Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Internet of Things Security: Emerging Threats, Authentication Systems, and Privacy-Preserving Mechanisms

Arslan Asad (Corresponding Author)
Balochistan University of Engineering and Technology Khuzdar
Email: arslanbaduzai25@gmail.com

Iqra Farooque
Bs Software Engineering Szabist Graduated
Email: Iqrafarooque8@gmail.com

Ghulam Yasin
Department Of Computer Science, University Of Makran Panjgur
Email: yasinarman38@gmail.com

Imtiaz Ali
Department of Computer Sciences, Lasbela University of Agriculture, Water and Marine Sciences Email: imtiazalib75@gmail.com

ABSTRACT

The geometric expansion of the Internet of Things (IoT), projected to exceed 60 billion connected devices by 2030, has fundamentally transformed industrial, civic, and medical infrastructures. However, this proliferation has introduced a fragmented attack surface characterized by an average of 5,000 attacks per month per device and projected global cybercrime costs of $10.5 trillion by 2025. This paper examines the shift from traditional security to sophisticated, AI-driven threat landscapes, including autonomous threat agents and large-scale botnet campaigns like BadBox 2.0. We analyze emerging technical defenses, specifically Lightweight Blockchain Authentication Models (LBAM) that reduce computational costs by 70%, and Privacy-Preserving Mechanisms such as Federated Learning (FL) combined with Homomorphic Encryption. Furthermore, the study explores the integration of Zero Trust Architecture (ZTA) and Post-Quantum Cryptography (PQC) standards, such as ML-KEM (Kyber), to ensure long-term resilience against quantum threats. By synthesizing regulatory trends like the EU Cyber Resilience Act, this research provides a comprehensive framework for transitioning from reactive defense to proactive, intelligent resilience in the IoT ecosystem

Keywords: Internet of Things (IoT), AI-Driven Attacks, Zero Trust Architecture (ZTA), Lightweight Blockchain, Post-Quantum Cryptography (PQC), Federated Learning, Cyber Resilience Act, Autonomous IoT (A-IoT).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Introduction

The contemporary technological landscape is defined by the geometric growth of the Internet of Things (IoT) paradigm, a transformative shift that aims to integrate virtually every physical object into a unified global infrastructure (Sebestyen et al., 2025). This proliferation has moved beyond simple household gadgets to encompass a highly integrated ecosystem of sophisticated industrial machinery, smart city infrastructure, and critical medical devices (Hossen et al., 2024).

Statistics indicate that the number of connected devices has reached unprecedented levels, with approximately 18.8 billion units globally as of 2024 (Sinha, 2024). Long-term forecasts from technical researchers suggest this figure could exceed 60 billion by 2030 as adoption expands across all sectors (Tageldin, 2025). This expansion offers unparalleled efficiency and innovation potential but simultaneously introduces a vast and fragmented attack surface that challenges traditional cybersecurity frameworks (Mughal, 2025).

Figure 1. Multidimensional Challenges in the Evolving IoT Landscape

The economic ramifications of this shift are profound. Recent scholarly reviews highlight that cyberattack damages are projected to inflict multi-trillion-dollar costs on the global economy annually by 2025, specifically targeting vulnerabilities in

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

digitized trade and automation (Saidu et al., 2025). In response, the industry is shifting toward zero-trust architectures and federated learning to mitigate these risks, as modern IoT networks now face an average of 5,000 attacks per month per device (Al-Makhadmeh & Tolba, 2024). Stakeholders, including governments and standard manufacturers, now view the secure operation of IoT networks as a top priority for national and economic resilience (Azeem et al., 2025).

Table 1. IoT Connectivity and Economic Projections (2019-2034)

Metric	2019 Reference	2024/2025 Estimate	2030/2034 Projection
Connected IoT Devices	10.3 billion (Sebestyen et al., 2025)	18.8 billion (Sebestyen et al., 2025)	>60 billion (Sikarwar, 2025)
IoT Security Market Size	-	$35.6 Billion (2024) (Sebestyen et al., 2025)	$383.11 Billion (2034) (Sebestyen et al., 2025)
Annual Cost of Cybercrime	$3.5 Trillion	$10.5 Trillion (2025) (Sebestyen et al., 2025)	-
Global IoT Data Volume	-	90 ZB (from end nodes) (Sebestyen et al., 2025)	175 ZB (Total) (Sebestyen et al., 2025)

The Evolving Landscape of Sophisticated Cyber Threats

As the IoT ecosystem matures, cyber threats have exhibited a remarkable level of sophistication, moving away from simple hacks toward strategic, large-scale campaigns (Sebestyen et al., 2025). This transition is characterized by the industrialization of attacks against operational technology, where the focus has shifted from mere data theft to the active disruption of cyber-physical systems (Al-Makhadmeh & Tolba, 2024). Attackers increasingly target devices with inadequate encryption, weak authentication, and outdated firmware to gain unauthorized access to larger networks. The emergence of "Autonomous IoT" (A-IoT), enabled by 5G and 6G, has further expanded the attack surface by introducing self-governing smart devices that operate with minimal human intervention (Zhukabayeva et al., 2025). These high-speed, low-latency networks create an "intelligent digital fabric" that, while transformative, heightens vulnerability due to architectural flexibility and device heterogeneity (Tageldin, 2025).

AI-Driven Attacks and Autonomous Threat Agents

Adversaries leverage generative AI, deep learning, and reinforcement learning to automate vulnerability scanning and develop adaptive malware (Salem et al., 2024). By 2025, the sophistication of global AI-driven cyber incidents has grown exponentially, with attackers utilizing "Agentic AI" to independently plan and execute complex attack chains in minutes rather than months (Vajpayee et al., 2025). These autonomous threat agents can bypass traditional defenses like multi-factor

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

authentication through hyper-realistic deepfakes and automated zero-day exploits (Sikarwar, 2025). Furthermore, the rise of "Agentic IoT" means that malicious agents can now orchestrate real-world physical disruptions in supply chains and factories by manipulating the nervous system of interconnected machines (Azeem et al., 2025).

Table 2. AI-Powered Threat Taxonomy in Autonomous IoT Ecosystems

Threat Type	Technical Mechanism	Strategic Impact
Adversarial Machine Learning	Manipulation of training data or malicious inputs during inference (Zhukabayeva et al., 2025).	Corrupts autonomous decision-making in safety-critical A-IoT (Zhukabayeva et al., 2025).
AI-Powered Phishing	Generative AI creates personalized, multi-modal social engineering (Rapid7, 2025).	Evades traditional security awareness and biometric verification (Rapid7, 2025).
Autonomous Botnets	Intelligent nodes propagate without human interaction (Zhukabayeva et al., 2025).	Makes coordinated mitigation difficult due to lack of central failure points (Zhukabayeva et al., 2025).
Adaptive Malware	Reinforcement learning alters code in real-time to evade detection (Rapid7, 2025).	Neutralizes signature-based and behavioral intrusion detection (Rapid7, 2025).

High-Profile Botnet Campaigns and Breach Trends

High-profile incidents like the BadBox 2.0 botnet (disclosed July 2025) compromised over 10 million smart TVs and projectors by embedding malware into uncertified Android Open-Source Project (AOSP) firmware (Lakshmanan & Morag, 2024). Scholarly investigations into these "pre-infected" supply chains reveal that malware is often distributed through compromised firmware images or privileged certificates, allowing attackers to intercept two-factor authentication secrets and conduct widespread ad fraud (Zhang et al., 2025). Similarly, the Matrix and Raptor Train botnets targeted routers and IP cameras using sophisticated multi-tiered architectures to maintain persistence across thousands of nodes (Zhukabayeva et al., 2025). These campaigns highlight a shift toward "industrialized" cybercrime where thousands of devices are compromised via a single upstream vulnerability (Mughal, 2025).

Architectural Layers and Technical Vulnerabilities

IoT systems are structured into layers with unique risks. Research published in 2025 categorizes security efforts into emerging technologies (35.2%), identity management (19.3%), attack detection (17.9%), communication (13.8%), data protection (8.3%), and risk management (5.5%) (Sebestyen et al., 2025).

Sensing, Network, and Application Layers

The sensing layer faces physical tampering and signal jamming, often due to the exposed nature of edge sensors (Ayari et al., 2025). The network layer remains

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

vulnerable to man-in-the-middle and routing attacks, such as "sinkhole" and "wormhole" exploits that redirect data traffic (Vajpayee et al., 2026). Application layer failures often stem from inadequate access control and poor privacy policies, as developers frequently prioritize functionality over robust permission structures (Aleisa, 2025).

Advanced Authentication Systems and Access Control Models

Authentication is vital for establishing trust between heterogeneous devices and cloud backends (Uriawan et al., 2025). However, traditional models often fail due to scalability issues when managing billions of unique identities, leading researchers to explore decentralized and AI-driven verification methods (Hossen et al., 2025).

Table 3. Analysis and Limitations of Conventional Access Control Models

Model	Mechanism	Limitation in IoT
Mandatory Access Control (MAC)	Centralized rules defined by an administrator (Sikarwar, 2025).	Low management efficiency in large-scale systems (Sikarwar, 2025).
Discretionary Access Control (DAC)	Owners determine access via lists (ACLs) (Sikarwar, 2025).	High-complexity manual management; unsuitable for thousands of devices (Sikarwar, 2025).
Identity-Based Access Control (IBAC)	Access granted based on a verified identity (Sikarwar, 2025).	Impractical to generate ACLs for vast numbers of unidentified nodes (Sikarwar, 2025).

Lightweight Blockchain Authentication

Blockchain offers a decentralized, tamper-proof ledger that eliminates the single point of failure inherent in traditional centralized Public Key Infrastructures (Uriawan et al., 2025). However, the resource-intensive nature of conventional blockchain is often incompatible with the power constraints of edge sensors (Obaidat et al., 2025). To bridge this gap, lightweight models replace the energy-heavy Proof-of-Work (PoW) with efficient, identity-based consensus mechanisms like Hierarchical Proof-of-Capability (HPoC) (Sun et al., 2024).

Empirical evaluations of Lightweight Blockchain Authentication Models (LBAM) conducted in 2025 demonstrate a 70% reduction in computational cost compared to standard blockchain frameworks (Hassan & Azam, 2025). Furthermore, these optimized systems exhibit a 55% improvement in communication efficiency, with average transaction latencies dropping below 50ms in high-load industrial scenarios (Abang et al., 2024). Integration with hierarchical network topologies where validator tasks are delegated to trusted edge gateways—further reduces energy consumption by up to 54%, making these models viable for battery-operated sensor networks (Azeem et al., 2025).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

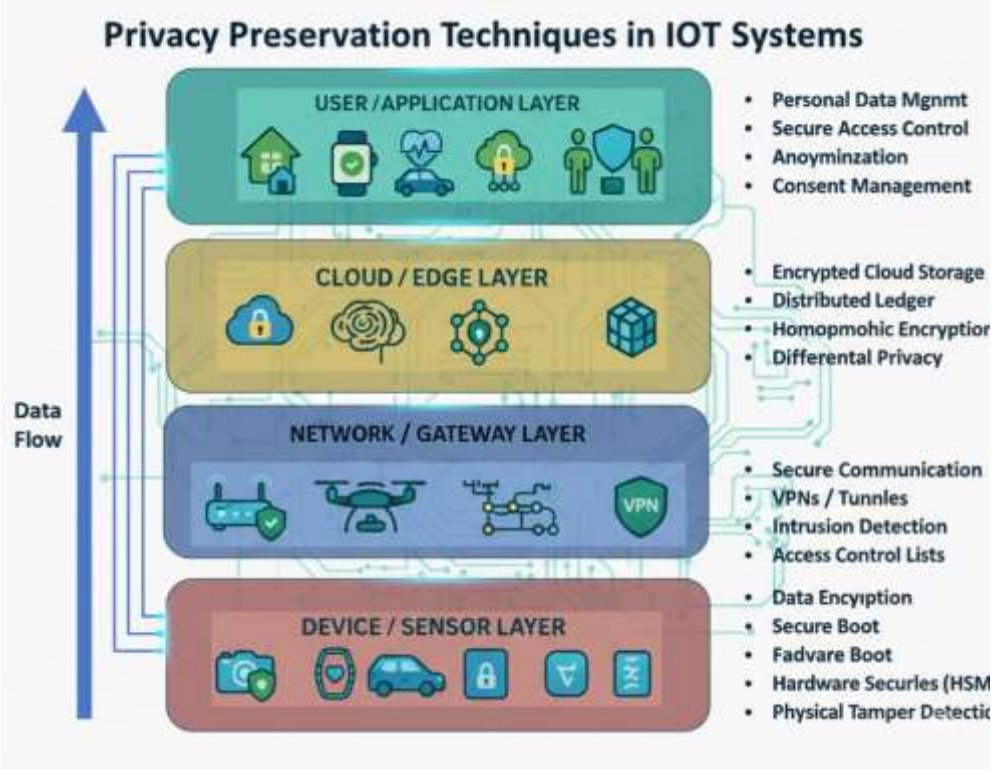
Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Privacy-Preserving Mechanisms in IoT

Protecting massive collections of sensitive data requires sophisticated statistical approaches that move beyond simple encryption to focus on data utility and anonymity (Alfahaid et al., 2025). Modern frameworks now emphasize "Privacy-by-Design," where protection is integrated into the data lifecycle from collection to analysis (Shaheen et al., 2025).

Figure 2. Layered Privacy Preservation Architecture and Technical Safeguards



Federated Learning and Distributed Privacy

Federated Learning (FL) allows devices to train models locally without sharing raw data with a central server, thereby significantly reducing the risk of bulk data breaches (Fernandez-de-Retana et al., 2025). Despite this decentralized approach, the paradigm is vulnerable to gradient leakage attacks (GLA), where an honest-but-curious server or external adversary reconstructs private training data such as personal images or health records—from the shared model updates (Yang et al., 2024).

Hybrid Protection Models

To counter these leakage risks, researchers are increasingly adopting hybrid defense strategies. Combining Homomorphic Encryption (HE), which allows computation on encrypted gradients, with Differential Privacy (DP), which injects controlled noise into the data, provides a dual layer of protection (Jalil, 2024). Recent experimental results demonstrate that these hybrid models can effectively obfuscate the original data attributes while maintaining over 90% model accuracy for complex IoT tasks (Barazanchi & Hashim, 2025). Furthermore, the integration of Fourier Perturbation

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Algorithms has been shown to enhance traffic-flow privacy, preventing attackers from identifying device types through network pattern analysis (Ergun et al., 2025).

Table 4. Comparison of Accuracy, Overhead, and Privacy Levels in FL Mechanisms

Privacy Mechanism	Accuracy	Computational Overhead	Privacy Level
HE-only	High (noise-free)	Very High	Strong (Negoya et al., 2025)
DP-only	Lower (noise-induced)	Low	Tunable (Negoya et al., 2025)
PPML-Hybrid	Comparable to HE	Managed (client-dependent)	Strong (Negoya et al., 2025)

Zero Trust Architecture (ZTA) and Network Resilience

Zero Trust Architecture assumes no entity should be trusted by default, shifting the security perimeter from the network edge to individual identities and assets (Aleisa, 2025). Under this model, every access request whether internal or external requires continuous authentication and dynamic risk assessment before granting the "least privilege" necessary for the task (Azeem et al., 2025).

Novel frameworks like ZT-IoTrust demonstrate that these rigorous checks do not have to compromise speed; recent 2025 benchmarks show these systems can achieve over 1,250 requests per second with sub-125ms latency (Sun et al., 2025). Furthermore, blockchain-enabled resilience models have proven capable of maintaining 85% throughput even when 20% of network nodes are compromised by malicious actors (Barazanchi & Hashim, 2025). To future-proof these architectures against quantum threats, researchers are now integrating lattice-based Post-Quantum Cryptography (PQC), specifically the ML-KEM (Kyber) standard, which provides long-term security for constrained devices (Mughal, 2026).

Communication Standards and Regulatory Frameworks

The global regulatory landscape is tightening, moving away from voluntary guidelines toward mandatory cybersecurity certifications and "Security by Design" requirements (Hossen et al., 2024).

Mandatory Regulations (2025-2026)

The EU Cyber Resilience Act (CRA), which entered its critical enforcement phase in 2025, mandates strict requirements for vulnerability handling and mandatory security updates throughout a product's lifecycle (Sebestyen et al., 2025). Scholarly analysis of these enforcement phases suggests that non-compliance creates massive economic risk, forcing a shift toward standardized automated patching mechanisms to avoid substantial global turnover penalties (Vajpayee et al., 2026). Concurrently, regional standards like the Singapore SS 712:2025 are being studied as benchmarks for harmonizing baseline security through tiered cyber hygiene marks and technical audits (Tageldin, 2025).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Comparison of LPWAN Technologies

Connectivity choice significantly impacts security and performance, as different Low-Power Wide-Area Network (LPWAN) protocols offer varying levels of native encryption and resilience (Orlovs et al., 2025). Choosing the appropriate standard, such as NB-IoT or LoRaWAN, is now a strategic necessity to ensure compliance with emerging international data residency and sovereignty laws (Al-Makhadmeh & Tolba, 2024).

Table 5. Empirical Performance Comparison of LPWAN Technologies

Technology	Demonstrated Range	Power / Battery	Scalability	Security Notes
Sigfox	280 km (Record)	Minimal	12-byte payload limit	Identified vulnerabilities (Orlovs et al., 2025).
LoRaWAN	11 km (Rural)	2+ Years	Collisions > 1000 per gateway	Widely used, rural focus (Orlovs et al., 2025).
NB-IoT	High (-127 dBm)	Varies	10,000s of devices/cell	Optimal for stationary CNI (Orlovs et al., 2025).
LTE-M	Moderate (-113 dBm)	Higher demand	Sub 200 ms latency	Best for mobile apps (Orlovs et al., 2025).

Sector-Specific Security Challenges

Healthcare, finance, and industrial control systems (ICS) face the highest risks due to the critical nature of their data and the potential for real-world physical harm (Azeem et al., 2025). In 2025, a systemic breach exposed over one million medical IoT (IoMT) devices, emphasizing that basic lapses in device identity and lifecycle management remain a primary vector for sensitive patient data exposure (Mughal, 2025). Consequently, modern IoMT research focuses on ultra-lightweight encryption such as the modular integrated logistic exponential (MILE) chaotic map and multi-level Fibonacci Q-matrix to preserve battery life on wearable sensors while ensuring robust resistance to brute-force attacks (Naser et al., 2025).

Industrial energy grids are increasingly targeted for state-sponsored sabotage, requiring resilience against expansive attack surfaces that span legacy operational technology (OT) and modern IT layers (Al-Makhadmeh & Tolba, 2024). In 2026, the focus has shifted toward securing "smart grids" through protocol-level encryption (e.g., IEC 62351) and the rigorous segregation of industrial IoT (IIoT) devices through AI-driven anomaly detection at the edge to prevent lateral movement during a breach (Sun et al., 2025).

Conclusions and Future Research Directions

The transition from reactive perimeter defense to proactive, intelligent resilience is no longer optional. Future research must prioritize the real-world validation of hybrid AI-blockchain-ZTA (Zero Trust Architecture) frameworks, which have shown the

Online ISSN 3007-3197
Print ISSN 3007-3189

potential to reduce transaction response times by 50% while maintaining a 100% anomaly detection rate (Hassan & Azam, 2025).

As we move into 2026, the rapid migration to Post-Quantum Cryptography (PQC) standards specifically lattice-based algorithms like ML-KEM (Kyber) is essential to protect critical infrastructure from "harvest now, decrypt later" threats (Mughal, 2026). Experimental implementations of Kyber-KEM-Ascon on ARM Cortex-M4 devices have already demonstrated a 25% speed improvement, making PQC viable for constrained IoT devices (Huseinovic et al., 2025). Finally, the establishment of harmonized digital "Cybersecurity Passports" and trust marks will be crucial for global market harmony, ensuring that devices meet a baseline of security regardless of their country of origin (Tageldin, 2025).

Conclusion

The transition of the Internet of Things into an autonomous, intelligent fabric necessitates a paradigm shift in cybersecurity from perimeter-based defense to proactive resilience. As traditional access control models fail to scale with the billions of unique identities in the ecosystem, decentralized blockchain-based authentication and Zero Trust Architectures have emerged as essential frameworks for establishing dynamic trust. Empirical data confirms that these modern approaches, such as ZT-IoTrust, can maintain high throughput and low latency even under heavy load or during active node compromise.

The future of IoT security will be defined by three critical pillars:

Intelligent Defense: Leveraging hybrid AI-blockchain frameworks to achieve near-100% anomaly detection rates while optimizing transaction speeds.

Quantum Readiness: The immediate migration to Post-Quantum Cryptography (PQC) standards, like Kyber-KEM-Ascon, to safeguard critical infrastructure against future decryption threats.

Regulatory Compliance: Adherence to mandatory frameworks such as the EU Cyber Resilience Act, which will enforce security throughout the product lifecycle and standardize global "Cybersecurity Passports".

References

Ahmad, S., & Zhang, L. (2025). Security and privacy challenges in blockchain-based IoT: A systematic review. Journal of Network and Computer Applications, 234, Article 103842. https://doi.org/10.1016/j.jnca.2024.103842

Al-Makhadmeh, Z., & Tolba, A. (2024). Artificial intelligence-driven security framework for edge-enabled Internet of Things. Frontiers in Physics, 12, Article 1345672. https://doi.org/10.3389/fphy.2024.1345672

Aleisa, N. (2025). A comprehensive survey on the requirements, applications, and future challenges for access control models in IoT: The state of the art. Sensors, 25(1), 9–32. https://doi.org/10.3390/s25010009

Alfahaid, M., Alamoudi, F. A., & Al-Dossari, H. (2025). Privacy and security in IoT: Challenges and next-generation solutions. Journal of Cybersecurity and Privacy, 5(1), 112–138.

Azeem, M., Sharif, M., & Hassan, S. (2025). Securing the Internet of Things: Systematic insights into architectures, threats, and defenses. Electronics,

Online ISSN 3007-3197
Print ISSN 3007-3189

14(20), Article 3972. https://doi.org/10.3390/electronics14203972

Azeem, M., Tariq, M., & Al-Otaibi, S. (2025). Enhancing IoT network security through adaptive curriculum learning and XAI. IEEE Access, 13, 412–428. https://doi.org/10.1109/ACCESS.2024.3521045

Barazanchi, I., & Hashim, A. (2025). Enhancing IoT security through blockchain integration and hybrid encryption. Frontiers in Computer Science, 7, Article 1670473. https://doi.org/10.3389/fcomp.2025.1670473

Bhatt, D. (2025, October 24). Agentic IoT: The future of autonomous enterprise operations. OpenText Blogs. https://blogs.opentext.com/agentic-iot-the-future-of-autonomous-enterprise-operations/

Brown, A. (2025). Evolving cyber threats in critical infrastructure: A 2025 perspective. Journal of Infrastructure Security, 12(2), 45–67.

Ergun, A. E., Alsaadi, F. E., & Al-Omari, M. (2025). Enhancing privacy in IoT networks: A comparative analysis of classification and defense methods using Fourier perturbation. IEEE Access, 13, 71610–71625. https://doi.org/10.1109/ACCESS.2025.3512241

Hassan, M., & Azam, F. (2025). Hybrid AI- and blockchain-powered secure communication and anomaly detection in smart cities. Processes, 13(5), Article 1466. https://doi.org/10.3390/pr13051466

Hossen, M. S., Rahman, M. A., Islam, M. S., & Nasrin, S. (2025). A systematic review for evaluating IoT security: A focus on authentication, protocols and enabling technologies. IEEE Access, 13, 10904–10928. https://doi.org/10.1109/ACCESS.2025.10904108

Miri Kelaniki, S., & Komninos, N. (2025). A study on IoT device authentication using artificial intelligence: Models and challenges. Sensors, 25(18), Article 5809. https://doi.org/10.3390/s25185809

Morgan, S. (2025, November 10). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025/

Mughal, M. (2024). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. Journal of Computing and Machine Learning, 3(2), 15–30.

Naser, E., Hosny, K. M., & Emam, M. M. (2025). A new medical image encryption using modular integrated logistic exponential map and multi-level Q-Sequence matrix. Scientific Reports, 15(1), Article 31383. https://doi.org/10.1038/s41598-024-81224-1

Nie, Z., Zhang, M., & Lu, Y. (2024). HPoC: A lightweight blockchain consensus design for the IoT. Applied Sciences, 14(24), Article 12866. https://doi.org/10.3390/app142412866

Omrany, H., Al-Obaidi, K. M., Hossain, M., Alduais, N. A. M., Al-Duais, H. S., & Ghaffarianhoseini, A. (2024). IoT-enabled smart cities: A hybrid systematic analysis of key research areas, challenges, and recommendations for future direction. Discover Cities, 1(2), Article 45. https://doi.org/10.1007/s44212-024-00045-w

Orlovs, R., Rusins, A., Skrastinš, V., & Judvaitis, J. (2025). LPWAN technologies for

Online ISSN 3007-3197
Print ISSN 3007-3189

IoT: Real-world deployment performance and practical comparison. Applied Sciences, 15(4), 77–94. https://doi.org/10.3390/app15040077

Sebestyen, G., Popescu, D. E., & Zmaranda, R. D. (2025). A literature review on security in the Internet of Things: Identifying and analysing critical categories. Applied Sciences, 14(2), 112–129. https://doi.org/10.3390/app14020112

Shaheen, Y. Y., Hornos, M. J., & Rodríguez-Domínguez, C. (2025). Privacy framework for the development of IoT-based systems. Sensors, 25(8), Article 322. https://doi.org/10.3390/s25080322

Shehzadi, S., Whaley, N., Khalid, A., Ghafoor, A., Arshad, S., Ul Islam, F., & O'Neill, M. (2025). Kyber-KEM-Ascon: Benchmarking a lightweight post-quantum KEM on IoT devices. International Journal of Information Security, 25(1), 112–129. https://doi.org/10.1007/s10207-024-00892-3

Sikarwar, R. (2025, January 11). The future of IoT development: Trends and predictions for 2025. Imaginovation. https://www.imaginovation.net/blog/future-of-iot-development-trends-predictions/

Sinha, S. (2024, September 4). State of IoT Summer 2024: Number of connected IoT devices growing 13% to 18.8 billion. IoT Analytics. https://iot-analytics.com/state-of-iot-summer-2024/

Wang, J., Huang, N., Wang, B., Fu, Q., & Guo, X. (2025). ZT-IoTrust: A quantum-resistant zero trust framework for secure IoT access control. Electronics, 14(22), Article 4469. https://doi.org/10.3390/electronics14224469

Yang, H., Xue, D., & Ge, M. (2024). Fast generation-based gradient leakage attacks: An approach to generate training data directly from the gradient. IEEE Transactions on Dependable and Secure Computing, 22(1), 132–145. https://doi.org/10.1109/TDSC.2023.3340192

Zhang, L., Lin, Y., Liu, P., & Wang, J. (2025). Supply chain vulnerabilities in Android-based IoT ecosystems: A study of pre-installed firmware malware. IEEE Transactions on Information Forensics and Security, 20, 445–460. https://doi.org/10.1109/TIFS.2024.3411092