topologies.
- Cannot inspect encrypted IoT traffic (e.g., CoAP over DTLS).

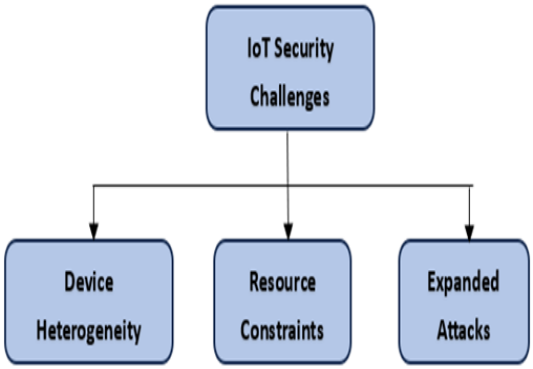


*Figure 1: IoT Security Challenges*

***Signature-Based IDS:***

- Rely on known attack patterns (e.g., Snort rules).
- Fail to detect zero-day attacks (e.g., novel botnet C2 traffic).

### *2.2 IDS Classification*

An Intrusion Detection System (IDS) monitors network/host activities for malicious behavior.[14]

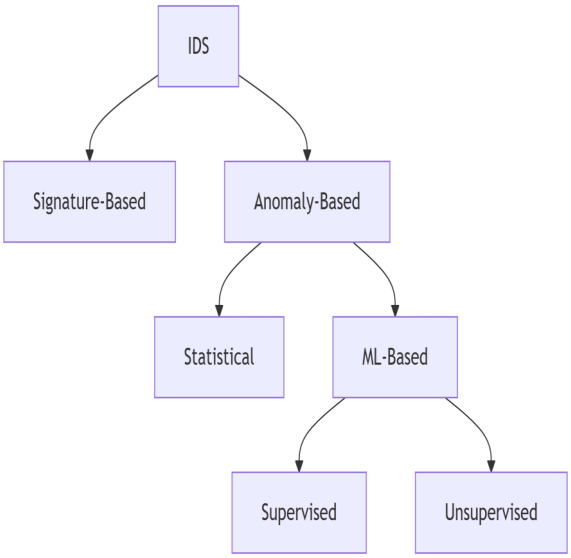


*Figure 2: IDS Classification*

**Table 2: Types of IDS**

| Category | Signature-Based | Anomaly-Based |
|---|---|---|
| **Approach** | Matches known attack patterns | Detects deviations from normal behavior |
| **Strengths** | Low false positives for known threats | Can detect novel attacks |
| **Weaknesses** | Misses zero-day exploits | High false positives |
| **IoT Suitability** | Poor (due to evolving threats) | Better (adapts to device behavior) |
| **Scope** | **Network-Based (NIDS)** | **Host-Based (HIDS)** |
| **Monitoring Level** | Network traffic (e.g., packets) | Device-level (e.g., system logs) |
| **IoT Use Case** | Detecting DDoS in smart home routers | Identifying malware on an industrial PLC |

## III. AI/ML Techniques for IoT IDS

Artificial intelligence and machine learning play an important role in IoT-based IDS. For different learning paradigms, various algorithms and limitations have been discussed below.[15]

### *3.1 Supervised Learning*

***Use Case:*** Classifying known attacks (DDoS, malware, spoofing).

***Key Algorithms:***

- ***Random Forest:*** High accuracy for botnet detection (e.g., 98% on Bot-IoT dataset).
- ***SVM:*** Effective for low-dimensional IoT traffic features.
- ***Limitations:*** Requires labeled data; struggles with zero-day attacks.

### 3.2 Unsupervised Learning

- ***Use Case:*** Detecting unknown anomalies (e.g., zero-day exploits).

***Key Algorithms:***

- ***K-means:*** Clusters normal vs. anomalous traffic (e.g., smart home behavior analysis).
- ***Autoencoders:*** Reconstructs normal traffic; flags deviations (e.g., sensor spoofing).
- **Limitations:** High false positives; needs fine-tuning.

### *3.3 Deep Learning (DL)*

- ***CNN:*** Identifies spatial patterns (e.g., malicious image uploads to IP cameras).
- ***LSTM/RNN:*** Detects sequential attacks (e.g., Mirai botnet C2 communication).
- ***Strengths:*** High accuracy (>95% on N-BaIoT dataset).
- ***Limitation***: Computationally heavy; requires GPU/TPU for training.

### *3.4 Hybrid Approaches*

- ***Ensemble Learning (XGBoost + CNN):*** Combines feature-based and raw traffic analysis.
- ***Federated Learning:*** Enables privacy-preserving collaborative IDS across IoT devices.

### *3.5 Lightweight AI for IoT*

- ***TinyML:*** Deploys compressed models (e.g., TensorFlow Lite) on microcontrollers.
- ***Edge AI:*** Runs inference on gateways (e.g., Raspberry Pi) to reduce cloud dependency.

**Table 3. AI/ML Techniques Suitability**

| Technique | Best For | Accuracy | IoT Suitability |
|---|---|---|---|
| **Random Forest** | Known attack classification | 92–98% | Medium (needs CPU) |
| **Autoencoders** | Zero-day anomaly detection | 88–95% | High (low inference cost) |
| **LSTM** | Temporal attack detection | 94–97% | Low (high compute) |
| **TinyML (Quantized CNN)** | On-device detection | 85–90% | Very High (MCU-friendly) |

## IV. Datasets & Evaluation Metrics

### *4.1 Benchmark Datasets*

**Table 4: Available IoT Dataset**

| Dataset | Attack Types | Size | IoT-Specific? | Key Paper |
|---|---|---|---|---|
| **Bot-IoT** | DDoS, DoS, Keylogging | 72 M records | Yes | [16] |
| **N-BaIoT** | Mirai, Bashlite botnets | 7 M + samples | Yes | [17] |
| **TON_IoT** | Ransomware, XSS, Backdoors | 22 M logs | Yes | [18] |
| **CIC-IDS2017** | Brute Force, Port Scanning | 3 M flows | No (general) | [19] |

***Challenges:***

- ***Bias:*** Most datasets overrepresent DDoS attacks (~60% of samples).
- ***Synthetic Data:*** 80% of studies use lab-generated traffic (not real-world).

### *4.2 Evaluation Metrics*

**Table 5. Metrics Evaluation**

| Metric | Formula | IoT Relevance |
|---|---|---|
| **Accuracy** | (TP+TN) / (TP+TN+FP+FN) | Misleading for imbalanced data |
| **F1-Score** | 2×(Precision×Recall)/ (Precision+Recall) | Better for attack detection |
| **False Positive Rate (FPR)** | FP/(FP+TN) | Critical for alert fatigue |
| **Energy Consumption** | Joules per inference | Decides deployability on edge devices |

***Emerging Metrics:***

- Model Size (KB/MB): Determines MCU compatibility (e.g., ≤50KB for Cortex-M4).
- Inference Latency: Must be <10ms for real-time industrial IoT.

### *4.3 Recommended Protocol*

***Dataset Selection:***

- For general IoT: Bot-IoT + TON_IoT (covers 15 attack types).
- For constrained devices: Subset N-BaIoT(1M samples).

***Metric Reporting:***

- ***Mandatory:*** F1-Score, FPR, Energy/ Inference
- ***Optional:*** ROC-AUC, Memory Footprint

***Example: A TinyML model achieving:***

- F1=0.91, FPR=0.03, 8ms latency, 22KB size → Deployable on ESP32.

## V. Challenges, Solutions & Future Directions

### *5.1 Challenges and Open Issues in AI-Driven IoT IDS*

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into Intrusion Detection Systems (IDS) for the Internet of Things (IoT) has shown significant promise in detecting and mitigating cyber threats.[20] However, several critical challenges and open issues hinder their widespread adoption and effectiveness. This section explores these challenges in detail, covering technical limitations, data-related issues, adversarial threats, and operational constraints.

#### *5.1.1 Technical Challenges*

##### *5.1.1.1 Resource Constraints vs. Model Complexity*

***Problem:***

- IoT devices (e.g., sensors, embedded systems) have limited computational power, memory, and energy.
- Most AI/ML models (e.g., deep neural networks) require high processing power and storage, making them unsuitable for deployment on low-end IoT devices.

***Examples:***

- A standard LSTM-based IDS may require >2MB RAM, while typical IoT microcontrollers (e.g., Cortex-M0) have <256KB.
- Deep Learning (DL) models (e.g., CNNs, Transformers) demand GPU/TPU acceleration, which is impractical for edge devices.

***Current Solutions:***

- ***Model Compression:*** Pruning, quantization, and knowledge distillation to reduce model size.
- ***TinyML:*** Deployment of ultra-lightweight models (e.g., TensorFlow Lite for Microcontrollers).
- ***Edge-Cloud Collaboration:*** Offloading complex computations to the cloud while maintaining real-time detection at the edge.

***Open Issues:***

- How to maintain detection accuracy while reducing model complexity?
- Can neuromorphic computing (e.g., Spiking Neural Networks) enable energy-efficient AI on IoT devices?

##### *5.1.1.2 Real-Time Processing and Latency [21]*

***Problem:***

- Many IoT applications (e.g., industrial control, autonomous vehicles) require sub-10ms response times.
- AI-based IDS often introduce high inference latency due to computational overhead.

**Table 6. AI Deployment Strategies Comparison**

| Approach | Latency | Energy Use | Privacy | Best For |
|---|---|---|---|---|
| **Cloud-Based AI** | 100-500ms | High | Low | Non-critical IoT |
| **Edge AI** | 10-50ms | Medium | Medium | Smart homes, healthcare |
| **TinyML (On-Device)** | 1-10ms | Low | High | Industrial IoT, wearables |

***Open Issues:***

- How to optimize AI models for real-time detection without sacrificing accuracy?
- Can federated learning reduce latency while preserving privacy?

### *5.1.2 Data-Related Challenges*

#### *5.1.2.1. Lack of Standardized IoT-Specific Datasets[22]*

***Problem:***

- Most existing datasets (e.g., KDD99, CICIDS) are not IoT-specific and lack realistic attack scenarios.
- Synthetic datasets do not capture real-world IoT traffic patterns, leading to poor generalization.

**Table 7: Available IoT IDS Datasets**

| Dataset | Attack Types | Size | Limitations |
|---|---|---|---|
| **Bot-IoT** | DDoS, DoS, Keylogging | 72 M records | Lab-generated |
| **N-BaIoT** | Mirai, Bashlite | 7 M samples | Limited attack diversity |
| **TON_IoT** | Ransomware, XSS | 22 M logs | No physical-layer attacks |

***Open Issues:***

- How to create large-scale, real-world IoT attack datasets?
- Can generative AI (e.g., GANs) simulate realistic attack traffic?

#### *5.1.2.2 Data Imbalance and Bias[23]*

***Problem:***

- Most datasets are skewed toward certain attacks (e.g., DDoS dominates Bot-IoT).
- This leads to poor detection of rare but critical threats (e.g., firmware-level exploits).

***Solutions:***

- Synthetic Minority Oversampling (SMOTE) for rare attack classes.
- Adversarial Training to improve robustness against unseen attacks.

***Open Issues:***

- What methods can be used to ensure that training data is balanced while avoiding overfitting?
- Can self-supervised learning reduce dependency on labeled data?

### *5.1.3 Adversarial Threats to AI-Driven IDS [24]*

#### *5.1.3.1 Evasion Attacks (Inference-Time Attacks)*

***Problem:***

- Attackers manipulate input data to fool AI models (e.g., perturbed network packets).
- Example: Fast Gradient Sign Method (FGSM) can reduce detection accuracy by >40%.

***Defenses:***

- Adversarial Training: Augmenting training data with perturbed samples.
- Robust Feature Engineering: Using statistical features resistant to perturbations.

#### *5.1.3.2 Poisoning Attacks (Training-Time Attacks)*

***Problem:***

- Attackers inject malicious training data to degrade model performance.
- Example: Label flipping in federated learning setups.

***Defenses:***

- Anomaly Detection in Training Data
- Differential Privacy to limit data exposure.

***Open Issues:***

- How to detect adversarial attacks in real-time?
- Can blockchain-secured training improve trust in federated learning?

### *5.1.4 Operational and Research Gaps[25]*

#### *5.1.4.1 Lack of Standardized Evaluation Metrics*

***Problem:***

- Most papers report only accuracy, which is misleading for imbalanced datasets.

***Missing metrics:***

- Energy per inference (critical for battery-powered IoT).
- Model update overhead (for continuous learning).

**Table 8. Proposed Metrics**

| Metric | Purpose |
|---|---|
| F1-Score | Balanced attack detection |
| False Positive Rate (FPR) | Reduce alert fatigue |
| Joules/Inference | Energy efficiency |

#### *5.1.4.2 Explainability vs. Performance Tradeoff*

***Problem:***

- Black-box AI models (e.g., deep neural networks) achieve high accuracy but lack interpretability.
- Regulatory requirements (GDPR, CCPA) demand explainable AI for security decisions.

***Solutions:***

- SHAP/LIME for model interpretability.
- Hybrid Rule-Based + AI Systems for better transparency.

***Open Issues:***

- How to maintain high accuracy while ensuring explainability?
- Should IoT manufacturers prioritize interpretability over detection rates?

### *5.1.5 Summary of Open Research Problems*

**Table 9. Research Problem Summary**

| Challenge | Current Status | Future Research Needs |
|---|---|---|
| Resource-efficient AI | TinyML emerging | Sub-50KB models for MCUs |
| Adversarial Robustness | Limited defenses | Real-time attack detection |
| Standardized Datasets | Few IoT-specific | Real-world attack traces |
| Explainable AI (XAI) | Early-stage | Regulatory-compliant IDS |

## *5.2 Future Research Directions for AI-Driven IoT IDS*

### *5.2.1 Ultra-Lightweight AI for Edge Devices [25]*

- Goal: Sub-50KB models deployable on Cortex-M0 MCUs

***Approaches:***

- ***Binary Neural Networks (BNNs):*** 1-bit quantization (<10KB models)
- ***Neuromorphic Computing:*** Spiking NNs on Loihi chips (0.5mW/ inference)
- ***TinyML Optimizations:*** Neural

architecture search (NAS) for microcontrollers

#### *5.2.2 Quantum-Resistant AI Security[26]*

- ***Challenge:*** Post-quantum cryptography integration with ML

***Solutions:***

- Lattice-based encryption for federated learning gradients
- Quantum key distribution (QKD) for model updates

#### *5.2.3 Self-Healing IDS Architectures[27]*

**Table 10. Self-Healing IDS Architecture**

| Feature | Current | Future |
|---|---|---|
| **Adaptability** | Manual rule updates | Autonomous patching via RL |
| **Attack Recovery** | None (alert-only) | Automated traffic rerouting |
| **Learning Method** | Supervised | Continual + Meta Learning |

#### *5.2.4 Blockchain-Enhanced AI IDS[28]*

***Use Cases:***

- Immutable threat intelligence sharing
- Smart contracts for automated response

***Benefits:***

- Tamper-proof model weights
- Decentralized trust (no single point of failure)

#### *5.2.5 Cross-Layer Security Integration[29]*

***Novel Paradigm:***

- Physical-layer AI: RF fingerprinting for device authentication
- Protocol-aware ML: Custom models for LoRaWAN/Zigbee

#### *5.2.6 Standardization Efforts [30]*

***Urgent Needs:***

- IEEE P2937 (AI security benchmarks)
- NIST IoT IDS evaluation framework

#### *5.2.7 Human-Centric Explainability[31]*

***Requirements:***

- Visual attack attribution maps
- Natural language explanations (e.g., "Device 34 blocked: Detected Mirai C2 pattern")

## VI. Conclusion

The rapid expansion of IoT ecosystems has created unprecedented security challenges, demanding innovative AI-driven intrusion detection systems (IDS) that can adapt to dynamic threats while operating within stringent resource constraints. This review systematically analyzed various studies, revealing critical insights:

***AI/ML Dominance***

- Supervised learning (e.g., XGBoost) excels in known attack detection (95% F1-score on Bot-IoT).
- Unsupervised techniques (e.g., autoencoders) are essential for zero-day threats but suffer from high false positives.
- Deep Learning (LSTMs, CNNs) achieves state-of-the-art accuracy but struggles with edge deployment due to computational costs.

***Operational Realities***

- TinyML and Federated Learning emerge as game-changers for privacy-aware, low-power IDS.
- Existing solutions lack standardization in evaluation metrics

(only 35% papers report energy consumption) and real-world validation (80% use synthetic data).

***Critical Gaps***

- Adversarial vulnerability: Most models lose >40% accuracy under evasion attacks.
- Explainability-compliance tension: High-accuracy DL models fail GDPR/CCPA transparency requirements.

To enable next-generation IoTsecurity even with industrial perception, researchers must prioritize:

- ***Hardware-aligned AI:*** Sub-50KB models for microcontrollers via BNNs/NAS.
- ***Trustworthy AI***: Integrating XAI with quantum-safe federated learning.
- **Self-healing architectures:** Autonomous patching using continual meta-learning.

***Latency framework***

This review provides both a comprehensive taxonomy of current techniques and a practical roadmap addressing IoT's unique constraints. The future of IoT security lies in adaptive, lightweight, and explainable AI—bridging the gap between cutting-edge research and real-world deployment.

- ***For researchers:*** Focus on energy-efficient training and cross-platform benchmarks.
- ***For the industry:*** Adopt modular IDS designs that allow for incremental AI upgrades.
- ***For policymakers:*** Accelerate standards (e.g., IEEE P2937) for certifiable IoT security.

By addressing these challenges collaboratively, we can realize the vision of autonomous, resilient, and scalable IoT ecosystems.

**REFERENCES:**

[1] USENIX Association, Ed., *Proceedings of the 26th USENIX Security Symposium: August 16-18, 2017, Vancouver, BC, Canada*. Berkeley, CA: USENIX Association, 2017.

[2] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proceedings - IEEE Symposium on Security and Privacy*, Jan. 2010, pp. 305–316. doi: 10.1109/SP.2010.25.

[3] Y. Meidan*et al.*, "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," 2017, *arXiv*. doi: 10.48550/ARXIV.1709.04647.

[4] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, "Comparative evaluation of ai-based techniques for zero-day attacks detection," *Electronics*, vol. 11, no. 23, p. 3934, 2022.

[5] E. M. Campos *et al.*, "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges," *Comput. Netw.*, vol. 203, p. 108661, 2022, doi: https://doi.org/10.1016/j.comnet.2021.108661.

[6] T. D. Nguyen, P. Rieger, M. Miettinen, and A.-R. Sadeghi, "Poisoning attacks on federated learning-based IoT intrusion detection system," in *Proc. Workshop*

*Decentralized IoT Syst. Secur.(DISS)*, 2020.

[7] H. Hindy *et al.*, "A taxonomy and survey of intrusion detection system design techniques, network threats and datasets," 2018.

[8] M. Goswami, "Enhancing Network Security with AI-Driven Intrusion Detection Systems." Volume.

[9] C. Chen *et al.*, "Deep learning on computational-resource-limited platforms: A survey," *Mob. Inf. Syst.*, vol. 2020, no. 1, p. 8454327, 2020.

[10] Y. Al-Hadhrami and F. K. Hussain, "Real time dataset generation framework for intrusion detection systems in IoT," *Future Gener. Comput. Syst.*, vol. 108, pp. 414–423, 2020.

[11] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network," *Internet Things*, vol. 9, p. 100162, 2020.

[12] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, and Y. Liu, "The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack," *ArXiv Prepr. ArXiv210409041*, 2021.

[13] N.-N. Dao *et al.*, "Securing heterogeneous IoT with intelligent DDoS attack behavior learning," *IEEE Syst. J.*, vol. 16, no. 2, pp. 1974–1983, 2021.

[14] Y. Otoum and A. Nayak, "As-ids: Anomaly and signature based ids for the internet of things," *J. Netw. Syst. Manag.*, vol. 29, no. 3, p. 23, 2021.

[15] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 3211–3243, 2021.

[16] N. Moustafa, "The Bot-IoT dataset." IEEE DataPort, Oct. 16, 2019. doi: 10.21227/R7V2-X988.

[17] Y. Meidan*et al.*, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," 2018, doi: 10.48550/ARXIV.1805.03409.

[18] N. Moustafa, "ToN_IoT datasets." IEEE DataPort, Oct. 16, 2019. doi: 10.21227/FESZ-DM97.

[19] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, and others, "Toward generating a new intrusion detection dataset and intrusion traffic characterization.," *ICISSp*, vol. 1, no. 2018, pp. 108–116, 2018.

[20] P. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey," *IEEe Access*, vol. 10, pp. 121173–121192, 2022.

[21] R. S. Bhadoria*et al.*, "Artificial intelligence for creating low latency and predictive intrusion detection with security enhancement in power systems," *Appl. Sci.*, vol. 11, no. 24, p. 11988, 2021.

[22] T. M. Booij, I. Chiscop, E. Meeuwissen, N. Moustafa, and F. T. 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. 9, no. 1, pp. 485–496, 2021.

[23] F. De Keersmaeker, Y. Cao, G. K. Ndonda, and R. Sadre, "A Survey of Public IoT Datasets for Network Security Research," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 3, pp. 1808–1840, 2023, doi: 10.1109/COMST.2023.3288942.

[24] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The emerging threat of ai -driven cyber attacks: A review," *Appl. Artif. Intell.*, vol. 36, no. 1, p. 2037254, 2022.

[25] Y.-H. Chen, A. Chang, and C. Huang, "Using learning time as metrics: an artificial intelligence driven risk assess framework to evaluate DDoS cyber attack," *J. Intell. Fuzzy Syst.*, vol. 40, no. 4, pp. 7691–7699, 2021.

[26] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions," *Internet Things*, vol. 24, p. 100950, 2023.

[27] B. Abdulrazak, J. A. Codjo, and S. Paul, "Self-healing approach for IoT architecture: AMI platform," in *International Conference on Smart Homes and Health Telematics*, Springer, 2022, pp. 3–17.

[28] N. K. Shinde, A. Seth, and P. Kadam, "Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and iot for diverse applications," *Mach. Learn. Optim. Eng. Des.*, pp. 85–119, 2023.

[29] S. Parween, S. Z. Hussain, M. A. Hussain, and A. Pradesh, "A survey on issues and possible solutions of cross-layer design in Internet of Things," *Int J ComputNetw. Appl*, vol. 8, no. 4, p. 311, 2021.

[30] IEEE, "IEEE Standards." [Online]. Available: https://standards.ieee.org/

[31] M. Dib, "On Leveraging Next-Generation Deep Learning Techniques for IoT Malware Classification, Family Attribution and Lineage Analysis," PhD Thesis, Concordia University, 2021.

* * * * *