



# Design and Development of an AI-Driven Framework to Secure IoT Networks

Afza Firdous  
[afzareyaz000@gmail.com](mailto:afzareyaz000@gmail.com)  
Integral University, Lucknow, India

Dr. Md. Faizan Farooqui  
[ffarooqui@iul.ac.in](mailto:ffarooqui@iul.ac.in)  
Integral University Lucknow

## ABSTRACT

*The rapid proliferation of Internet of Things (IoT) devices across industrial, domestic, and critical-infrastructure environments has created a correspondingly rapid expansion of cyber-attack surfaces, while the heterogeneity, resource constraints, and high-volume dynamic traffic of IoT networks render conventional signature- and rule-based security mechanisms increasingly inadequate. This article presents a comprehensive review of twelve recent studies (2020–2026) on artificial intelligence (AI)-driven approaches to securing IoT networks, spanning machine learning and deep learning intrusion detection systems (IDS), federated and blockchain-assisted learning frameworks, 5G software-defined network (SDN) security architectures, service-oriented edge-layer architectures, and large-scale systematic and taxonomic reviews. Reported detection accuracies across the empirical studies range from approximately 82% to 98.25%, with federated and hybrid blockchain–AI approaches offering the strongest privacy–accuracy trade-offs and 5G-SDN frameworks achieving the lowest detection latencies (as low as 15 milliseconds). Despite these advances, the literature consistently reports unresolved research gaps, including limited adaptability to evolving traffic patterns, elevated false-positive rates, insufficient attention to the computational and energy constraints of IoT endpoints, dependence on single machine learning or deep learning algorithms rather than integrated pipelines, and an absence of unified, lightweight, and quantum-resistant frameworks validated on real hardware. Building on this synthesis, the review articulates a research problem, four research objectives, and a proposed seven-stage AI-driven security framework — spanning data collection, preprocessing, feature extraction and selection, AI-based threat detection, attack classification, adaptive security response, and continuous monitoring — intended for validation on benchmark datasets (CICIoT2023, TON\_IoT, BoT-IoT/N-BaIoT) and on constrained hardware platforms (Raspberry Pi, ESP32). The proposed research direction aims to deliver a lightweight, adaptive, and empirically validated AI-driven security solution suited to resource-constrained IoT deployments.*

**Keywords:** Internet of Things (IoT), IoT Security, Intrusion Detection System (IDS), Artificial Intelligence, Machine Learning, Deep Learning, Federated Learning, Blockchain-AI Integration, Edge Computing, Anomaly Detection, 5G Software-Defined Networking (SDN), Lightweight Security Framework, and Adaptive Threat Responses.

## 1. INTRODUCTION

The Internet of Things (IoT) now connects billions of heterogeneous devices, sensors, gateways, and edge/cloud services, underpinning applications in healthcare, smart cities, industrial automation, and critical infrastructure. This explosive growth, however, has been accompanied by a parallel expansion of the cyber-attack surface. IoT environments are characterized by large-scale and heterogeneous device populations, limited computational and energy resources at the endpoint, weak or inconsistent authentication mechanisms, insecure communication channels, high-volume and highly dynamic network traffic, and an increasing frequency of IoT-specific cyberattacks such as botnet-driven distributed denial-of-service (DDoS) campaigns. Compounding these challenges is the difficulty of detecting previously unseen (zero-day) attacks using conventional security mechanisms.

Traditional signature- and rule-based intrusion detection systems (IDS), while effective against known attack patterns, are fundamentally reactive: they require continuous manual signature updates and are unable to generalize to novel or evolving threats. Artificial intelligence (AI), encompassing machine learning (ML), deep learning (DL), reinforcement learning (RL), and federated learning (FL), has therefore emerged as the dominant paradigm for building adaptive, data-driven IoT security mechanisms capable of learning normal and anomalous behavior directly from network and device telemetry. This review synthesizes twelve recent

contributions to this field, identifies the research gaps that persist despite substantial progress, and proposes a research problem, objectives, and a candidate AI-driven security framework for resource-constrained IoT networks.

## 2. LITERATURE REVIEW

Table 1 consolidates twelve studies published between 2020 and 2026 on AI-driven IoT security, summarizing each study's publication year, authorship, methodological approach, reported accuracy, principal limitations, and key quantitative results.

**Table -1:** Consolidated Literature Review of AI-Driven IoT Security Studies (2020–2026)

| S. No | Year | Author(s)                                         | Title/Topic                                                                  | Key Findings                                                                                                                       | Algorithms Used                                                                                                                             | Accuracy                                                                            | Limitations                                                                                                                                 | Results                                                                                                                          |
|-------|------|---------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1     | 2020 | HaddadPajouh, Khayami, Dehghantanha, Choo, Parizi | AI4SAFE-IoT: AI-powered secure architecture for IoT edge layer               | 3-layer architecture (application/network/edge) with AI security modules (CTA, WAF, CTH, CTI) mapped to Cyber Kill Chain stages    | Conceptual AI engines; no single ML classifier specified                                                                                    | N/A (uses IoT service management score instead of accuracy)                         | No empirical detection results; comparison is qualitative (feature checklist) vs peer architectures                                         | Scored 84.7/100 on service management metric — highest among IIoTTEED, SeCReT, TEE                                               |
| 2     | 2025 | Akinsiku, Akin-Olayemi, Idris-Tajudeen            | Survey: AI-Driven Security Frameworks for IoT in 5G Edge                     | Taxonomy of IDS/IPS, malware/botnet detection, privacy-preserving AI, access control, blockchain-AI hybrids; FL + edge ML dominant | SVM, RF, CNN, RNN, GNN, Autoencoders, Federated Learning, TabTransformer, LSTM (survey of 20 papers)                                        | ~85–100% across reviewed studies (dataset-dependent)                                | Cross-paper comparison unreliable (different datasets/balancing); no standardized benchmarks; latency rarely measured on real edge hardware | Survey synthesis: identifies gaps in scalability, real-time detection, privacy assurance                                         |
| 3     | 2025 | Krishna Chaitanya Chaganti                        | A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems      | 3-layer framework combining AI-IDS, blockchain, and edge computing; optimization and game theory for resource allocation           | Unspecified ML-based IDS + Adam optimizer, KKT conditions, Lagrangian, Nash equilibrium, Markov chains                                      | 94.2% → 94.78% (post-optimization)                                                  | Single-author, conceptual/numerical study; no real deployment; validated only on ToN-IoT dataset                                            | Response time ↓14.98%, energy consumption ↓12.01%, false positive rate ↓9.99%, attack mitigation ↑0.95% (all p<0.05)             |
| 4     | 2026 | Jawad Yaqoob Mir, Fawad Mir                       | Strengthening U.S. Digital Infrastructure (AICR-SDF)                         | Six-layer conceptual framework integrating AIOps, DevSecOps/SLSA, and policy-governed response for cloud-native resilience         | No ML implementation — theoretical measures only (availability/reliability equations, burn rate, DORA metrics, graph centrality, CVSS/EPSS) | N/A (conceptual, not implemented)                                                   | No prototype or empirical data; standards require organization-specific adaptation                                                          | Four qualitative scenarios demonstrate decision logic; passed ex ante evaluation (consistency, standards alignment, feasibility) |
| 5     | 2024 | Ejeofobiri, Victor-Igun, Okoye                    | AI-Driven Secure Intrusion Detection for IoT Networks (Literature Review)    | Categorizes supervised/unsupervised/RL approaches; discusses transfer learning, XAI, federated learning as future directions       | DNN, SVM, RF, CNN, RNN, GNN, Autoencoders, Federated Learning, Q-learning (reviewed works)                                                  | DNN 92%, SVM 88%, RL 87%, RF/Ensemble 90%, Federated Learning 85%, Autoencoders 82% | High computational/energy cost on constrained devices; protocol heterogeneity; data privacy/regulatory issues                               | No original experiments — review only; recommends lightweight, federated, and hybrid models for future work                      |
| 6     | 2026 | Mohanty, More, Prakhayath, Krishn, Kumar          | SmartSecure: An AI-Driven Network Threat Analysis & Detection Framework      | Real-time IDS combining live packet sniffing, flow aggregation, and RandomForest classification with a web dashboard               | RandomForest                                                                                                                                | Not numerically stated (described as “high accuracy, low false-positive rate”)      | Flow-level smoothing may miss short/stealthy attacks; needs elevated privileges; class imbalance/drift; unreviewed preprint                 | Detects DDoS, brute-force, port scan, botnet, web attacks in real time on consumer-grade hardware                                |
| 7     | 2024 | Thaker, Nay                                       | Enhancing IoT Security with AI-Driven Hybrid ML and Neural Network-Based IDS | Dual-layer hybrid IDS: signature-based detection (Layer 1) + SVM-based anomaly detection (Layer 2)                                 | SVM (hybrid with rule-based/signature detection)                                                                                            | 96.38% (stated as 96.36% in comparison table)                                       | IoT constraints (limited battery, low compute, intermittent node activity) restrict always-on IDS; threshold tuning trade-off               | Outperforms compared works: Sharma 93.05%, Sun 90.76%, Alwahedi 92.79%, Liao 94.89% — highest overall                            |

| S. No | Year | Author(s)                                           | Title/Topic                                                                                                                                                        | Key Findings                                                                                                                                                                                                           | Algorithms Used                                                                                                                                                    | Accuracy                                                                               | Limitations                                                                                                                                                              | Results                                                                                                                                                                                                                     |
|-------|------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8     | 2024 | Kaliappan, Palaniappan, Ananthavadi el, Subramanian | Advancing IoT security: a comprehensive AI-based trust framework for intrusion detection                                                                           | Combines anomaly detection with adaptive trust assessment and RL-based dynamic response for real-time IoT intrusion detection                                                                                          | Isolation Forest, Autoencoder, LSTM, CNN, Bayesian Network, PPO (Reinforcement Learning), Transfer Learning                                                        | 98.25% (N-BaIoT); 97.25% (IoTID20)                                                     | Relies on conventional AI methods; may struggle with advanced/evolving attacks; needs transformer/hybrid optimization in future work                                     | Outperformed CNN-TSODE, culSTMGRU, ELET-IDS, Fed-Inforce-Fusion, Conv-LSTM on accuracy, precision, recall, F1-score and specificity                                                                                         |
| 9     | 2026 | Shameli, Rajkumar                                   | Design of an AI-driven secure 5G-SDN framework with federated reinforcement learning for anomaly detection, mitigation, and attack forensics                       | Multi-layered, causally-aligned security pipeline mapping detection, classification, mitigation and forensics onto SDN data/control/management planes                                                                  | EfficientNet + Knowledge Distillation, Transformer Networks, Spiking Neural Networks (SNN), Federated Reinforcement Learning (PPO/DQN), Blockchain (PoC consensus) | 97.75% average across CICIDS2017, UNSW-NB15, IoT-23, InSDN                             | Evaluated in Mininet simulation, not live 5G deployment; blockchain consensus adds ~120ms latency; assumes largely honest controllers (limited Byzantine tolerance)      | 15 ms detection latency, <5% throughput degradation, 0.25 J energy/detection (40% lower than CNN/LSTM baselines), scales to 20 controllers with 95.1% accuracy                                                              |
| 10    | 2023 | Tarek, Rahman                                       | AI-Driven Cybersecurity, IoT Networking, and Resilience Strategies for Industrial Control Systems: A Systematic Review for U.S. Critical Infrastructure Protection | AI capability strongly predicts ICS resilience; resilience partially mediates AI's effect on perceived protection; IoT maturity enables AI adoption                                                                    | Systematic literature review + survey (210 practitioners) analyzed via Pearson correlation and multiple regression / mediation modeling                            | Not a classifier study — regression $R^2 = 0.57-0.64$ ; $\alpha = .87-.92$ reliability | Cross-sectional, self-reported data limits causal inference; non-probability sampling; no objective incident/performance data; U.S.-sector focus limits generalizability | AICS→ICSR $\beta=0.62$ ; IoT→AICS $\beta=0.60$ ; ICSR & AICS jointly explain 64% of variance in perceived protection; all 5 hypotheses supported                                                                            |
| 11    | 2026 | Ramalingam, Kumar, Gupta, Alsekait, AbdElminaa m    | A hybrid federated learning framework with generative AI for privacy-preserving and sustainable security in IoT-enabled smart environments                         | Hybrid Federated Learning + Generative AI (HFL-GAI) reduces the privacy-accuracy trade-off while lowering energy and communication overhead via hierarchical aggregation                                               | FedAvg / FedProx, GAN & VAE (FedGAN/FedVAE), Differential Privacy, Homomorphic Encryption, Blockchain (Hyperledger Fabric)                                         | 96.8% (vs 98.5% centralized, 95.2% basic FL, 94.1% FL with DP)                         | Degrades under extreme non-IID conditions; DP noise sensitivity affects anomaly detection; resource-constrained devices produce less realistic synthetic data            | 21.2% average energy reduction, 90% sustainability efficiency, 7.5 MB/round communication, 93.8% accuracy at 100 clients, 8–12% attack success rate vs 85–90% for centralized model                                         |
| 12    | 2026 | Kaushik, Gulia, Gill, Yahya, Shukla, Shreyas        | Synergizing blockchain and AI to fortify IoT security: a comprehensive review                                                                                      | Proposes a seven-axis Blockchain–AI Security Integration Schema (BASIS) classifying solutions by security objectives, intelligence modalities, trust primitives, deployment, scalability, privacy and interoperability | Review of ML, DL, Reinforcement Learning, Multi-Agent Systems, Layer-2 consensus protocols, Federated Learning, lightweight DL models                              | Not applicable — narrative/systematic review, no single reported accuracy              | Scalability, computational overhead, and balancing privacy auditability with privacy remain unresolved; lack of standardized interoperability frameworks                 | Case studies (supply chain, healthcare, smart grid) show AI improves detection accuracy/responsiveness while blockchain ensures tamper-proof provenance; recommends hybrid on-chain/off-chain and quantum-safe cryptography |

## 2.1 Synthesis of the Literature

The reviewed literature can be grouped into several complementary strands. First, trust- and behavior-based frameworks (e.g., Kaliappan et al., 2024) combine anomaly detection (Isolation Forest, Autoencoders) with behavioral modeling (LSTM, CNN) and reinforcement-learning-driven response, achieving the highest reported accuracy in this review (98.25% on N-BaIoT). Second, 5G-SDN-oriented frameworks (Shameli & Rajkumar, 2026) integrate lightweight deep learning (EfficientNet with knowledge distillation), transformer-based temporal modeling, spiking neural networks, federated reinforcement learning, and blockchain-based forensic logging to achieve ultra-low detection latency (15 ms) at 97.75% average accuracy. Third, privacy-preserving federated and generative-AI approaches (Ramalingam et al., 2026) demonstrate that hybrid federated learning combined with generative models (GANs/VAEs) and differential privacy can narrow the privacy–accuracy trade-off, sustaining 96.8% accuracy while reducing energy consumption by 21.2%.

Fourth, service-oriented and conceptual architectures (HaddadPajouh et al., 2020; Mir & Mir, 2026) propose layered security models for the IoT edge and cloud-native layers respectively, but largely lack empirical classification accuracy, instead relying on qualitative or service-management scoring. Fifth, broad surveys and taxonomies (Akinsiku et al., 2025; Ejeofobiri et al., 2024; Kaushik et al.,

2026) synthesize dozens of individual studies, consistently highlighting federated learning, lightweight deep learning, and blockchain–AI hybrids as dominant but still-maturing paradigms, while flagging the absence of standardized benchmarks and real-hardware latency measurements as a persistent methodological weakness. Sixth, lightweight and optimization-driven frameworks (Chaganti, 2025) apply Karush–Kuhn–Tucker optimization and game theory to balance detection accuracy against energy and response-time constraints, while real-time prototype systems (Mohanty et al., 2026; Nay, 2024) demonstrate the practical feasibility of RandomForest- and SVM-based detection on commodity or hybrid signature-plus-ML architectures. Finally, an empirical survey-based study (Tarek & Rahman, 2023) provides cross-sectional, practitioner-reported evidence (n = 210) that AI capability and IoT networking maturity jointly predict perceived critical-infrastructure protection effectiveness, lending organizational and behavioral support to the technical findings elsewhere in the literature.

### 3. PROBLEM STATEMENT

Across the reviewed literature, existing IoT security mechanisms exhibit recurring and overlapping limitations, summarized in Table 2.

**Table -2:** Limitations of Existing IoT Security Approaches

| Existing Approach             | Major Limitation                                                |
|-------------------------------|-----------------------------------------------------------------|
| Signature-based IDS           | Cannot effectively detect unknown (zero-day) attacks            |
| Rule-based systems            | Require continuous manual rule updates                          |
| Conventional machine learning | Struggles with evolving, high-dimensional traffic patterns      |
| Deep learning                 | Computationally expensive for resource-constrained environments |
| Standalone detection modules  | Limited response and adaptation capability                      |

### 4. LIMITATION

Existing AI-based IoT security frameworks lack a unified, real-world-validated, lightweight, and quantum-resistant solution that combines intelligent threat detection with adaptive response for resource-constrained IoT devices. Specifically, the following research gaps are identified:

- Limited adaptability to changing IoT traffic patterns.
- High false-positive rates in some existing IDS approaches.
- Insufficient consideration of IoT resource constraints (energy, memory, and processing power).
- Dependence on individual machine learning or deep learning algorithms rather than integrated, hybrid pipelines.
- Limited integration of feature optimization, intelligent classification, and attack response within a single framework.
- Difficulty detecting novel or previously unknown (zero-day) attack patterns.
- Lack of an integrated, end-to-end security framework validated on real IoT hardware.

### 5. RESEARCH OBJECTIVES

1. To critically review existing AI-driven security techniques for IoT networks.
2. To identify key issues and research gaps in securing IoT networks.
3. To develop an AI-driven security framework for IoT networks.
4. To implement the proposed algorithms within the developed framework and validate them empirically.

### 6. PROPOSED METHODOLOGY AND FRAMEWORK

#### 6.1 Methodology and Validation Strategy

The proposed research will be validated using the methodology components summarized in Table 3, combining benchmark dataset evaluation with physical hardware deployment to ensure that reported performance reflects real-world resource-constrained conditions rather than simulation alone.

**Table -3:** Proposed Methodology and Validation Components

| Methodology Component | Details                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------|
| Benchmark datasets    | CICIoT2023, TON_IoT, BoT-IoT / N-BaIoT                                                             |
| AI techniques         | Classical machine learning, deep learning, and lightweight/optimized models                        |
| Hardware validation   | Raspberry Pi, ESP32, and other constrained edge-IoT devices                                        |
| Evaluation metrics    | Accuracy, precision, recall, F1-score, detection latency, memory/CPU usage, and energy consumption |

## 6.2 Proposed AI-Driven IoT Security Framework

Building on the gaps identified in Section 4, the proposed framework follows a sequential, seven-stage pipeline designed to integrate feature optimization, intelligent classification, and adaptive response within a single lightweight architecture suitable for constrained IoT devices:

**IoT Devices / Sensors → Network Data Collection → Data Preprocessing → Feature Extraction & Selection → AI-Based Threat Detection → Attack Classification → Adaptive Security Response → Continuous Monitoring & Validation**

Raw traffic and device telemetry are first collected at the network layer, cleaned and normalized during preprocessing, and reduced to the most discriminative attributes through feature extraction and selection. An AI-based detection stage (combining lightweight machine learning and deep learning models) flags anomalous behavior, which is then categorized by an attack-classification module. Detected threats trigger an adaptive security response, and the entire pipeline is continuously monitored and revalidated to maintain performance under evolving traffic and attack conditions.

## 7. EXPECTED CONTRIBUTION

The proposed research is expected to provide the following contributions:

- A unified AI-driven security framework for IoT networks.
- Intelligent detection of malicious activities across heterogeneous IoT traffic.
- Lightweight AI models suitable for resource-constrained devices.
- Adaptive response mechanisms against detected threats.
- Reduced detection latency and computational overhead.
- Improved security performance through continuous monitoring.
- Empirical validation using benchmark IoT datasets and constrained hardware platforms.

The expected framework flow mirrors the pipeline in Section 6.2, progressing from AI-based detection through lightweight processing, attack classification, adaptive response, continuous monitoring, and ultimately real-world IoT validation.

## 8. CONCLUSION

This review has synthesized twelve recent studies on AI-driven IoT security, spanning trust-based behavioral frameworks, 5G-SDN architectures, federated and generative-AI privacy-preserving systems, blockchain-AI hybrid taxonomies, service-oriented edge architectures, and real-time lightweight prototypes. While reported detection accuracies are consistently high (frequently exceeding 95%), the literature reveals persistent and unresolved challenges: computational overhead on constrained devices, limited adaptability to evolving traffic, elevated false-positive rates, fragmented single-algorithm approaches, and a general absence of unified, real-world-validated, lightweight, and quantum-resistant security solutions. The proposed research aims to bridge this gap by designing and developing an AI-driven, lightweight, and adaptive security framework for IoT networks that integrates AI-based threat detection, attack classification, adaptive response, and continuous monitoring, validated empirically on benchmark datasets and constrained edge hardware such as the Raspberry Pi and ESP32.

## REFERENCES

- [1] HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K.-K. R., & Parizi, R. M. (2020). AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of Things. *Neural Computing and Applications*. <https://doi.org/10.1007/s00521-020-04772-3>
- [2] Akinsiku, A. M., Akin-Olayemi, T. H., & Idris-Tajudeen, R. (2025). AI-driven security frameworks for IoT devices in 5G edge environments: A survey. *Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*, 2(1). <https://doi.org/10.5281/zenodo.16972423>
- [3] Chaganti, K. C. (2025). A scalable, lightweight AI-driven security framework for IoT ecosystems: Optimization and game theory approaches. *IEEE Access*, 13, 72235–72247. <https://doi.org/10.1109/ACCESS.2025.3558623>
- [4] Mir, J. Y., & Mir, F. (2026). Strengthening U.S. digital infrastructure through AI-powered cloud-native software resilience and secure delivery systems. *Journal of Computer Science and Technology Studies*, 8(8), 347–363. <https://doi.org/10.32996/jcsts.2026.8.8.26>
- [5] Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024). AI-driven secure intrusion detection for Internet of Things (IoT) networks. *Asian Journal of Mathematics and Computer Research*, 31(4), 40–55. <https://doi.org/10.56557/ajomcor/2024/v31i48971>
- [6] Mohanty, A., More, A. N., Prakhyath, R. C., Krishn, D., & Kumar, G. V. S. (2026). SmartSecure: An AI-driven network threat analysis & detection framework. *TechRxiv preprint*. <https://doi.org/10.36227/techrxiv.177041322.25563353/v1>
- [7] Nay, T. (2024). Enhancing IoT security with AI-driven hybrid machine learning and neural network-based intrusion detection system. *Babylonian Journal of Artificial Intelligence*, 2024, 158–167. <https://doi.org/10.58496/BJAI/2024/017>
- [8] 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*. <https://doi.org/10.1007/s12083-024-01684-0>
- [9] Shameli, R., & Rajkumar, S. (2026). Design of an AI-driven secure 5G-SDN framework with federated reinforcement learning for anomaly detection, mitigation, and attack forensics. *Frontiers in Artificial Intelligence*, 9, 1701944. <https://doi.org/10.3389/frai.2026.1701944>

- [10] Tarek, J. H., & Rahman, W. (2023). AI-driven cybersecurity, IoT networking, and resilience strategies for industrial control systems: A systematic review for U.S. critical infrastructure protection. *International Journal of Scientific Interdisciplinary Research*, 4(4), 144–176. <https://doi.org/10.63125/mbyhj941>
- [11] Ramalingam, V., Kumar, B., Gupta, S. K., Alsekait, D. M., & AbdElminaam, D. S. (2026). A hybrid federated learning framework with generative AI for privacy-preserving and sustainable security in IoT-enabled smart environments. *Scientific Reports*, 16, 3071. <https://doi.org/10.1038/s41598-025-31769-6>
- [12] Kaushik, D., Gulia, P., Gill, N. S., Yahya, M., Shukla, P. K., & Shreyas, J. (2026). Synergizing blockchain and AI to fortify IoT security: A comprehensive review. *Artificial Intelligence Review*, 59, 41. <https://doi.org/10.1007/s10462-025-11434-0>