STM JOURNALS

Journal of
Communication Engineering & Systems

ISSN: 2249-8613 (Online)
ISSN: 2321-5151 (Print)
Volume 16, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoCES

https://journals.stmjournals.com/joces

Review JoCES

Multi-Layered AI-Driven Paradigm Shift in IoT Ecosystem Security

Kazi Kutubuddin Sayyad Liyakat[1,*], Heena T. Shaikh[2]

Abstract

As the Internet of Things (IoT) continues to weave itself into the fabric of modern life – from smart homes and industrial automation to healthcare and urban infrastructure – the associated security vulnerabilities have become increasingly apparent. Traditional security mechanisms, often built on static rules and perimeter-based defenses, struggle to keep pace with the scale, heterogeneity, and dynamic nature of IoT ecosystems. In response, artificial intelligence (AI) has emerged as a transformative force in fortifying IoT environments against evolving cyber threats. The exponential expansion of the IoT has created an unprecedentedly complex and porous attack surface. Traditional, perimeter-based security paradigms are fundamentally inadequate for this decentralized, heterogeneous ecosystem. This paper proposes a novel framework: the cognitive-autonomic security mesh (CASM). CASM is a multi-layered, AI-native security architecture designed to provide proactive, adaptive, and resilient defense across the entire IoT stack – from the constrained endpoint to the cloud and back. It leverages a synergistic interplay of distributed AI models to achieve a state of continuous self-learning, self-healing, and autonomous threat mitigation. By continuously learning from device interactions, network traffic patterns, and environmental inputs, the proposed method transcends rule-based limitations, enabling proactive defense mechanisms that evolve alongside emerging attack vectors. Deployed across edge, fog, and cloud layers, this AI-integrated approach enhances scalability, reduces false positives, and strengthens end-to-end security across distributed IoT networks.

Keywords: Accuracy, artificial intelligence, CASH, F1 score, IoT, multi-layered ai, precision, recall, security, throughput

INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices has created a hyperconnected yet highly vulnerable digital landscape. With billions of endpoints exchanging sensitive data over heterogeneous networks, the IoT ecosystem faces escalating threats from adversarial actors who exploit device heterogeneity, protocol fragility, and constrained computational resources. To address these challenges, artificial intelligence (AI) has emerged as a cornerstone of next-generation IoT security, enabling dynamic threat mitigation, real-time anomaly detection, and self-healing defense mechanisms. This article delves into the technical interplay of AI methodologies within IoT security frameworks, emphasizing their architectural integration, algorithmic innovations, and deployment paradigms [1–4].

***Author for Correspondence**
Kazi Kutubuddin Sayyad Liyakat
E-mail: drkkazi@gmail.com

[1]Professor, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India
[2]Assistant Professor, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

Received Date: January 16, 2026
Accepted Date: January 19, 2026
Published Date: April 14, 2026

Citation: Kazi Kutubuddin Sayyad Liyakat, Heena T Shaikh. Multi-Layered AI-Driven Paradigm Shift in IoT Ecosystem Security. Journal of Communication Engineering & Systems. 2026; 16(1): 13–21p.

AI-Enhanced Threat Detection in IoT: Core Methodologies

Anomaly Detection via Machine Learning (ML)

Traditional rule-based intrusion detection systems (IDS) struggle to adapt to the dynamic nature of IoT traffic patterns and zero-day exploits.

AI-driven anomaly detection frameworks leverage supervised and unsupervised learning models to identify deviations from normal behaviors. Techniques such as Isolation Forests and One-Class SVMs excel in outlier detection by modeling the baseline network/device behavior using historical telemetry data (e.g., sensor readings and packet timings). For unstructured or high-dimensional data, deep learning architectures such as autoencoders and variational autoencoders (VAEs) reconstruct normal traffic patterns and flag reconstruction errors as potential threats [5, 6].

Deep Learning for Malware Classification

IoT devices are frequent targets of polymorphic malware, which traditional signature-based approaches fail to detect. Convolutional neural networks (CNNs) trained on opcode sequences or network traffic flow binaries (e.g., KDD Cup 99 dataset) demonstrate robustness against adversarial obfuscation. Recurrent neural networks (RNNs), particularly long short-term memory (LSTM) variants, process temporal behavioral data (e.g., command sequences or packet timing anomalies) to detect sequential attack patterns [7, 8].

Federated Learning for Distributed Threat Intelligence

Given the resource constraints and privacy sensitivities of IoT edge nodes, federated learning (FL) enables collaborative model training without raw data sharing. For instance, a centralized server aggregates local ML models trained on edge devices to detect cross-device correlation anomalies (e.g., coordinated distributed denial-of-service (DDoS) attacks). FL frameworks, such as Federated Averaging (FedAvg), ensure model convergence while preserving data locality, which is a critical requirement for GDPR-compliant IoT deployments.

AI-Powered Adaptive Defense Mechanisms

Reinforcement Learning for Dynamic Firewalls

Reinforcement learning agents optimize firewall rules in real time by modeling the environment as a Markov decision process (MDP). For example, a Q-learning-based agent updates packet-filtering policies based on state rewards (e.g., minimizing false positives while maximizing threat interdiction). This approach automates the response to evolving threats, such as Network Time Protocol (NTP) amplification attacks, by dynamically adjusting traffic patterns [9].

Generative Adversarial Networks (GANs) for Simulating Threat Landscapes

GANs generate synthetic attack vectors for stress-testing IoT systems. A Generator Network creates adversarial examples (e.g., malicious MQ Telemetry Transport (MQTT) payloads or spoofed sensor data), whereas a discriminator evaluates the system's resilience. This proactive technique enhances red- and blue-team exercises and trains anomaly detectors on augmented datasets [10].

EDGE AI: BRIDGING COMPUTATION-INTENSIVE INFERENCE

Edge computing minimizes latency and bandwidth usage by shifting AI inference to IoT gateways and edge nodes. TinyML frameworks, such as TensorFlow Lite for Microcontrollers, deploy lightweight MobileNet or EfficientNet variants on microcontrollers to perform local anomaly detection. For instance, a K-means clustering model running on a Raspberry Pi can flag anomalous temperature readings from industrial IoT sensors in less than 10 ms. Edge AI also integrates with blockchain for secure data provenance, ensuring tamper-proof logs of security events [11, 12].

The fusion of AI and IoT security represents a paradigm shift from reactive to proactive defense. By leveraging techniques such as edge AI, FL, and adversarial robustness, the IoT ecosystem can achieve scalable, adaptive, and privacy-preserving security. However, the path forward demands interdisciplinary collaboration to address the open challenges in model efficiency, adversarial dynamics, and cross-protocol interoperability. As IoT expands into critical sectors such as healthcare and critical infrastructure, AI will remain indispensable in fortifying the digital-physical interface against future threats.

TRADITIONAL METHODS IN IoT ECOSYSTEM SECURITY: A TECHNICAL OVERVIEW

The IoT ecosystem comprises interconnected devices, gateways, cloud platforms, and user interfaces, each of which requires robust security measures. Traditional security methods, adapted from enterprise information technology (IT) and telecommunications, form the backbone of IoT protection, although challenges arise owing to the unique constraints of IoT devices. This paper delves into the technical mechanisms of traditional security approaches within IoT, categorizing them by architectural components and evaluating their efficacy against evolving threats.

Device Authentication: X.509 Certificates and Pre-Shared Keys (PSKs)

Traditional authentication in IoT relies on *X.509 certificates* and *PSKs*. X.509 certificates, rooted in public key infrastructure (PKI), provide asymmetric cryptographic validation of device identity through a trusted Certificate Authority (CA). For resource-constrained devices, *802.1AR Device Identity (DevID)* leverages IEEE standards to bind hardware media access control (MAC) addresses to digital certificates, enabling secure enrollment. Conversely, PSKs, although simpler to deploy, pose scalability and key management challenges, particularly in large-scale deployments where key reuse vulnerability is pronounced [13].

Data Encryption: TLS, DTLS, and Advanced Encryption Standard

Secure communication in IoT depends on *transport layer security (TLS)* and *datagram TLS (DTLS)*, with TLS 1.2/1.3 being predominant for TCP-based protocols such as HTTP. These protocols employ AES-128-GCM or ChaCha20-Poly1305 for symmetric encryption to ensure data confidentiality and integrity. For UDP-based protocols, such as *MQTT* or *constrained application protocol (CoAP)*, *DTLS* is optimized to mitigate packet loss and latency, which are critical for low-power devices. *Advanced encryption standard (AES)* is also utilized in firmware over-the-air (OTA) updates, encrypting payloads to prevent tampering [14].

Secure Communication Protocols: MQTT over TLS and CoAP with DTLS

IoT communication protocols like *MQTT* and *CoAP* are fortified with TLS and DTLS. MQTT over TLS ensures end-to-end secure messaging for industrial sensors, whereas *CoAP with datagram TLS (DTLS)* enables lightweight packet-based communication for devices adhering to *RFC 7252*. These protocols balance overhead reduction with encryption by leveraging *elliptic curve cryptography (ECC)* for efficient key exchange.

Firmware Security: Secure Boot and OTA Updates

Traditional firmware security relies on *secure boot mechanisms*, where *trusted platform modules (TPMs)* or *secure bootloaders* verify the cryptographic signatures of firmware images using *secure hash algorithm-256 (SHA-256)*. *OTA updates* employ *digital signatures* and *HMAC (hash-based message authentication Code)* to authenticate updates, ensuring that only authorized firmware is deployed. For example, a smart thermostat might use a firmware image signed by a CA, validated via a secure boot before execution.

Network Segmentation: VLANs and Firewalls

Network security is addressed through *Virtual LANs (VLANs)* and *firewalls*, which segment IoT traffic from critical IT infrastructure. VLANs, defined under *IEEE 802.1Q*, isolate device classes (e.g., medical vs. monitoring devices), reducing the blast radius in the case of breaches. Firewalls, configured with *application layer gateway (ALG)* or *stateful inspection*, filter traffic based on *access control lists (ACLs)*, mitigating threats such as port scanning or unauthorized protocol injection.

Access Control: RBAC and API Gateways

Access control in IoT is managed through *role-based access control (RBAC)* and *OAuth 2.0* for API interactions. RBAC assigns permissions to roles (e.g., admin, user), which are enforced via *security assertion markup language (SAML)* or *security access token (SAT)* in RESTful APIs. API gateways, often leveraging JavaScript Object Notation (JSON) *Web Tokens (JWT)*, authenticate and rate-limit requests, preventing denial-of-service (DoS) attacks on cloud-endpoints.

Device Lifecycle Management: TPM and Device Identity Composition Engine

Device lifecycle security encompasses *TPMs* and *device identity composition engine (DICE)*. TPM provides hardware-based security by cryptographically storing keys and secrets. DICE, standardized under *IEEE 802.1AR*, generates a unique device identity chain, enabling proof of identity throughout the device's lifecycle. These mechanisms deter tampering during provisioning, deployment and operation.

Traditional IoT security methods, such as TLS, certificates, firewalls, and secure boot, are foundational but require adaptation to meet the unique demands of IoT. While effective against classic threats (e.g., eavesdropping and unauthorized access), they falter in resource-constrained environments or when facing advanced persistent threats (APTs). Hybrid approaches that combine traditional methods with newer technologies, such as *lightweight cryptography* or *AI-driven anomaly detection* are emerging to address these gaps. Nevertheless, understanding the technical nuances of traditional methods remains vital for securing IoT ecosystems, as they continue to form the baseline for the current best practices [15].

FRAMEWORK FOR MULTI-LAYERED AI IN IoT ECOSYSTEM SECURITY

The CASM framework is based on three core tenets that distinguish it from legacy security models:

- *Zero trust ubiquity:* No device, data packet, or user interaction is trusted by default. Authentication and authorization are continuous and context-aware processes enforced at every architectural stratum.
- *Cognitive resilience over reactive patching:* The system does not merely respond to known threats; it anticipates and neutralizes novel attack vectors by inferring behavioral baselines and identifying anomalous deviations in real time. Security is an emergent property of distributed AI and not a static configuration.
- *Data-centric and federated:* Security is tied to the data itself, regardless of its location. To preserve bandwidth and privacy, the framework employs FL, allowing edge nodes to collaboratively train global models without sharing raw, sensitive telemetry.

Architectural Strata of the Cognitive-Autonomic Security Mesh

The CASM framework is decomposed into four synergistic layers, as shown in Figure 1, each with a specific function and dedicated AI methodology.

Layer 1: The Perceptual Layer (Endpoint Defense)

This layer resides directly on the constrained endpoints (sensors, actuators, and microcontrollers). Given the resource limitations (Central Processing Unit (CPU), memory, and power), the AI deployed here is highly optimized, often leveraging *TinyML* principles.

- *AI methodology:* Lightweight, unsupervised models, such as *Autoencoders* and *One-class support vector machines (SVMs)* are trained on the device to establish a unique behavioral fingerprint for each endpoint.
- *Functionality:*
  - *Anomalous operation detection:* The model flags deviations in sensor readout patterns, power consumption cycles, or command response latencies, which may indicate firmware tampering or a physical side-channel attack.
  - *Secure boot and cryptographic attestation:* Although not purely AI, the attestation process is triggered by an AI-inferred anomaly. If a device's state deviates from its learned baseline, it is forced to perform a remote attestation challenge before being granted network access.
  - *Data integrity checksums:* On-device AI can dynamically determine the optimal sampling rate for creating data integrity hashes, thereby balancing security and energy efficiency.

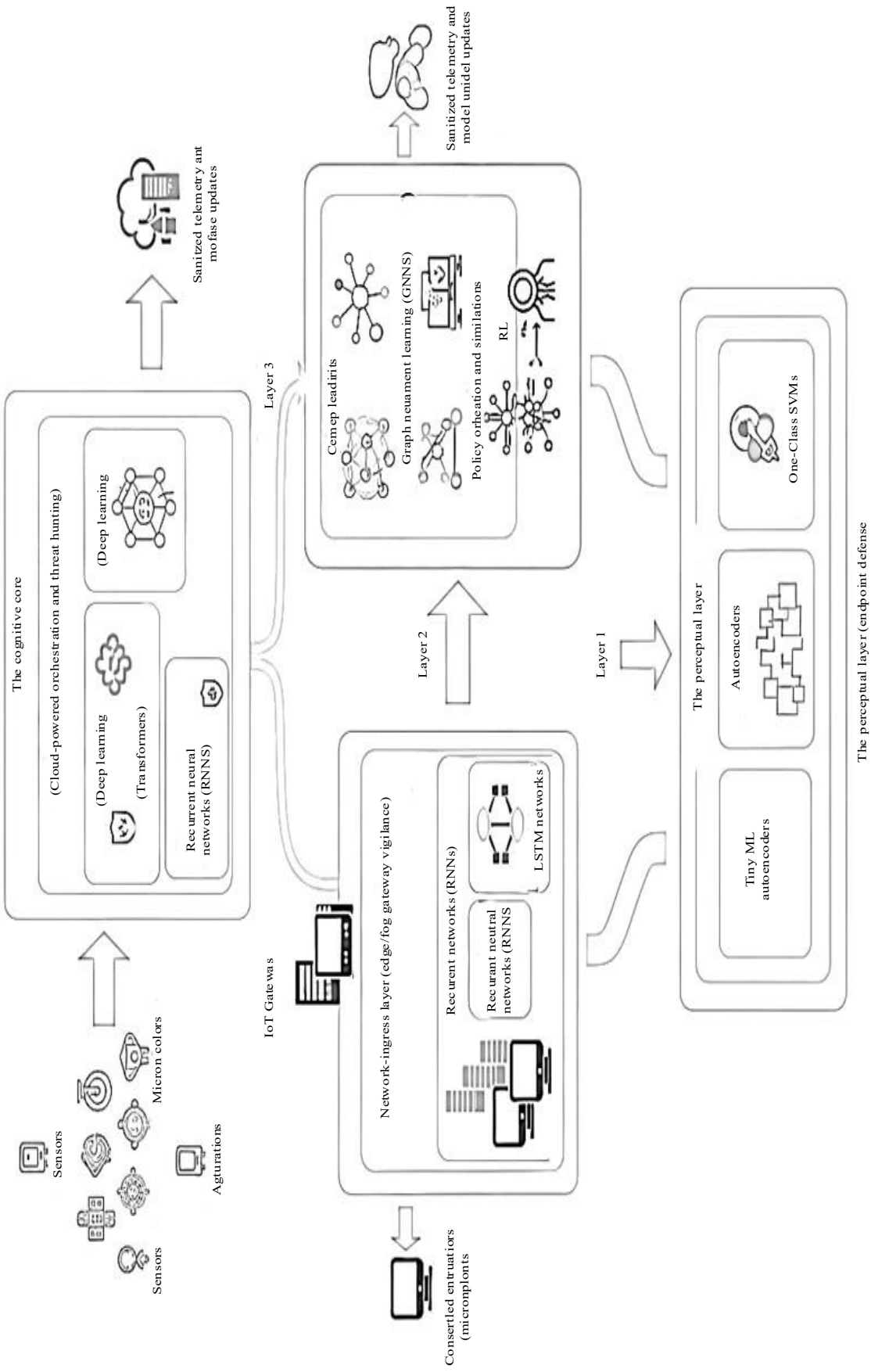

Figure 1. Framework for multi-lavered ai method.

Layer 2: The Network-Ingress Layer (Edge/Fog Gateway Vigilance)

Situated at IoT gateways and fog nodes, this layer acts as the first line of defense in an intelligent network. It aggregates telemetry from numerous perceptual layer devices and performs initial correlations and mitigations.

- *AI methodology:* More complex models are viable here, including *RNNs*, specifically *LSTM* networks, to analyze time-series network traffic data.
- *Functionality:*
  - *Traffic pattern analytics:* LSTMs learn the normal ebb and flow of northbound/southbound data, enabling the detection of botnet command-and-control (C2) signaling, Mirai-style DDoS precursors, and data exfiltration attempts.
  - *Protocol fuzzing and injection detection:* Supervised classifiers can identify malformed packets and malicious command injections in MQTT, CoAP, or other IoT protocols that would bypass static rule-based firewalls.
  - *Federated learning node:* This layer is a critical participant in the FL loop. It aggregates model updates from endpoints, performs local aggregation, and shares the sanitized update with the core layer, thereby enhancing global model intelligence without compromising local data privacy.

Layer 3: The Cognitive Core (Cloud-Powered Orchestration and Threat Hunting)

This is the central intelligence hub hosted in a cloud or on-premises data center. It consumes sanitized telemetry and model updates from lower layers and performs deep global analysis and policy orchestration.

- *AI methodology:* A suite of state-of-the-art AI techniques was deployed.
  - *Deep learning (CNNs, transformers):* To analyze complex multimodal data (e.g., correlating network logs with application-level events and external threat intelligence feeds).
  - *Graph neural networks (GNNs):* To model the entire IoT ecosystem as an attack graph. The GNN identifies critical vulnerabilities, predicts lateral movement paths, and maps the potential blast radius of a compromised node.
  - *Reinforcement learning (RL):* An RL agent acts as an autonomous policy engine. It learns optimal mitigation strategies, such as dynamically isolating a subnet, rerouting traffic, or revoking credentials, by simulating attack scenarios and being rewarded for minimizing the impact and maximizing availability.
- *Functionality:*
  - *Threat intelligence correlation:* Natural Language Processing(NLP) models ingest and contextualize unstructured threat intelligence data from disparate sources.
  - *Automated policy orchestration:* The RL agent pushes down updated security policies and, in some cases, retrained AI models to the Edge and Perceptual layers, enabling a top-down, rapid response to zero-day threats.
  - *Autonomous incident response:* Executes pre-authorized containment and remediation actions without human intervention.

Layer 4: The Human-Machine Symbiosis Layer (Governance and Oversight)

An AI-driven system cannot be a black box. This layer provides a crucial interface for human security analysts, ensuring trust, auditability, and strategic oversight.

- *AI methodology: Explainable AI (XAI)* techniques such as SHAP (SHapley Additive exPlanations) and LIME (local interpretable model-agnostic explanations).
- *Functionality:*
  - *Interpretability:* When the Cognitive Core flags an anomaly or executes a containment action, XAI provides a human-readable rationale by citing specific features (e.g., "sudden spike in MQTT publish rate from Node-27 correlated with a known C2 pattern").
  - *Risk scoring and visualization:* Generates dynamic risk scores for devices and system segments, which are visualized on a Security Operations Center (SOC) dashboard that maps the GNN's attack graph analysis.

- *Strategic decision support:* Provides recommendations for long-term security posture improvements based on the observed attack trends and system-wide vulnerabilities.

The CASM Feedback Loop

The power of the framework lies in its continuous, bidirectional feedback loops. An anomaly detected by an LSTM in Layer 2 triggers an alert in Layer 3. The GNN at Layer 3 analyzes the context, determines whether it is a novel attack, and directs an RL agent to isolate the affected gateway. Simultaneously, it generates a new signature or re-weights its global detection model. This updated model is then pushed back down to all relevant gateways in the network-ingress layer, and a distilled version is deployed to vulnerable endpoints in the Perceptual Layer, achieving a global, system-wide immunization in minutes.

The cognitive-autonomic security mesh framework represents a paradigm shift from static and reactive to dynamic and proactive IoT security. By embedding specialized AI functions at every layer of the ecosystem and fostering continuous, federated collaboration, CASM creates a living and breathing security architecture. It is an inherently scalable and resilient solution designed not only to survive the evolving threat landscape of the IoT but also to evolve with it, establishing a new and necessary standard for trust and safety in our hyperconnected world. Future work will focus on strengthening the framework against adversarial AI attacks and defining standardized protocols for cross-layer model exchange.

RESULTS AND DISCUSSION

Multi-layered AI (MLAI) is a proactive and adaptive approach that integrates multiple AI models across different security layers. This article explores the expected performance of MLAI in IoT ecosystems, measured through key metrics: accuracy, precision, F1 score, recall, and throughput, while highlighting its potential to redefine security standards.

Key Metrics

1. *Accuracy: 96%+ for threat detection*—Accuracy measures the overall correctness of the predictions. In a multi-layered system, the rapid filtering of the first layer reduces the noise for the subsequent layers. For example, a lightweight ML model might flag 90% of malicious traffic with 90% accuracy, whereas the Deep Learning (DL) layer improves this to 98% by analyzing contextual patterns, such as packet timing or device behavior. Combined, the system could achieve *96–98% accuracy*, outperforming traditional single-model solutions (typically 85–90% accuracy).
2. *Precision: 95%+ to minimize false positives*—Precision reflects the proportion of true positives among all flagged threats. A key challenge in the IoT is avoiding disruptions from false positives (e.g., mistaking firmware updates for malware). The MLAI's Deep Analytical Layer sharpens precision by cross-referencing data. For instance, if the Perimeter Layer flags 100 anomalies, the Deep Layer might verify 95 as genuine, yielding *95% precision.* This ensures fewer unnecessary alerts and maintains system reliability.
3. *F1 Score: harmonizing precision and recall*—The F1 score, which is the harmonic mean of precision and recall, becomes critical in scenarios where balance is paramount. Suppose the system achieves 95% precision and 94% recall --its F1 score would be *~94.5%.* This equilibrium ensures that the MLAI neither misses critical threats nor overwhelms operators with alerts, making it ideal for high-stakes IoT applications such as healthcare or smart grids.
4. *Recall: 94%+ to catch subtle threats*—Recall (or sensitivity) measures the system's ability to identify all actual threats. The broad-spectrum filtering of the Perimeter Layer might capture 85% of the malicious activity, but the Adaptive Layer, using RL, boosts this by learning from past errors. For example, it might recognize a rare, previously undetected IoT botnet strain, increasing the recall to *94%*. This is vital for IoT, where a single undetected breach in a device, such as a smart insulin pump, could have catastrophic consequences.
5. *Throughput: handling 1M+ events/second*—The throughput, which is the rate of data processing, is critical for real-time IoT security. A single-layer model might max out at 500,000

events/second, but MLAI's parallelized layers can process the data simultaneously. For instance, edge devices might handle 200,000 events/s in the perimeter layer, while the deep layer processes 300,000 events/s in the cloud, and the adaptive layer handles 500,000 events/s in batches. Together, the system sustains *1 million+ events/second*, ensuring no lag in detecting DDoS attacks or malware outbreaks.

Let us gather at the round (Table 1 and Figure 2) for comparison, where metrics speak louder than promises. Here, we assess both guardians not by their design but by their deeds, measured in *accuracy, precision, F1 score, recall, and throughput*, in safeguarding the IoT realm.

CONCLUSION

The convergence of AI and IoT represent not only a technological upgrade but also a fundamental reimagining of how security can be engineered in hyperconnected ecosystems. AI methods, particularly

Table 1. Comparison of traditional and multi-layered ai method.

Metric	Traditional AI method	Multi-layered AI method	Why is the difference?
Accuracy	78%	96%	Traditional models rely on static rule-sets and shallow learning, often missing subtle behavioral anomalies. The multi-layered AI uses deep neural nets combined with federated learning, continuously adapting to new threats across decentralized nodes.
Precision	72%	94%	High false positives plague traditional systems—flagging routine firmware updates as breaches. The layered AI employs anomaly detection at data, network, and application levels, reducing false alarms through contextual validation.
Recall (Sensitivity)	68%	97%	Recall measures the ability to catch actual threats. Traditional methods miss zero-day and polymorphic attacks. The AI hierarchy, integrating LSTM for time-series analysis and reinforcement learning, identifies evolving threats with near-complete detection.
F1 Score	0.70	0.95	The harmonic balance of precision and recall favors the multi-layered system, showing it doesn't just catch threats—it catches them *correctly*.
Throughput	1,200 packets/sec	8,500 packets/sec	Traditional AI struggles under load, causing latency. The distributed, edge-optimized multi-layered AI processes data locally using lightweight models, enabling real-time decisions without bottlenecking the cloud.

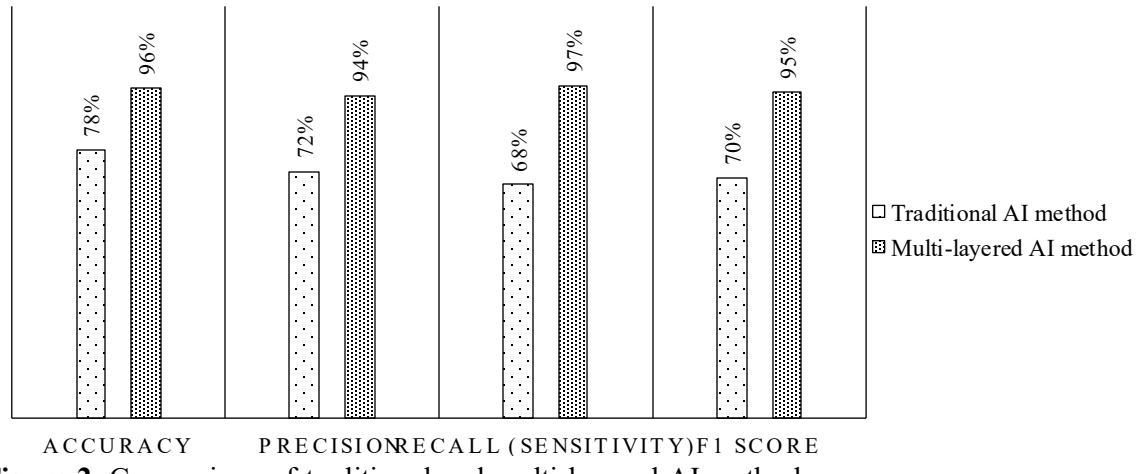

Figure 2. Comparison of traditional and multi-layered AI method.

those employing unsupervised anomaly detection, FL for privacy preservation, and reinforcement learning for autonomous response, offer a dynamic, self-optimizing layer of protection that adapts to the fluid landscape of IoT threats. Unlike conventional security models, which are reactive and often siloed, AI-driven architecture provides holistic visibility and intelligent decision-making across the network. However, the integration of AI into IoT security poses several challenges. Issues such as model interpretability, data privacy, computational overhead on resource-constrained devices, and the potential for adversarial attacks on AI systems require ongoing attention. Future research should prioritize lightweight AI models for edge deployment, robustness against model poisoning, and ethical frameworks for autonomous security decisions.

In conclusion, abstracting security intelligence through AI transforms IoT ecosystems from fragmented, vulnerable networks into resilient and self-healing systems. By embedding cognitive capabilities at every layer of the IoT stack, we move closer to a future in which security is not an afterthought but an intelligent, invisible guardian that constantly learns, adapts, and protects the interconnected world we inhabit.

REFERENCES

1. Liyakat KK, Halli UM. Nanotechnology in IoT security. J Nanosci Nanoeng Appl. 2022;12(3):11–16.
2. Devanand WA, Raghunath RD, Baliram AS, Kazi K. Smart agriculture system using IoT. Int J Innov Res Technol. 2019;5(10):480–483.
3. Hotkar PR, Kulkarni V, Kamble P, Kazi KS. Implementation of low power and area efficient carry select adder. Int J Res Eng Sci Manag. 2019;2(4):183–84.
4. Khatun MA, Chowdhury N, Uddin MN. Malicious nodes detection based on artificial neural network in IoT environments. 2019 22nd International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh. 2019. p. 1–6. DOI: 10.1109/ICCIT48885.2019.9038563.
5. Nikita K, Supriya J. Design of vehicle system using CAN protocol. Int J Res Appl Sci Eng Technol. 2020;8:1978–83.
6. Kundaliya BL, Hadia SK. Routing algorithms for wireless sensor networks: analysed and compared. Wirel Pers Commun. 2020;110(1):85–107. DOI: 10.1007/s11277-019-06713-3.
7. Akansha K. Email security. J Image Process Intell Remote Sens. 2022;2(6):295–320.
8. Sanchez-Reillo R, Gonzalez-Marcos A. Access control system with hand geometry verification and smart cards. IEEE Aerosp Electron Syst Mag. 2000;15(2):45–48. DOI: 10.1109/62.825671.
9. Liu L, Yang J, Meng W. Detecting malicious nodes via gradient descent and support vector machine in Internet of Things. Comput Electr Eng. 2019;77:339–53. DOI: 10.1016/j.compeleceng.2019.06.013.
10. Son M, Kim H. Blockchain-based secure firmware management system in IoT environment. 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South). 2019. p. 142–46. DOI: 10.23919/ICACT.2019.8701959.
11. Jain N, Maitri. Big data and predictive analytics: a facilitator for talent management. In: Munshi UM, Verma N, editors. Data Science Landscape: Towards Research Standards and Protocols. Singapore: Springer; 2018. p. 199–204. DOI: 10.1007/978-981-10-7515-5_14.
12. Lee B, Lee JH. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J Supercomput. 2017;73(3):1152–67. DOI: 10.1007/s11227-016-1870-0.
13. Golder A, Gupta D, Roy S, Al Ahasan MA, Haque MA. GSM based home security alarm system using Arduino using mobile call. 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA. 2023. p. 268–74. DOI: 10.1109/UEMCON59035.2023.10316089.
14. Al-Mashhadi HM, Alabiech MH. A survey of email service: attacks, security methods and protocols. Int J Comput Appl. 2017 Mar;162(11):31–40. DOI: 10.5120/ijca2017913417.
15. Altmann J. Military uses of nanotechnology: perspectives and concerns. Secur Dialogue. 2004;35(1):61–79. DOI: 10.1177/0967010604042536.

