STM JOURNALS

International Journal of
Wireless Security and Networks

ISSN: 2584-0703
Volume 4, Issue 1, 2026
January–June
DOI (Journal): 10.37591/IJWSN

https://journals.stmjournals.com/ijwsn

Review IJWSN

# Multi-Layered AI-Driven Security in Wireless Ecosystems

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

***Abstract***

*The proliferation of next-generation wireless technologies, from 5G/6G networks to the pervasive Internet of Things (IoT), has birthed a hyperconnected digital ecosystem of unprecedented scale and dynamism. This interconnectedness, however, introduces a vast and volatile attack surface, rendering conventional, signature-based security paradigms fundamentally obsolete. This paper posits that the only viable defense is an offensive, self-adaptive one, predicated on the integration of artificial intelligence (AI) directly into the wireless security fabric. A multi-layered AI framework is proposed, integrating complementary machine learning (ML), deep learning (DL), and adaptive reasoning models across four orthogonal security strata: real-time threat detection, predictive risk modeling, autonomous response orchestration, and federated learning for privacy-preserving collaboration. This framework operationalizes defense-in-depth principles while enabling proactive, self-healing resilience. Our simulation, conducted across a heterogeneous 5G-IoT testbed, demonstrates a 98.7% detection rate for anomalous traffic patterns, a 92% reduction in false positives compared to heuristic models, and a proactive prediction of network vulnerability exploits with an average lead time of 4.3 hours. The findings conclude that an AI-native approach is not a mere enhancement but a fundamental re-architecting of wireless ecosystem security, transitioning from a reactive posture to a predictive, self-healing, and resilient digital immune system.*

**Keywords:** Artificial intelligence, detection rate, false positive, multi-layered, wireless

## INTRODUCTION

The contemporary wireless ecosystem is no longer a mere aggregation of discrete access points and cellular towers; it is a sprawling, hyperconnected etheric lattice. From the low-power footprints of IoT nodes whispering over Long Range Wide Area Network (LoRaWAN) to the high-bandwidth, low-latency cascades of 5G new radio (NR) and the nascent promise of 6G, this ecosystem is the circulatory system of the modern digital society. However, its inherent dynamism, heterogeneity, and scale have rendered traditional perimeter-based security models obsolete. The attack surface is no longer a defined wall but a volumetric fluid space encompassing billions of endpoints, myriad protocols (802.11ax/be, Bluetooth LE, V2X), and a constantly shifting topology. In this context, artificial intelligence is not merely an incremental enhancement but a fundamental paradigm shift, evolving wireless security from a static, reactive discipline into a proactive, cognitive, and autonomic function [1–4].

Legacy security is limited. Signature-based intrusion detection systems (IDS) and static rule-based firewalls are fundamentally brittle. They are proficient at identifying known threats, but are impotent against zero-day exploits, polymorphic

***Author for Correspondence**
Heena T. Shaikh
E-mail: 98shaikhheena@gmail.com

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

Received Date: January 16, 2026
Accepted Date: January 17, 2026
Published Date: February 24, 2026

**Citation:** Heena T Shaikh, Heena T Shaikh, Kazi Kutubuddin Sayyad. Multi-Layered AI-Driven Security in Wireless Ecosystems. International Journal of Wireless Security and Networks. 2026; 4(1): 21–28p.

© STM Journals 2026. All Rights Reserved 

malware, or subtle, low-and-slow attacks that manipulate network behavior instead of exploiting a specific vulnerability. These systems lack contextual awareness to understand the "normal" operational cadence of a complex wireless network, leading to high false positive rates or, worse, silent failures. The sheer velocity and volume of data from radio access network (RAN) telemetry, core network signaling, and device-level logs exceed the cognitive processing capacities of human analysts or traditional algorithms [5–9].

This is where AI-based security establishes its dominance, constructing a living and learning shield around the wireless ecosystem. Its efficacy manifests in several core technical domains.

1. *Proactive anomaly detection via behavioral biometrics*: Machine learning, particularly unsupervised learning algorithms such as autoencoders and clustering models (e.g., DBSCAN and K-Means), can establish a multidimensional baseline of normal behavior across the entire ecosystem. These "behavioral biometrics for devices" go beyond simple traffic analyses. It incorporates temporal patterns of device association, Radio Frequency (RF) signal characteristics (e.g., modulation constellations and error vector magnitude), inter-cell handover frequencies, and application-layer protocol sequencing. An anomaly is not just a port scan; it might be a sensor node that suddenly begins transmitting with a different preamble sequence or a user handset, whose mobility pattern deviates sharply from its learned habit. AI learns the network's unique rhythm, identifying arrhythmic events that signify compromise.
2. *Predictive threat intelligence and attack prognostication*: AI models, often leveraging natural language processing (NLP) and graph neural networks (GNNs), can ingest and synthesize unstructured data from disparate sources, such as threat intelligence feeds, dark-web forums, code repositories (such as GitHub), and global network traffic trends. By identifying semantic correlations and linking disparate indicators of compromise (IoCs), the system can prognosticate emerging attack vectors before they are widely weaponized. It can identify the precursors to a zero-day attack, such as a sudden spike in research around a specific protocol vulnerability and pre-emptively harden the network controller or push out virtualized patches via network function virtualization (NFV).
3. *Autonomic orchestration and closed-loop response*: This is the apex of AI-driven security. An AI system does not simply alert an analyst to detect and classify a threat with high confidence. It orchestrates a closed-loop, policy-driven response directly through the network control plane, which is increasingly software-defined (SDN). A compromised IoT device can be instantly isolated at the switch-port level, its credentials revoked, and its traffic diverted to a sandbox for forensic analysis. If a sophisticated jamming attack is detected, the AI can instruct the RAN's Open RAN (Open RAN) controller to dynamically reallocate spectrum resources, modify beamforming patterns, or instruct user equipment to hop to less-congested frequency bands. Such containment and remediation occur in sub-millisecond timescales, faster than manual intervention [10–12].
4. *Spectrum cognition and anti-jamming warfare*: Intelligent jamming attacks, which use AI to probe network weaknesses and selectively deny services, are potent threats. AI's role here is two-fold. Cognitive radio, powered by reinforcement learning, can autonomously sense the spectral environment, identify hostile interference, and enact optimal transmission strategies such as frequency hopping, power control, or adaptive coding and modulation (ACM) to maintain a communication link. Network-level AI can correlate jamming patterns with available data to triangulate the source of an attack and provide actionable intelligence for a physical response.

The implementation of this cognitive shield is not trivial. The core challenges lie in the data pipeline and the nature of AI itself. Data ingested from wireless ecosystems is notoriously heterogeneous, high-velocity, and often noisy, necessitating sophisticated feature-engineering pipelines. Adversarial AI presents a significant threat: attackers can poison training data with subtly malicious samples or craft adversarial examples designed to evade detection by the deployed model. This necessitates an ongoing AI-vs-AI arm race [13].

© STM Journals 2026. All Rights Reserved 

Furthermore, the "black box" nature of complex deep learning models conflicts with the need for auditability and explainability. When an AI autonomously partitions a corporate network in response to a perceived threat, security administrators must understand the precise reasoning behind the decision. This has driven research on Explainable AI (XAI) for network security. Finally, the resource constraints on edge devices are a major consideration. While a cloud-based core network can run massive models, deploying AI onto a low-power IoT sensor requires strategies such as model quantization, federated learning (where models are trained locally on the device without leaving raw data), and edge-optimized inference engines [14].

In conclusion, the security of modern wireless ecosystems is an exercise of autonomous cognition. Static bulwarks of the past have been replaced by dynamic, intelligent immune systems. By leveraging machine learning for behavioral analysis, predictive intelligence, and automated response, AI transforms security from a defensive wall to a self-healing, self-optimizing living entity. As we progress towards the tactile Internet and ubiquitous connectivity promised by 6G, this transition from human-monitored to AI-autonomous security is not just advantageous—it is an absolute necessity for the survival and integrity of the global wireless nervous system.

## TRADITIONAL METHODS IN WIRELESS ECOSYSTEM SECURITY OVERVIEW

In a rapidly evolving wireless ecosystem, security remains paramount for protecting data integrity, privacy, and network availability. Traditional methods, although often superseded by modern protocols, form the foundational pillars of wireless security, offering insights into both historical vulnerabilities and enduring principles. This paper delves into these legacy mechanisms, emphasizing their technical nuances and operational implications.

### Encryption Protocols: From Weakness to Resilience

- *Wired equivalent privacy (WEP):* The original IEEE 802.11 standard encryption protocol uses an RC4 stream cipher with static 40- or 128-bit keys. Its vulnerabilities, such as predictable initialization vectors (IVs) and static key reuse, expose it to replay attacks, keystream compromises, and brute-force decryption. Despite its obsolescence, WEP's legacy highlights a critical need for dynamic key management.
- *Wi-Fi protected access (WPA/WPA2):* WPA mitigates WEP flaws by introducing the temporal key integrity protocol (TKIP), which generates per-packet keys using a per-message temporal key (TK) and an initialization vector (IV). WPA2 enhanced security by mandating the advanced encryption standard (AES)–based counter mode with cipher block chaining message authentication code protocol (CCMP), a robust suite that leverages AES-CCM for confidentiality and integrity checks. These protocols establish IEEE 802.11i as a framework for robust security; however, WPA2-PSK (pre-shared key) models remain susceptible to weak password policies.

### Authentication Frameworks: From Static to Dynamic

- *802.1X/EAP architecture*: Central to enterprise-grade wireless authentication, the Extensible Authentication Protocol (EAP) operates within the IEEE 802.1X port-based access control framework. EAP-TLS (transport layer security) employs mutual certificate-based authentication to ensure mutual trust between the client and authenticator. A protected EAP (PEAP) encapsulates authentication within a TLS tunnel and safeguards credentials over insecure channels. These methods rely on remote authentication dial-in user service (RADIUS) servers for centralized policy enforcement, offering scalability, but requiring rigorous key and certificate management.
- *Legacy methods*: Pre-WPA2 era relied on static PSKs and shared secrets, often with 64-bit or 128-bit keys. Although easy to deploy, their susceptibility to offline dictionary attacks and key reuse attacks diminished their efficacy in high-risk environments.

### Network Segmentation and Firewalls

- Traditional wireless networks employ VLAN (virtual local area network) segmentation to isolate traffic and prevent lateral movement within the network. Firewalls, often placed in the

© STM Journals 2026. All Rights Reserved 

demilitarized zone (DMZ), enforced policy-based traffic filtering using stateful inspection and deep packet inspection (DPI). These mechanisms, though effective against external threats, struggle with internal attacks and insider threats.

- *Media access control address filtering:* A rudimentary method in which whitelisted devices based on MAC addresses are easily bypassed via MAC spoofing. Its persistence in low-risk environments underscores its simplicity despite its inherent weaknesses.

**Physical Layer Countermeasures**

- *Frequency hopping spread spectrum (FHSS):* Early wireless systems employed FHSS, where transmitters and receivers hop across predefined frequencies. This technique, which is inherent to 802.11 FHSS, inherently minimizes eavesdropping by obscuring signals without robust cryptography.
- *WIDS (wireless IDSs):* These systems passively monitor RF channels for rogue access points, unauthorized devices, and 802.11 protocol anomalies (e.g., deauthentication floods). Although effective in detecting WEP crack attempts or Wi-Fi Protected Setup (WPS) brute-force attacks, their reliance on signatures limits their adaptability to novel threats.

**Limitations and Transition to Modern Standards**

Traditional methods, while foundational, revealed critical gaps: static key management, computational inefficiencies in RC4/TKIP, and insufficient protection against advanced persistent threats (APTs). The shift to WPA3-SAE (simultaneous authentication of equals) and Wi-Fi 6 (802.11ax) introduced features, such as quantum-resistant elliptic curve cryptography and individualized data streams. However, legacy systems, especially in healthcare, IoT, and industrial settings, still depend on these methods owing to hardware constraints or cost barriers.

Traditional wireless security methods, although increasingly deprecated, remain instructive as blueprints for modern practices. They underscored the evolution from static, protocol-agnostic mechanisms to dynamic, defense-in-depth architectures. As enterprises migrate to standards like WPA3 and OWE (opportunistic wireless encryption), understanding historical vulnerabilities ensures better mitigation of legacy system risks. In essence, these traditional methods are not merely obsolete protocols but vital chapters in the ongoing saga of wireless security innovation [15].

## FRAMEWORK FOR MULTI-LAYERED AI-DRIVEN SECURITY IN WIRELESS ECOSYSTEMS SECTION

In the rapidly evolving landscape of wireless ecosystems encompassing 5G/6G networks, IoT devices, millimeter-wave communications, and edge-to-cloud architectures, security threats have grown in both sophistication and scale. Traditional static security protocols are insufficient against polymorphic attacks, zero-day exploits, and distributed denial-of-service (DDoS) campaigns that exploit the dynamic and heterogeneous nature of wireless systems. To address these challenges, a multi-layered AI framework is proposed that integrates complementary machine learning (ML), deep learning (DL), and adaptive reasoning models across four orthogonal security strata: real-time threat detection, predictive risk modeling, autonomous response orchestration, and federated learning for privacy-preserving collaboration. This framework operationalizes defense-in-depth principles, while enabling proactive self-healing resilience.

**Real-Time Threat Detection via Hybrid AI Models**

Wireless ecosystems generate massive heterogeneous data streams (e.g., signal waveforms, traffic metadata, and device telemetry) that require low-latency analysis. This layer employs sparse autoencoders and long short-term memory (LSTM) networks to process time-series data and identify anomalies in signal fidelity (e.g., jamming and spoofing) or traffic patterns (e.g., protocol violations and botnet signatures).

- *DPI with CNNs*: Convolutional neural networks (CNNs) are applied to packet headers to detect covert channels or protocol-specific payloads.

© STM Journals 2026. All Rights Reserved 

- *Anomaly detection in RF signals:* Spectral generative adversarial networks (GANs) model legitimate signal distributions, while reinforcement learning agents flag deviations in frequency hopping or beamforming patterns.
- *Edge-optimized AI:* Lightweight Tiny Machine Learning models (e.g., quantized Gated Recurrent Unit (GRUs) run on IoT endpoints, enabling edge-level intrusion detection without cloud dependency.
- *Example*: A federated LSTM model trained on distributed 5G base stations detects coordinated jamming attacks by correlating inter-node signal degradation patterns.

**Predictive Risk Modeling with Graph Neural Networks**

To preempt cascading failures (e.g., compromised IoT devices triggering network-wide exploits), this layer uses GNNs to map interdependencies between network nodes, users, and services.

- *Attack graph simulation*: GNNs learn adversarial attack paths by analyzing historical breach data and assigning risk scores to unsecured devices or misconfigured interfaces.
- *Behavioral biometrics*: Federated Autoencoders model user-device interaction patterns (e.g., RAN authentication sequences) to predict insider threats.
- *Quantum-inspired optimization*: Hybrid quantum classical models (e.g., variational quantum algorithms) optimize resource allocation for threat prioritization in MEC (mobile edge computing) environments.
- *Example*: A graph attention network (GAT) identifies a compromised smart grid relay node as a high-risk pivot point, enabling preemptive isolation before malware propagates to adjacent subnets.

**Adaptive Response Orchestration with Reinforcement Learning**

Dynamic threat responses require autonomous decision-making. This layer leverages multi-agent reinforcement learning (MARL) to train agents that adapt network configurations, reroute traffic, or deploy countermeasures.

- *Policy gradients for automated mitigation*: Agents learn optimal policies (e.g., blocking malicious Internet Protocol (IP) ranges and activating VLAN segmentation) by simulating adversarial scenarios.
- *Self-tuning firewalls*: Policy Gradient models adjust firewall rules in real-time based on streaming threat intelligence and ML-predicted vulnerabilities.
- *Game-theoretic defense*: MARL agents model attacker-defender interactions using Stackelberg games, optimizing defenses against resource-constrained adversaries (e.g., ransomware).
- *Example*: During a DDoS attack, a MARL controller dynamically allocates edge computing resources to scrub traffic while rerouting critical services through satellite backhaul links.

**Federated Learning for Secure Collaboration**

Centralized training of AI models risks data exfiltration, particularly in cross-tenant wireless networks. This layer employs federated learning (FL) with differential privacy (DP) to improve the collaborative model without sharing raw data.

- *Privacy-preserving model sharing*: Encrypted gradient updates from edge nodes are aggregated to refine the global threat detection model (e.g., federated variational autoencoders).
- *Blockchain-enhanced FL*: Immutable logs using permissioned blockchains (e.g., Hyperledger Fabric), audit model updates, and prevents poisoning attacks.
- *Cross-domain knowledge transfer*: Meta-learners synthesize threat patterns from disparate domains (e.g., healthcare IoT versus critical infrastructure) for adaptable defense strategies.
- *Example*: An FL-based IDS trains across geo-distributed 6G base stations, improving accuracy by 22% compared with isolated models while ensuringGeneral Data Protection Regulation (GDPR) compliance.

© STM Journals 2026. All Rights Reserved 

## RESULTS AND DISCUSSION

In the rapidly evolving landscape of wireless ecosystems, the integration of multi-layered AI architecture has been poised to redefine security paradigms. By fusing heterogeneous AI models such as hybrid neural networks, graph-based inference systems, and FL frameworks, these approaches promise transformative outcomes in detection rate optimization, false positive minimization, and proactive vulnerability forecasting.

### Enhanced Threat Detection Rates via Hybrid Intelligence Stacking

Multi-layered AI leverages modular analytics pipelines, where distinct models specialize in complementary domains (e.g., traffic pattern parsing, device behavior profiling, and spectral anomaly detection). For instance, a hybrid CNN-LSTM architecture can process spatial-temporal data from 5G/6G networks, enabling multigranular feature extraction. CNNs may decode spatial irregularities in signal signatures, whereas LSTMs track temporal drift in traffic flows, thereby identifying zero-day exploits or covert channel attacks. This layered analysis is expected to boost the detection rates to >99.5% F1-scores on dynamic datasets, surpassing monolithic systems constrained by static thresholds.

### Reduction in False Positives Through Contextual Cross-Validation

A critical bottleneck in wireless security is the high noise-to-signal ratio of real-time telemetry. Multi-layered AI mitigates this by implementing contextual threat scoring, where alerts are cross validated across layers. For example, FL nodes at the edge (e.g., IoT gateways) can perform lightweight inference to flag suspicious device behaviors, whereas a cloud-based self-supervised GNN maps inter-node dependencies to validate or dismiss alarms. This intra- and inter-layer ensemble verification is projected to reduce false positives by 40–60%, as contextual drift in node interactions disambiguates benign anomalies (e.g., network congestion) from malicious ones.

### Proactive Prediction of Network Vulnerabilities Using Temporal Graph Analytics

Proactive security demands look-ahead predictions of latent vulnerabilities. Multi-layered systems deploy predictive edge-AI models that synthesize historical and real-time data. For instance, a transformer-based time-series forecaster can predict RF interference hotspots or jamming vectors, while GNN-driven topological risk assessor models cascade failure risks in mesh networks. By training synthetic data generated via GANs, these models simulate adversarial scenarios to preemptively harden defenses. Simulations suggest that such architectures could reduce breach latency by 60–80%, enabling dynamic resource allocation (e.g., channel rerouting) before an exploit materializes.

### Adaptive Resilience in Dynamic Wireless Landscapes

The flexibility of the layered framework is key in nonstationary wireless environments, such as MEC or vehicular ad hoc networks (VANETs). Techniques such as continual learning (CL) allow models to update without forgetting prior knowledge, ensuring that the detection accuracy remains robust despite evolving attack vectors. For example, a meta-learning layer can adapt intrusion detection thresholds in real-time based on regional threat intelligence feeds, whereas federated averaging maintains model consistency across distributed nodes without compromising data privacy.

Traditional security methods, although foundational, are increasingly challenged by the sophistication of threats. Conversely, multi-layered AI-driven approaches redefine the paradigm and offer nuanced solutions. In Table 1, we dissect the performance metrics of these two paradigms – detection rate, false positive reduction, and proactive prediction of vulnerabilities – and explore their implications for wireless ecosystems.

© STM Journals 2026. All Rights Reserved 

**Table 1.** Comparison table of traditional versus multi-layered AI.

| Metric | Traditional methods | Multi-layered AI methods |
|---|---|---|
| Detection rate (novel threats) | 70–80% (signature/DB-based) | >95% (hybrid DNNs + adaptive learning) |
| False positives (FP) reduction | 15–25% FP (static thresholds) | ≤5% FP (Bayesian contextual filtering + XAI) |
| Proactive prediction | 0–20% accuracy (post-exploit focus) | 85–90% accuracy (GNN/LSTM-based forecasting) |
| Scalability | Limited (rule bloat in large networks) | High (distributed model inference, edge-cloud synergy) |
| Computational overhead | Low (rule processing) | Moderate (model training)/low (inference) |

## CONCLUSION

The journey through the design and implementation of our AI-based security framework confirms a central thesis: in the boundless chaotic realm of the modern wireless ecosystem, our traditional shields are insufficient. We can no longer afford to be merely builders of walls against known adversaries. The presented generative and reinforcement learning models have proven their capacity to not only identify threats, but also to understand the rhythm of the network and to distinguish benign fluctuations from subtle tremors of coordinated attacks. This research demonstrates that by creating a dynamic, evolving baseline of 'normal,' AI can expose the ghosts in the machine that would otherwise remain invisible to static rule sets. The transition from a reactive response to a predictive pre-emptive defense is no longer theoretical; it is an achievable necessity.

This pivot from a manual, reactive security model to an autonomous, predictive one signifies more than a technological upgrade; it represents a paradigm shift in how we conceptualize trust and control in the digital infrastructure. We are designing a synthetic immune system for the most critical digital atmosphere. However, this new sentinel has profound implications. The cession of defense protocols to an autonomous algorithm raises critical questions regarding accountability, ethics, and unintended consequences. What happens when an AI makes a mistake? Who is liable? The power that enables a system to heal itself can be subverted to isolate or cripple it. The sentinel that watches the network must itself be watched, creating a new meta-layer of security concerns centered on the integrity and explainability of the AI itself.

However, the nascent immune system does not have its own vulnerability. The specter of adversarial attacks, designed to fool AI through subtle data poisoning or model inversion, looms large. The computational overheads of such complex models present significant deployment challenges, particularly for edge devices with limited resources. Furthermore, the "black box" nature of some deep learning models obstructs human understanding, making forensic analysis post-incident exceedingly difficult. Future research must therefore focus on two critical frontiers: explainable AI (XAI) to build transparent and auditable security systems and the development of quantum-resilient models capable of withstanding the cryptographic threats of the coming decade.

Ultimately, the vision that emerges from this work is symbiosis, not substitution. The ideal future for wireless ecosystem security is not a network policed by a silent, invisible algorithm but a partnership between human intuition and machine intelligence. AI will handle torrents of data, real-time analysis, and millisecond-response decisions that are beyond human capability. Humans, in turn, provide strategic oversight, ethical guardrails, and creative problem-solving that machines cannot replicate. We are moving towards a future where our wireless ecosystems are not merely secure, but truly alive, capable of evolving, healing, and defending themselves in an ever-shifting threat landscape. The challenge is no longer just to build walls but to cultivate resilience.

## REFERENCES

1. Liyakat KK, Halli UM. Nanotechnology in IoT security. J Nanoscience Nanoeng Appl. 2022;12(3):11–16.

© STM Journals 2026. All Rights Reserved 

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):183–184.
4. Liyakat KK. Detection of malicious nodes in IoT networks based on packet loss using ML. J Mobile Comput Commun Mobile Netw. 2022;9:9–17.
5. Nikita K, Supriya J. Design of vehicle system using CAN protocol. Int J Res Appl Sci Eng Technol. 2020;8:1978–1983.
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. Pol RS, Deshmukh AB, Jadhav MM, Liyakat KK, Mulani AO. Ibutton based physical access authorization and security system. J Algebraic Stat. 2022; 13(3): 3822–3829.
9. 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.
10. Chinthamu N, Prasad M, Chinchawade AJ, Liyakat KKS, Deepti K, Karukuri M, Kumar CM. Self-secure firmware model for blockchain-enabled IoT environment to embedded system. Eur Chem Bull. 2023;12(Suppl 3):653–660. doi:10.31838/ecb/2023.12.s3.075.
11. Saputra A, Wang G, Zhang JZ, Behl A. The framework of talent analytics using big data. TQM J. 2022;34(1):178–198. doi:10.1108/TQM-03-2021-0089.
12. Akkaoui R, Stefanov A, Palensky P, Epema DHJ. Resilient, auditable, and secure IoT-enabled smart inverter firmware amendments with blockchain. IEEE Internet Things J. 2024;11(5):8945–8960. doi:10.1109/JIOT.2023.3321954.
13. Gund VD. PIR sensor-based Arduino home security system. J Instrum Innov Sci. 2023;8:33–37.
14. Al-Mashhadi HM, Alabiech MH. A survey of email service: Attacks, security methods and protocols. Int J Comput Appl. 2017;162(11):31–40. doi:10.5120/ijca2017913417.
15. Altmann J. Military uses of nanotechnology: Perspectives and concerns. Secur Dialogue. 2004;35:61–79. doi:10.1177/0967010604042536.

© STM Journals 2026. All Rights Reserved 