

# AI Powered Security for IoT Networks Ensuring Adaptive Threat Detection Privacy and Resilience

Mohd Abdul Raheem<sup>1</sup>, Moin Uddin Khaja<sup>2</sup>

State University of New York Institute of Technology, NY, USA<sup>1</sup>

Lindsey Wilson College, KY, USA<sup>2</sup>

**Abstract:** The proliferation of IoT devices across industries has revolutionized efficiency but created an expansive, complex attack surface characterized by heterogeneous devices, weak protocols, and low physical security. Conventional security solutions are often ineffective due to IoT's resource constraints and unique latency and scalability needs. Artificial Intelligence approaches—spanning deep learning, federated, and edge-based frameworks—address these gaps through adaptive, autonomous, and privacy-aware threat detection using real-time telemetry and behavioural analytics. Techniques such as intrusion detection, device fingerprinting, and anomaly detection enable timely response against known and novel threats. This review surveys leading AI strategies for IoT security, explores dataset benchmarks, adversarial resilience, resource allocation, explainable AI, and privacy safeguards. Ongoing challenges include defending against advanced persistent threats, ensuring robust operation across diverse environments, optimizing efficiency, and providing standardized datasets. The findings advise stakeholders on building scalable, trustworthy, and resilient AI-powered IoT security systems.

**Keywords:** Edge AI Security, IoT Anomaly Detection, Device Fingerprinting, Botnet Detection, Bot-IoT Dataset, N-BaIoT Dataset, Privacy-Preserving Machine Learning, Adversarial Machine Learning for IoT, Explainable AI (XAI) for IoT, Hybrid Edge-Cloud Security Architecture, IoT Threat Modelling, Distributed Intrusion Detection, Secure Federated Aggregation, and real-time threat mitigation for IoT.

## I. INTRODUCTION

The Internet of Things (IoT), which links millions of physical devices to the internet and allows the real and digital worlds to seamlessly merge, is arguably the most revolutionary technology paradigm of the twenty-first century [1]. Among the applications of IoT technology are critical infrastructure, transportation networks, smart homes, industrial automation, and health monitoring. Real-time data and analytics are gathered by shared systems, which boost business efficiency, save expenses, and enhance decision-making [2]. But the very qualities that make IoT attractive are its ubiquity, heterogeneity, and autonomy. Additionally, those same traits lead to a wildly enlarged and extremely intricate cyberattack surface.

IoT devices in general operate with highly constrained limits on processing, memory, and energy, which makes the deployment of strong, resource-intensive security components difficult. In addition, heterogeneity in hardware platforms, operating systems, and communications protocols bring interoperability concerns as well as the constraint on portability of native security products that have been installed for legacy computing systems [3]. Mass placement of devices in reachable areas places them in physical jeopardy of attack, and slow firmware updates expose most devices to publicly available vulnerabilities. DDoS assaults, hijacking of devices, exfiltration of data, and botnet creation (such as the Mirai botnet) already have the capability to create unprecedented disruption by hijacking IoT devices [4].

With such adversities, Artificial Intelligence (AI), such as Machine Learning (ML), Deep Learning (DL), and Federated Learning (FL), has emerged as a robust enabler of IoT security [5]. Compared to traditional rule-based systems relying on pre-defined signatures, AI-based controls have the ability to learn from normal and suspicious pattern behaviour from data, educate themselves with threats, and identify new attack vectors. For instance, ML models are employed to categorize network traffic flows to determine benign traffic and intrusions while DL architectures such as CNNs and RNNs can extract deep spatial and temporal features for anomaly detection without requiring specifications to be defined manually [6]. Federated Learning goes one step further and provides decentralized training of models on edge devices over distributed IoT without compromising raw data, thus enhancing privacy and conserving bandwidth.

In addition to detection, AI can facilitate predictive security — foresight of potential attack vectors ahead of time — and facilitate automated incident response. Built into edge computing platforms, AI facilitates low-latency decision-making close to sources of data, required in real-time applications such as driverless vehicles or industrial automation systems

[7]. However, using AI for IoT security is not without challenges, such as model adversary attacks, explainable decisions, energy-aware computing, and resilience in diverse systems.

This paper would like to give a holistic overview of the AI contribution to IoT network security, from technical fundamentals, existing practices, evaluation mechanisms, privacy, and research challenges, ultimately in the sequence of building scalable, reliable, and resilient AI-based IoT security systems [8].

## II. BACKGROUND AND THREAT MODEL

### 2.1 IoT Features That Affect Security

IoT networks differ from conventional computer environments in a number of ways [9].

- Gigantic Scale and Diversity: IoT networks contain billions of devices of different manufacturers with their own proprietary firmware, hardware, and communication protocols [10].
- Because of their limited CPU, RAM, and battery capacity, devices in an IoT network cannot employ costly encryption or computationally intensive security measures [11].
- Dynamically Changing Topology: Devices are continually joining and departing networks, particularly in mobile IoT applications such as vehicular networks and wearable devices [12].
- Physical Accessibility: The majority of devices are deployed in uncontrolled situations and hence vulnerable to physical compromise [13].

Since AI systems are able to learn and adjust to new circumstances, they are excellent at providing the light, flexible, and mostly decentralized security mechanisms that are required for such capabilities [14].

### 2.2 Common types of threats in IoT

#### 1. Network-Level Attacks

- Examples: Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM), port scanning [15].
- Impact: Disruption of services, eavesdropping on confidential communication.

#### 2. Device-Level Attacks

- Examples: Firmware tampering, illegal device access, hardware backdoors [16].
- Impact: Total control of device functions, enabling participation in botnets or theft of data.

#### 3. Data-Level Threats

- Examples: Eavesdropping, unauthorized data gathering, injection of forged sensor readings [17].
- Impact: Incorrect decision-making and loss of data integrity.

#### 4. Model-Level Threats (Adversarial ML)

- Evasion (altering input to avoid detection) and poisoning (tampering with malicious training data) are examples of assaults [18].
- Impact: Enhanced false negatives in intrusion detection and decreased performance of AI models.

### 2.3 Threat Modelling in AI-Enabled IoT Security

AI-enabled Threat Modelling IoT security is the process of detecting potential attack surfaces and mapping them to AI mitigation solutions [19]. It contributes to the implementation of proactive defence strategies. AI models can be trained in real time to detect anomalies and categorize threats using network data, device behaviour records, and environmental context [20].

Table 1. IoT Threats and AI-Driven Mitigation Strategies

Threat Category	Example Attacks	AI-Based Mitigation Approach	Expected Outcome
Network-Level	DDoS, MITM	Deep Learning-based Intrusion Detection (e.g., CNN, LSTM)	Early detection, reduced downtime
Device-Level	Firmware tampering, unauthorized access	Device fingerprinting via ML, anomaly detection	Unauthorized devices blocked
Data-Level	Data spoofing, eavesdropping	Federated Learning for secure collaborative detection	Maintained data integrity, privacy preservation
Model-Level	Adversarial evasion, poisoning	Adversarial training, robust aggregation in FL	Improved model resilience and robustness

## 2.4 AI Role in the Threat Model

In the IoT threat paradigm, artificial intelligence (AI) is crucial for several reasons. threat model in several ways [21]:

- Adaptive protection modifies detection thresholds in response to evolving attack trends.
- **Proactive Predictive Risk:** This approach foresees possible attacks by using predictive analytics.
- **Distributed intelligence:** Increases detection capabilities and decreases single points of failure by utilizing edge and federated learning [22].
- **Continuous Improvement:** Models are redeployed on fresh data in an effort to counter new, unrecognized attack vectors.

Companies can use AI-driven threat modelling to create a proactive and flexible layered security plan for IoT networks that will protect against current and future threats while also adjusting to the ever-evolving IoT ecosystem [23].

## III. AI TECHNIQUES FOR IOT SECURITY

IoT network security, including adaptive, data-driven intrusion detection, anomaly detection, device authentication, and botnet prevention, is quickly relying on artificial intelligence (AI). The four main categories of AI techniques utilized in IoT security are Hybrid Edge AI, Federated and Distributed Learning (FL/DL), Deep Learning (DL), and Classical Machine Learning (ML). Each has deployment-related benefits and drawbacks [24].

### 3.1 Classical Machine Learning (ML)

Decision trees, Random Forest, Support Vector Machines (SVMs), and K-Nearest Neighbours (KNN) are examples of traditional machine learning models that have been used for IoT intrusion detection for decades due to their moderate interpretability and cheap computational complexity [25]. From IoT network flows or device behaviour records, they employ feature engineering to extract statistical, temporal, or frequency-domain information.

- Benefits include interpretability, efficient training on tiny datasets, and low resource consumption.
- Its limitations include an inability to handle raw high-dimensional data and a reduced ability to handle new threats unless re-trained on a regular basis.

### 3.2 Deep Learning (DL)

Without requiring human intervention, deep learning methods like autoencoders, recurrent neural networks (RNNs), convolutional neural networks (CNNs), and long short-term memory (LSTM) networks may be able to autonomously learn the hierarchical features of IoT data streams [26]. Without requiring extensive manual feature selection, DL excels in identifying anomalies, categorizing traffic, and analysing behaviour.

- Raw data processing, sensitivity to new patterns, and low detection error are among its advantages.
- Higher processing demands, susceptibility to overfitting, and reduced interpretability in the absence of XAI tools are some of its disadvantages.

### 3.3 Federated and Distributed Learning (FL/DL)

By allowing cooperative model training across several IoT devices or gateways without needing raw data sharing, Federated Learning (FL) preserves confidentiality and reduces bandwidth expenses [27]. The same concepts are used in distributed learning for decentralized, extensive training that incorporates resilience.

- Benefits include reducing dependency on central servers, protecting privacy, and supporting a large number of devices.
- Cons: Requires strong aggregation and communication-efficient techniques; susceptible to model poisoning attacks.

### 3.4 Hybrid and Edge AI

With hybrid approaches, cloud-based AI and edge computing are combined [28]. While complicated processing and retraining occur in the cloud, lightweight ML/DL models operate locally on edge devices for quick, low-latency detection. In terms of speed, accuracy, and resource limitations, this achieves equilibrium.

- **Benefits:** Real-time decision-making, reduced latency, improved bandwidth usage.
- **Limitations:** Needs proper partitioning of the model and synchronization between edge and cloud.

Table-to-Visual Mapping: The conceptual bar diagram below to compare these techniques.

Table 2: Comparative Strength of AI Techniques in IoT Security

Technique	Detection Accuracy	Resource Efficiency	Scalability	Privacy Preservation
ML	7	9	6	5
DL	9	6	7	6
FL	8	7	9	9
Hybrid Edge AI	8	8	8	8

### Bar Figure Concept: "Comparative Strength of AI Techniques in IoT Security"

X-axis: AI Techniques (ML, DL, FL, Hybrid Edge AI)

Y-axis: Scaled Performance Scores (0–10) across metrics: Detection Accuracy, Resource Efficiency, Scalability, Privacy Preservation.

Illustrative Values:

The resulting bar chart would be four grouped bars across categories, enabling easy visual comparison of strengths and trade-offs.

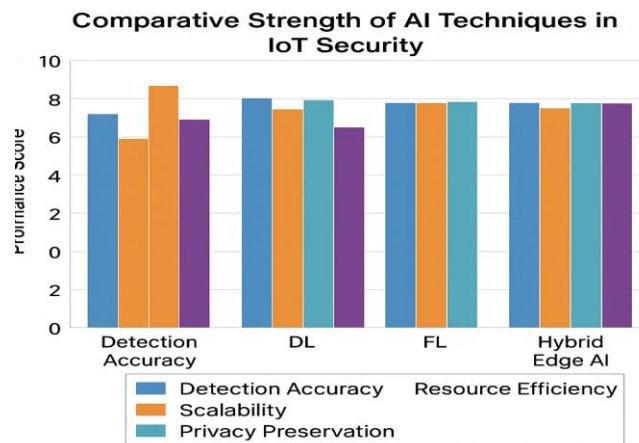


Figure 1: Comparative Strength of AI Techniques in IoT Security

## IV. DATASETS AND EVALUATION

Sufficient assessment of AI-IoT security systems depends on the selection of sufficient datasets and application of standardized metrics to facilitate simple, replicable comparisons. Dataset selection affects system generality, susceptibility to novel attacks, and readiness for real-world deployment [29].

### 4.1 Commonly-Used Datasets for IoT Security

#### 4.1.1 Bot-IoT Dataset

BoT-IoT is a dataset that was created by the UNSW Canberra Cyber Range Lab to simulate actual IoT network scenarios of normal and attack traffic involving DDoS, DoS, reconnaissance, and data steal attacks [30]. It supports binary and multiclass classification issues with network flow-based features for supervised and unsupervised models.

#### 4.1.2 N-BaIoT Dataset

Evolved formula and sheltie malware-infected commercial IoT devices, N-BaIoT provides time-series network data from real-world scenarios [31]. It is highly beneficial for botnet detection and anomaly-based intrusion detection due to its variety of devices.

#### 4.1.3 CICIoT2023 and CIC-IDS Variants

Such Canadian Institute for Cybersecurity (CIC) data sets highlight end-to-end intrusion detection settings, capturing IoT-extractive and generic classes of attack behaviour [32]. They are always used to compare AI-based IDS systems with their traditional network counterparts.

## 4.2 Evaluation Metrics

### 4.2.1 Performance Metrics

- **Accuracy** — Tallies the number of correct predictions; applicable with balanced data sets.
- **Precision & Recall** — Vital for attack detection under skewed conditions (high recall keeps false negatives low) [33].
- **F1-Score** — Harmonic mean of precision and recall; keeps both in balance.
- **AUC-ROC** — Considers trade-offs between true positive and false positive rates [34].

### 4.2.2 Deployment Metrics

- **Inference Latency** — Latency to detect and respond to threats [35].
- **Model Size** — Relevant when deploying on resource-constrained IoT devices.
- **Energy Consumption** — Of highest priority for battery-operated devices [36].
- **Scalability** — Ability to keep up with increasing device quantity and traffic load.

### 4.2.3 Security-Specific Metrics

- **Adversarial Robustness** — Determined through controlled evasion or poisoning experiments [37].
- **Cross-Device Generalization** — Verified accuracy against unfamiliar protocols or devices.

## 4.3 Recommended Evaluation Process

1. Employ several datasets (e.g., BoT-IoT + N-BaIoT) to minimize dataset bias.
2. Use train-test splits per device to test generalization.
3. Integrate resource and latency profiling with measurement of accuracy.
4. Perform adversarial robustness testing to mimic the realistic threats.

### Diagram Concept: "AI-Based IoT Security Evaluation Pipeline"

#### Flow

• Dataset Collection → Preprocessing & Feature Extraction → Model Training (ML/DL/FL) → Evaluation Metrics (Performance, Deployment, Security) → Deployment & Continuous Monitoring.

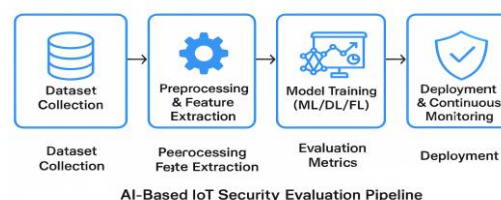


Figure 2: AI-Based IoT Security Evaluation Pipeline

## V. REPRESENTATIVE ARCHITECTURES & PROPOSED FRAMEWORK

AI and IoT security convergence should enhance through the use of well-designed architectures to enable processing very large volumes of diverse data, providing real-time threat detection, and responding to emerging cyber threats [38]. Blueprints are example architectures, while an outlined framework combines the best practices into an efficient future-proof design.

### 5.1. Centralized AI-Driven Security Architecture

In this design, IoT devices send raw or lightly processed information to a centralized server or cloud where AI models monitor traffic patterns, identify anomalies, and manage responses [39].

#### Strengths:

- Strong computational resources for complex AI models
- single security policy and centralized management

#### Weaknesses:

- single point of failure and privacy risk
- high latency for real-time security

### 5.2. Edge AI Security Architecture

Edge AI minimizes latency by proximity of computation to IoT devices, enabling near-real-time threat detection. AI models are trained on gateways or even on devices [40].

#### Advantages:

- Lower latency and faster mitigation
- Lower bandwidth usage

## Disadvantages:

- Lower computational power
- Frequent updates of AI models

## 5.3. Federated Learning-Enabled Architecture

Federated Learning (FL) allows collaborative model training of AI models by distributed IoT devices without revealing raw data, thus preserving privacy. Model updates only are shared [41].

- Restrictive privacy protection
- Device-specific environments enabled by distributed learning

## Limitations:

- Communication overhead from model updates through frequent communications
- Susceptible to poisoning attacks with device attacks

## 5.4. Hybrid AI-Security Architecture

Hybrid models take advantage of cloud-based AI processing for long-term analysis and edge-based AI for real-time protection [42]. Centralized as well as decentralized benefits are reaped by the balance.

## Advantages:

- Scalable and adaptable to various environments
- Resource assignment is optimized

## Limitations:

- Increased design complexity
- Requires robust synchronization mechanisms

## 5.5. Proposed AI-Based IoT Security Framework

The proposed framework is a federated-edge hybrid framework that comprises the following [43]:

1. **Data Acquisition Layer** – Harvests IoT traffic and sensor data securely.
2. **Edge Pre-Processing Layer** – Conducts feature extraction and light-weight anomaly detection.
3. **Federated Learning Layer** – Trains global AI models from end-to-end encrypted, aggregated local updates.
4. **Cloud Analytics Layer** – Conducts in-depth forensic analysis, trend prediction, and long-term policy tuning.
5. **Response & Policy Enforcement Layer** – Applies mitigation measures locally (edge) and globally (cloud level).
6. **Continuous Learning & Adaptation** – Updates models with new and available data on an ongoing basis.

## 5.6. Architecture Diagram Description (for generation):

A multi-layer diagram showing five horizontal layers:

1. **IoT Devices Layer** (sensors, cameras, wearables) providing input to
2. **Edge Processing & Detection Layer** (AI model-enabled gateways),
3. **Federated Learning Coordination Layer** (model updates shared),
4. **Cloud AI Analytics Layer** (big data analytics central AI server), and
5. **Security Response Layer** (enforcement to devices).

Upward data flow and downward policy feedback loops are shown by arrows.

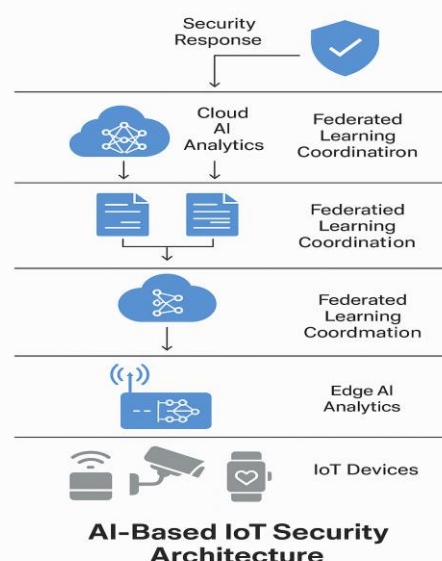


Figure 3: AI-Based IoT Security Architecture



## VI. ADVERSARIAL THREATS AND DEFENCES

Securing IoT networks with AI has the following unique challenge: AI models themselves can be attacked with adversarial attacks [44]. Attackers can manipulate inputs or exploit model vulnerabilities to evade security, disable detection, or inject malicious behaviour into the devices connected. This section defines common adversarial threats in AI-IoT systems and countermeasures.

### 6.1. Types of Adversarial Threats

#### a. Evasion Attacks

Attackers subtly manipulate IoT data inputs (i.e., sensor reading, network packet) to deceive AI models [45]. For example, slight alterations of a monitoring image may deceive an intrusion detection model to incorrectly mark the object.

#### b. Poisoning Attacks

Attackers add tainted data during training, which continuously degrades the AI model's performance. In the IoT network, tainted devices can provide deceptive readings to skew model responses [46].

#### c. Model Inference Attacks

Attackers test the AI model in anticipation of inferring sensitive information, such as its architecture, parameters, or training data, for the purpose of intellectual property breach or privacy breach [47].

#### d. Replay & Injection Attacks

Pre-recorded, manipulated signals or forged packets of data are injected into the system with the aim of developing clones of real traffic, avoiding detection algorithms [48].

### 6.2. Defence Mechanisms

#### a. Adversarial Training

Integrating adversarial examples into the training dataset of the model for enhancing robustness. This causes the model to learn patterns that are perturbation-resistant [49].

#### b. Input Preprocessing & Sanitization

Techniques used for normalization, feature squeezing, and denoising filters help remove adversarial noise before providing input to the AI model [50].

#### c. Model Hardening

Defensive distillation or creating strong architectures are some of the methods that desensitize the model against perturbations, and it is harder to attack [51].

#### d. Anomaly Detection Layers

Insertion of another AI layer to detect model output for outlier patterns that expose adversarial tampering [52].

Table 3: Comparative Analysis of Threats and Defences

Threat Type	Impact on IoT AI Systems	Defense Strategy
Evasion Attacks	Bypasses detection without raising alerts	Adversarial Training, Input Sanitization
Poisoning Attacks	Corrupts training dataset and weakens model	Data Validation, Federated Learning
Model Inference Attacks	Leaks model and training data details	Differential Privacy, Query Limiting
Replay & Injection Attacks	Disrupts normal operations	Secure Communication, Signature Verification

### 6.3. Future Research Directions

- Development of self-recovering AI model that can auto-retrain if it detects adversarial patterns.
- IoT security on a blockchain foundation for immutable, trust-based authentication of data [53].
- Federated adversarial training was used to protect distant IoT systems without disclosing private information to a central location.

### Line Diagram Description

Two lines that meet over time must be present in the line diagram:

- The Threat Intensity Curve, which rises with increasingly sophisticated attacks.
- The defence robustness curve, which rises with more sophisticated defences.

To demonstrate strength improvements, growth milestones such as "Adversarial Training Adoption," "Model Hardening," and "Federated Defence Integration" should be used [54].

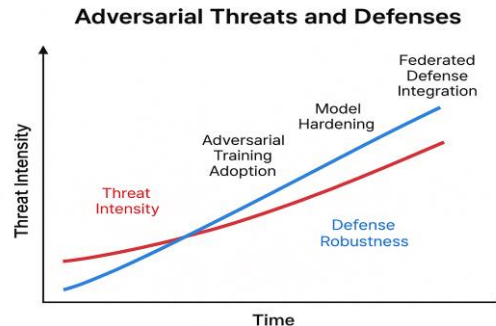


Figure 4: Adversarial Threats and Defence

## VII. PRIVACY, ETHICS, AND GOVERNANCE IN AI-ENABLED IOT SECURITY

Along with threat detection, automation, and resilience, integrating AI into IoT security also brings with it complicated issues like data protection, ethical responsibility, and governance [55]. They are necessary because sensitive data is being processed by IoT devices more often and AI-powered decision-making can have practical applications in smart cities, healthcare, industrial automation systems, and personal devices.

### 7.1. Privacy Considerations

#### a. Data Minimization

IoT networks reduce their exposure in the event of a vulnerability by only accepting information necessary for proper operation. It is possible to create AI-based systems that can identify threats without gaining access to any personally identifiable information [56].

#### b. Federated Learning

A privacy-preserving AI method whereby AI models are trained locally on Internet of Things devices and only offer summary updates, guaranteeing that private data never leaves its source [57].

#### c. Data Anonymization & Encryption

Encryption-at-rest, encryption-in-transit, and tokenization techniques render obtained data incoherent and render it hard to link it to specific individuals [58].

### 7.2. Ethical Issues

#### a. Algorithmic Bias

IoT security systems may disproportionately identify or exclude particular devices or people when biased data is used to train AI algorithms, leading to unfair treatment [59].

#### b. Transparency & Explainability

Explainable AI (XAI) techniques are necessary so that people can understand the rationale behind particular security decisions, especially in crucial industries like autonomous vehicles or medicine [59].

#### c. Accountability & Responsibility

Procedures for assigning responsibility must be clearly specified in case AI-IoT security solutions are ineffective or fail to identify an attack [60].

### 7.3. Governance Frameworks

#### a. Regulatory Compliance

Laws like GDPR, HIPAA, and cybersecurity regulations unique to IoT that set data management and protection requirements must be followed by AI-IoT security [61].

#### b. Auditing & Certification

Procedures for third-party auditing and certification aid in guaranteeing the privacy, robustness, and equity of AI models [62].

#### c. Ethical AI Governance Boards

Establishing governance boards is necessary for organizations to manage AI implementation in compliance with legal and ethical standards [63].



Table 4: Comparative Analysis of Privacy, Ethics, and Governance

Domain	Challenges	Best Practices
Privacy	Data leakage, unauthorized access	Federated Learning, Encryption, Data Minimization
Ethics	Algorithmic bias, lack of transparency	XAI, Bias Mitigation, Clear Accountability Policies
Governance	Regulatory non-compliance, poor oversight	Regular Audits, Legal Compliance, Governance Committees

## 7.4. Future Directions in Research

- Develop AI models that respond to recent privacy laws.
- Consistent AI governance guidelines for IoT across nations.
- Added ethical assessments in real time to IoT AI pipelines.



<b>PRIVACY, ETHICS, AND GOVERNANCE</b>		
 <b>Privacy</b>	 <b>Ethics</b>	 <b>Governance</b>
Data leakage, unauthorized access	Algorithmic bias, lack of transparency	Regulatory non-compliance, poor oversight
Challenges Federated Learning, Encryption, Data Minimization	XAI, Bias Mitigation, Clear Accountability Policies	Regular Audits, Legal Compliance, Governance Committees
Best Practices	Best Practices	Best Practices

Figure 5: Privacy, Ethics and Governance

## VIII. OPEN CHALLENGES & FUTURE DIRECTIONS IN AI FOR IOT SECURITY

It is a field with unsolved technical, ethical, and operational issues despite tremendous advancements [64]. These issues will shape IoT security innovation in the upcoming ten years.

### 8.1. Open Challenges

#### a. Scalability and Heterogeneity

The billions of devices that comprise IoT networks have different protocols, capabilities, and resource limitations [65]. AI solutions need to be small and reliable across a wide range of network architectures and devices.

#### b. Data Quality and Availability

The effectiveness of artificial intelligence is largely dependent on high-quality big data [66]. It is challenging to produce broad and significant sets of IoT security data because of privacy issues and device heterogeneity.

#### c. Adversarial Robustness

Adversarial attacks that confound detection techniques with simple inputs can nonetheless affect machine learning algorithms. It is essential that they be able to withstand these dangers in order to use the IoT in real time.

#### d. Real-Time Processing Constraints

IoT devices and edge nodes of constrained resources will perhaps not be capable of efficiently computing high-end AI models, impacting threat detection and response latency [67].

#### e. Governance and Regulatory Uncertainty

Laws on IoT security vary geographically, and worldwide paradigms on AI regulation are yet to be developed, resulting in challenges around compliance and interoperability [68].

## 8.2. Future Directions

### a. Federated and Distributed AI

Transition from central AI to federated learning and distributed wisdom may increase scalability, privacy, and security without compromising performance.

### b. Autonomous and Self-Healing Networks

AI-based IoT security systems will become increasingly endowed with self-healing capabilities that enable automatic anomaly detection, segmentation, and recovery without human intervention [69].

### c. Post-Quantum AI Security

As quantum computing advances further, AI-based IoT security will need to adopt post-quantum cryptography to protect information and communications.

### d. Multimodal Threat Intelligence AI

IoT security in the future will leverage multimodal AI—network traffic feeds, sensor feeds, and device behaviour patterns—combined to enhance detection accuracy [70].

### e. Ethical AI-First Frameworks

Adoption will be ethical if IoT AI solutions are developed with fairness, transparency, and privacy protection features.

Table 5: AI in IoT Security (2025–2035)

Timeline	Milestones
2025–2026	Standardization of IoT AI security protocols, wider adoption of federated learning
2027–2028	Deployment of lightweight, edge-optimized AI models for real-time threat detection
2029–2030	Integration of self-healing AI-enabled IoT networks across industries
2031–2032	Quantum-resistant AI algorithms implemented in IoT security
2033–2035	Fully autonomous, ethical AI IoT security ecosystems with global governance frameworks

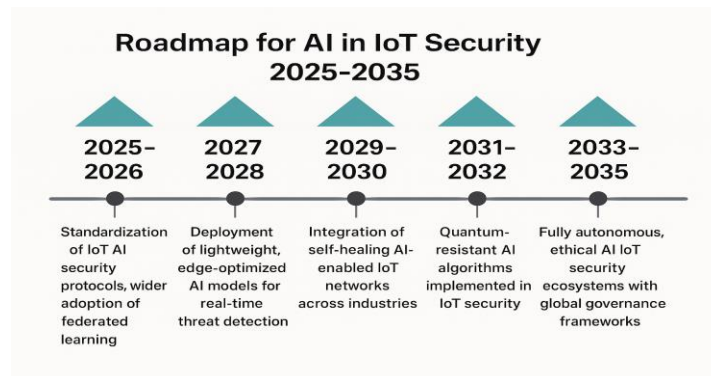


Figure 6: AI in IoT Security (2025–2035)

## IX. CONCLUSION

The combination of artificial intelligence (AI) with Internet of Things (IoT) security is a revolutionary development in the creation of intelligent, flexible, and robust cyber security defence systems. The volume of data generated by billions of connected devices keeps expanding the attack surface for cybercrime. The dynamic and sophisticated threat ecosystem of today will be too much for prior signature-based and rule-based security solutions to handle. Active defence, automated incident response, and real-time threat identification are made possible by artificial intelligence (AI) through the use of machine learning, deep learning, natural language processing, and anomaly detection.

The threat models that IoT systems face, AI-based security methods, and the architectures, datasets, evaluation paradigms, and adversarial defensive frameworks needed for their implementation have all been explored. By employing reinforcement learning-based agents to learn and adjust security policies and supervised machine learning models for malware detection, artificial intelligence (AI) enables defence mechanisms that expand in lockstep with new threats. Moreover, with AI blended with edge computing and fog computing, latency is resolved to enable real-time decision-making on device in mission-critical IoT applications such as healthcare monitoring, autonomous driving, and industrial control systems.

However, our analysis also identifies inherent issues—scalability, interoperability, adversarial vulnerabilities, and ethical control—before optimal deployment of AI-facilitated IoT security. Data privacy, the foundation of trust within IoT networks, must meet regulatory requirements by applying privacy-enhancing AI methods such as federated learning and homomorphic encryption. Moreover, building secure AI models against attacks is central to supporting countermeasures developed against changing attack trends, particularly model vulnerability attacks.

In the years ahead, the future of AI within IoT security is to progressively more independent, self-repairing, and quantum-proof defence systems. The path toward federated, decentralized, and multimodal AI will enhance threat detection and response without compromising user privacy or system performance. As ethical AI platforms develop and implement IoT security mechanisms, they will guarantee equity, openness, and responsibility—qualities essential to widespread adoption and public confidence.

Last but not least, AI is a developing foundation upon which future IoT protection will be constructed, not a security advantage of the Internet of Things. By using AI-based solutions to address open issues, the global IoT community can create a secure, reliable, and robust ecosystem that fosters innovation without compromising security. As a more connected society develops, IoT security and artificial intelligence will play a key role in maximizing the advantages of connectivity while reducing risks.

## REFERENCES

- [1]. Salama, R., Al-Turjman, F., Aeri, M., & Yadav, S. P. (2023, April). Internet of intelligent things (IoT)—an overview. In 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 801-805). IEEE.
- [2]. Kekevi, U., & Aydın, A. A. (2022). Real-time big data processing and analytics: Concepts, technologies, and domains. *Computer Science*, 7(2), 111-123.
- [3]. Milojicic, D., Faraboschi, P., Dube, N., & Roweth, D. (2021, February). Future of HPC: Diversifying heterogeneity. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 276-281). IEEE.
- [4]. Cho, H., Kim, H. J., Lee, J., Kim, C. M., Bae, J., & Nam, T. J. (2021, June). IoTIZER: A Versatile Mechanical Hijacking Device for Creating Internet of Old Things. In Proceedings of the 2021 ACM Designing Interactive Systems Conference (pp. 90-103).
- [5]. Khadri, S. W., Mohammed, I. K., Rasheed, H., & Gunda, S. K. R. (2025). Adaptive Trade Exception Handling in Financial Institutions: A Reinforcement Learning Approach with Dynamic Policy Optimization. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 19-23.
- [6]. Janamolla, K., Sultana, G. S., Aasimuddin, F. M., Mohammed, A. F., & Pasha, F. S. A. P. (2025). Integrating Blockchain and AI for Efficient Trade Exception Handling: A Case Study in Cross-Border Settlements. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 24-30.
- [7]. Mohammed, N. U., Mohammed, Z. A., Gunda, S. K. R., Mohammed, A., & Khaja, M. U. Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence.
- [8]. Mohammed, A., Mohammed, N. U., Gunda, S. K. R., & Mohammed, Z. Fundamental Principles of Network Security.
- [9]. Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, 80, 3554-3559.
- [10]. Sander, P. M., Griebeler, E. M., Klein, N., Juarbe, J. V., Wintrich, T., Revell, L. J., & Schmitz, L. (2021). Early giant reveals faster evolution of large body size in ichthyosaurs than in cetaceans. *Science*, 374(6575), eabf5787.
- [11]. Heinrich, F., Klapper, P., & Pruckner, M. (2021). A comprehensive study on battery electric modeling approaches based on machine learning. *Energy Informatics*, 4(Suppl 3), 17.
- [12]. You, J. W., Ma, Q., Lan, Z., Xiao, Q., Panoiu, N. C., & Cui, T. J. (2021). Reprogrammable plasmonic topological insulators with ultrafast control. *Nature communications*, 12(1), 5468.
- [13]. Zhang, H., Liu, B., & Wu, H. (2021). Smart grid cyber-physical attack and defense: A review. *IEEE Access*, 9, 29641-29659.
- [14]. Mohammed, S., Sultana, G., Aasimuddin, F. M., & Chittoju, S. S. R. AI-Driven Automated Malware Analysis.
- [15]. Franzoni, F., & Daza, V. (2022). Sok: Network-level attacks on the bitcoin p2p network. *IEEE Access*, 10, 94924-94962.
- [16]. Aasimuddin, M., & Mohammed, S. AI-Generated Deepfakes for Cyber Fraud and Detection.
- [17]. Prabhaker, N., & Bopche, G. S. (2024). 10 Data-Level Cyber. *Cloud of Things: Foundations, Applications, and Challenges*, 173.

- [18]. Ansari, M. F. Redefining Cybersecurity: Strategic Integration of Artificial Intelligence for Proactive Threat Defense and Ethical Resilience.
- [19]. Akhunzada, A., Al-Shamayleh, A. S., Zeadally, S., Almogren, A., & Abu-Shareha, A. A. (2024). Design and performance of an AI-enabled threat intelligence framework for IoT-enabled autonomous vehicles. *Computers and Electrical Engineering*, 119, 109609.
- [20]. Mohammed, A. K., Ansari, S. F., Ahmed, M. I., & Mohammed, Z. A. Boosting Decision-Making with LLM-Powered Prompts in PowerBI.
- [21]. Chittoju, S. S. R., Kolla, S., Ahmed, M. A., & Mohammed, A. R. Synergistic Integration of Blockchain and Artificial Intelligence for Robust IoT and Critical Infrastructure Security.
- [22]. Thatikonda, R., Vaddadi, S. A., Arnepalli, P. R. R., & Padthe, A. (2023). Securing biomedical databases based on fuzzy method through blockchain technology. *Soft Computing*, 1-9.
- [23]. Mohammed, Z., Mohammed, N. U. M., Mohammed, A., Gunda, S. K. R., & Ansari, M. A. A. (2025). AI-Powered Energy Efficient and Sustainable Cloud Networking. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 31-36.
- [24]. Chittoju, S. R., & Ansari, S. F. (2024). Blockchain's Evolution in Financial Services: Enhancing Security, Transparency, and Operational Efficiency. *International Journal of Advanced Research in Computer and Communication Engineering*, 13(12), 1-5.
- [25]. Teles, G., Rodrigues, J. J., Rabêlo, R. A., & Kozlov, S. A. (2021). Comparative study of support vector machines and random forests machine learning algorithms on credit operation. *Software: practice and experience*, 51(12), 2492-2500.
- [26]. Gandhi, U. D., Malarvizhi Kumar, P., Chandra Babu, G., & Karthick, G. (2021). Sentiment analysis on twitter data by using convolutional neural network (CNN) and long short-term memory (LSTM). *Wireless Personal Communications*, 1-10.
- [27]. Kerkouche, R., Acs, G., Castelluccia, C., & Genevès, P. (2021, April). Privacy-preserving and bandwidth-efficient federated learning: An application to in-hospital mortality prediction. In *Proceedings of the conference on health, inference, and learning* (pp. 25-35).
- [28]. Munir, A., Blasch, E., Kwon, J., Kong, J., & Aved, A. (2021). Artificial intelligence and data fusion at the edge. *IEEE Aerospace and Electronic Systems Magazine*, 36(7), 62-78.
- [29]. Balamagary, S., Mohammed, N., Mohammed, S., & Begum, A. (2025). AI-Driven Behavioural Insights for Ozempic Drug Users. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 10-13.
- [30]. Peterson, J. M., Leevy, J. L., & Khoshgoftaar, T. M. (2021, August). A review and analysis of the bot-iot dataset. In *2021 IEEE International Conference on Service-Oriented System Engineering (SOSE)* (pp. 20-27). IEEE.
- [31]. Hossain, M., Rudro, R. A. M., Razzaque, R., & Nur, K. (2024, December). Machine learning approaches for detecting iot botnet attacks: A comparative study of n-baiot dataset. In *2024 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 1-7). IEEE.
- [32]. Tseng, S. M., Wang, Y. Q., & Wang, Y. C. (2024). Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset. *Future Internet*, 16(8), 284.
- [33]. Miao, J., & Zhu, W. (2022). Precision-recall curve (PRC) classification trees. *Evolutionary intelligence*, 15(3), 1545-1569.
- [34]. Tafvizi, A., Avci, B., & Sundararajan, M. (2022). Attributing auc-roc to analyze binary classifier performance. *arXiv preprint arXiv:2205.11781*.
- [35]. Yang, Y., Zhao, L., Li, Y., Zhang, H., Li, J., Zhao, M., ... & Li, K. (2022, February). Inless: a native serverless system for low-latency, high-throughput inference. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (pp. 768-781).
- [36]. Padthe, A., Thatikonda, R., & Ashtagi, R. (2024). Leveraging generative adversarial networks for cross-modal image processing. In *Artificial Intelligence and Information Technologies* (pp. 176-180). CRC Press.
- [37]. Shao, R., Shi, Z., Yi, J., Chen, P. Y., & Hsieh, C. J. (2021). On the adversarial robustness of vision transformers. *arXiv preprint arXiv:2103.15670*.
- [38]. Mohammed, A., Sultana, G., Aasimuddin, F. M., & Mohammed, S. (2025). Leveraging Natural Language Processing for Trade Exception Classification and Resolution in Capital Markets: A Comprehensive Study. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 14-18.
- [39]. Khadri, W., Reddy, J. K., Mohammed, A., & Kiruthiga, T. (2024, July). The Smart Banking Automation for High Rated Financial Transactions using Deep Learning. In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 686-692). IEEE.
- [40]. Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON\_IoT datasets. *Sustainable Cities and Society*, 72, 102994.



- [41]. Naser, S., Bariah, L., Muhaidat, S., Sofotasios, P. C., Al-Qutayri, M., Damiani, E., & Debbah, M. (2022). Toward federated-learning-enabled visible light communication in 6G systems. *IEEE Wireless Communications*, 29(1), 48-56.
- [42]. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating artificial intelligence with zero trust architecture: Enhancing adaptive security in modern cyber threat landscape. *International Journal of Research and Analytical Reviews*, 9, 712-728.
- [43]. Kaliappan, C. P., Palaniappan, K., Ananthavadeivel, D., & Subramanian, U. (2024). Advancing IoT security: a comprehensive AI-based trust framework for intrusion detection. *Peer-to-Peer Networking and Applications*, 17(5), 2737-2757.
- [44]. Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2021). A survey on adversarial attacks and defences. *CAAI Transactions on Intelligence Technology*, 6(1), 25-45.
- [45]. Wang, S., Ko, R. K., Bai, G., Dong, N., Choi, T., & Zhang, Y. (2023). Evasion attack and defense on machine learning models in cyber-physical systems: A survey. *IEEE communications surveys & tutorials*, 26(2), 930-966.
- [46]. Tian, Z., Cui, L., Liang, J., & Yu, S. (2022). A comprehensive survey on poisoning attacks and countermeasures in machine learning. *ACM Computing Surveys*, 55(8), 1-35.
- [47]. Hu, H., Salcic, Z., Sun, L., Dobbie, G., Yu, P. S., & Zhang, X. (2022). Membership inference attacks on machine learning: A survey. *ACM Computing Surveys (CSUR)*, 54(11s), 1-37.
- [48]. Shen, Y., & Qin, Z. (2024). Detection, differentiation and localization of replay attack and false data injection attack based on random matrix. *Scientific Reports*, 14(1), 2758.
- [49]. Jia, X., Zhang, Y., Wu, B., Ma, K., Wang, J., & Cao, X. (2022). Las-at: adversarial training with learnable attack strategy. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 13398-13408).
- [50]. Alemi Pedram, K. (2021). Input Validation and Input Sanitization for Web Applications.
- [51]. Tao, G., Liu, Y., Shen, G., Xu, Q., An, S., Zhang, Z., & Zhang, X. (2022, May). Model orthogonalization: Class distance hardening in neural networks for better security. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 1372-1389). IEEE.
- [52]. You, Z., Cui, L., Shen, Y., Yang, K., Lu, X., Zheng, Y., & Le, X. (2022). A unified model for multi-class anomaly detection. *Advances in Neural Information Processing Systems*, 35, 4571-4584.
- [53]. Syed, W. K., Mohammed, A., Reddy, J. K., & Dhanasekaran, S. (2024, July). Biometric Authentication Systems in Banking: A Technical Evaluation of Security Measures. In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 1331-1336). IEEE.
- [54]. Kalejaiye, A. N. (2024). Adversarial machine learning for robust cybersecurity: strengthening deep neural architectures against evasion, poisoning, and model-inference attacks. *International Journal of Computer Applications Technology and Research*, 13(12), 72-95.
- [55]. Imoize, A. L., Balas, V. E., Solanki, V. K., Lee, C. C., & Obaidat, M. S. (Eds.). (2023). *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things* (pp. 1-460). Boca Raton, FL, USA: CRC press.
- [56]. Ganesh, P., Tran, C., Shokri, R., & Fioretto, F. (2025, June). The data minimization principle in machine learning. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (pp. 3075-3093).
- [57]. Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. *Knowledge-Based Systems*, 216, 106775.
- [58]. Pratomo, A. B., Mokodenseho, S., & Aziz, A. M. (2023). Data encryption and anonymization techniques for enhanced information system security and privacy. *West Science Information System and Technology*, 1(01), 1-9.
- [59]. Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkänen, K., & Kujala, S. (2023). Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, 159, 107197.
- [60]. Mohammed, N., Mohammed, A. F., & Balammagary, S. (2025). Ransomware in Healthcare: Reducing Threats to Patient Care. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(2), 27-33.
- [61]. Mohammed, S., DDS, Dr. S. T. A., Mohammed, N., & Sultana, W. (2024). A review of AI-powered diagnosis of rare diseases. *International Journal of Current Science Research and Review*, 07(09).  
<https://doi.org/10.47191/ijcsrr/v7-i9-01>
- [62]. Bishop, K. J., & Carlson, K. M. (2022). The role of third-party audits in ensuring producer compliance with the Roundtable on Sustainable Palm Oil (RSPO) certification system. *Environmental Research Letters*, 17(9), 094038.
- [63]. Mohammed, A. K., & Ansari, M. A. (2024). The Impact and Limitations of AI in Power BI: A Review . *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, , Pp. 23-27, 2024. , 7(7), 24–27.

- [64]. Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A., & Jin, Z. (2023). UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions. *IEEE Transactions on Intelligent Vehicles*, 9(4), 4583-4605.
- [65]. Wibisono, A., Sammon, D., & Heavin, C. (2022). Data availability issues: decisions as patterns of action. *Journal of Decision Systems*, 31(sup1), 241-254.
- [66]. Althati, C., Tomar, M., & Malaiyappan, J. N. A. (2024). Scalable machine learning solutions for heterogeneous data in distributed data platform. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, 4(1), 299-309.
- [67]. Katkov, S., Liotta, A., & Vietti, A. (2024, November). Benchmarking whisper under diverse audio transformations and real-time constraints. In *International Conference on Speech and Computer* (pp. 82-91). Cham: Springer Nature Switzerland.
- [68]. Ahsan, T., Mirza, S. S., Al-Gamrh, B., Bin-Feng, C., & Rao, Z. U. R. (2021). How to deal with policy uncertainty to attain sustainable growth: the role of corporate governance. *Corporate Governance: The International Journal of Business in Society*, 21(1), 78-91.
- [69]. Tan, Y. J., Susanto, G. J., Anwar Ali, H. P., & Tee, B. C. (2021). Progress and roadmap for intelligent self-healing materials in autonomous robotics. *Advanced Materials*, 33(19), 2002800.
- [70]. Moraliyage, H., Sumanasena, V., De Silva, D., Nawaratne, R., Sun, L., & Alahakoon, D. (2022). Multimodal classification of onion services for proactive cyber threat intelligence using explainable deep learning. *IEEE Access*, 10, 56044-56056.