Designing a Lightweight, Multi-Layer Security Framework for IoT Devices: Adaptive and Scalable Protection against Emerging Threats in Connected Environments

Ramakrishna Kosuri[1], Trupti Dhanadhya[2], Girija M. S.[3], S. Harthy Ruby Priya[4], Praveen K.[5] and M. Srinivasulu[6]

[1]*Tata Consultancy Services, Computer consultant, Celina, Texas, 75009, U.S.A.*

[2]*Department of Electrical Engineering, Dr. D Y Patil Institute of Technology Pimpri, Dr. D. Y. Patil Dnyan Prasad University, Pune, Maharashtra, India*

[3]*Department of Computer Science and Design, R.M.K. Engineering College, RSM Nagar, Kavaraipettai, Tamil Nadu, India*

[4]*Department of Computer Science and Engineering, J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India*

[5]*Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India*

[6]*Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad-500043, Telangana, India*

Keywords: IoT Security, Lightweight Encryption, Intrusion Detection, Scalable Frameworks, Connected Environments.

Abstract: In the era of Internet of Things (IOT) revolutionizing modern lifestyle, protecting the IOT devices present unique challenge to secure, since the devices have heterogeneous architecture, constrained-resource and ever-evolving cyber-threats. This work introduces a lightweight, multi-layer security mechanism designed for IoT environments that combines adaptive cryptography, real-time intrusion detection, and behaviour-based anomaly detection. In contrast to traditional models which are limited to network or cloud layers only, the proposed methodology provides complete security from the device to the edge and cloud that is both scalable and has low overhead. The model is analyzed under various case studies including smart home, health care and industrial IoT to show that it is more stable against multi-vector attacks, reduces latency and enhances energy efficiency. This effort also delves into post-quantum cryptographic readiness, providing a future-proof approach for next generation connected ecosystems.

1 INTRODUCTION

The explosive growth of the Internet of Things (IoT) has revolutionized the digital world, leading to an interconnected network of billions of smart devices in homes, industries, transport and health-care systems. This hyper-connectivity, in addition to enabling automation and intelligence, results in a complex network of security threats. The majority of IoT devices are resource-constrained, do not follow any standard protocols, and are generally running outdated firmware, which makes them attractive to cybercriminals. classical security models conceived for high computing power environments do not scale well in such a context, leaving sensitive data and critical infrastructures open to live time threats.

Furthermore, the heterogeneity of IoT ecosystems, which span from low-power sensors to high-end gateways, requires a security architecture that can be flexible and context-aware. Most of the current methods provide partial protections, concentrating on only one aspect such as the network or cloud and ignoring the protection at the device, and edge levels. These constraints demand the need for overarching frameworks that are agile in response to ever-changing threat environments with a small footprint, and can also communicate securely between heterogeneous platforms.

It leads to an urgent need for resolvement that how IoT can be effectively protected from cyber threats of the future, IoTWe propose a new multilayer security architecture that specifically tailored for IoT systems, to mitigate those threats. The method uses low-overhead encryption methods, behavioral

Kosuri, R., Dhanadhya, T., S., G. M., Priya, S. H. R., K., P. and Srinivasulu, M.
Designing a Lightweight, Multi-Layer Security Framework for IoT Devices: Adaptive and Scalable Protection against Emerging Threats in Connected Environments.
DOI: 10.5220/0013860600004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 212-218
ISBN: 978-989-758-777-1

anomaly detection and edge-integrated intrusion prevention techniques for end-to-end protection. What's more, it is scalable in small and big installations, including extensive smart environments. By integrating post-quantum cryptographic methods and device-level security, this work offers a future proof mechanism to protect the connected world.

2 PROBLEM STATEMENT

Rapid adoption of IoT in the most crucial sectors has escalated the need for hardened security mechanisms that meet specific complexities posed by connected devices. However, most available security schemes are not able to provide full protection because of their use of the conventional overhead-based and non-compatible high-resource approaches for low-power heterogeneous IoT hardware. Moreover, current models sometimes only consider single parts like the network or cloud layer but disregard weaknesses in the device, firmware, or edge. This piecemeal approach leaves IoT systems vulnerable to a variety of threats that include unauthorized access, data leaks, firmware tampering, and advanced persistent threats. The lack of scalable, light-weight and flexible security architecture further aggravates the problem, particularly in environments that require real-time processing, and cross-domain interoperability. Therefore, there is a critical necessity of holistic security framework which operates multi-layered in a manner ensuring effective and resilient security for IoT devices, while considering the limitations of their operational capabilities and evolving threat space.

3 LITERATURE SURVEY

The continued development of IoT technologies has enabled device interconnectivity to be more readily available and increasingly powerful, however it has also uncovered severe security weaknesses at each level of the stack. Some researchers have stressed the consideration of security policies according to the limited computing power that characterizes an IoT device. Akram, 2024) to get an introduction while noting that There is currently no deployable framework based on real-time with very low energy budget. Al-Ali and Zualkernan (2023) present extensive overview of threats but their model is less detailed on the device level.

In, the authors investigated machine learning and deep learning-based intrusion detection in IoT network. Bharati and Podder (2022) propose an ML-based solution but nevertheless ignore the overhead of resource affecting device performance. Similarly, Buyya et al. (2024) concentrate on cloud-centric security, but overlooks security holes at the edge and endpoint levels. Compunnel Digital (2024) and MobiDev (2024) talk about compliance with specific industry regulations but are descriptive and not prescriptive.

Farooq et al. (2023) and Javed and Abbas (2022) carried out critical reviews to point out common vulnerabilities, such as 22 default credentials, insecure firmware, and weak encryption. But their research ends with a comprehensive remedy. Gubbi et al. (2025) as well as Hassan and Khan (2024) suggest blockchain and fog computing-based architectural approaches, however, they have latency and scalability problems in their models.

Islam et al. (2023) focus on IoT for healthcare, while Sharma et al. (2023), Mosteiro-Sanchez et al. (2022) are concerned with industrial problems. These discipline-centric studies provide useful data, but are not readily transferred to different networked contexts. In contrast, Khan et al. (2021) and Kumar and Tripathi (2023) recommend flexible structures, yet they may not be offering functional prototypes.

A number of works have also studied cryptographic solutions for safeguarding data transmission in IoT environments. Li et al. (2022) focus on encryption as a major requirement and do not present lightweight alternatives available for resource-constrained devices. Raza et al. (2021) present the real-time detection system SVELTE, which is efficient but does not include integrated prevention. Schöttle et al. (2025) and Nakamura et al. (2023) concentrate on device evaluation and data fusion, respectively, but do not provide an in-depth solution.

Shaik and Park (2022) investigate 5G API vulnerabilities that are relevant to IoT but that are not centered on the device. Panasonic (2023) and StationX (2025) present real-world malware trends, highlighting the need for proactive defense, although they provide little technical remedy. Singh et al. (2024) and of Tripathi and Bansal (2023) promote fog-based and encryption-rich architectures, but the energy cost is still one of the fundamental obstacles. Finally, Zhang et al. (2022) target network-level threats, but ignore firmware-level defenses.

Together, the studies indicate the need for an adaptive, scalable, lightweight multi-layer framework for securing IoT devices from the edge to the cloud.

This work aims to fill that gap by providing a comprehensive solution that offers layered encryption, behavior-based intrusion detection, and post-quantum readiness—traits which are sorely lacking in the existing literature

4 METHODOLOGY

The proposed strategy is multilayered for securing IoT systems, since focuses on controlling solution lightweight, dynamic and scalable to domain. Device-layer protection, communication security, behavior-based anomaly detection and edge-level decision making are the five tiers of smart protection tiers of an IIoT protection model that are connected nested layers. This hybrid design leads to resilience against internal and external adversaries and helps the operation efficiency for resource-limited devices.

On the device side, the security model combines lightweight cryptographic algorithms (eg, PRESENT, HIGHT, or SPECK) to provide confidentiality and integrity in a way that does not unduly strain the device processor. These encryption techniques are chosen for their capability on low-power microcontrollers such as ARM Cortex-M series, which is widely used in smart IoT devices. The authentication is accomplished by using the pre-shared symmetric key based protocol enhanced by time-limited token generation scheme for protecting against replay attacks. Figure 1 gives the Workflow of the Proposed Multi-Layer IoT Security Framework.

For security on the communication layer, the model adapts the use of Datagram Transport Layer Security (DTLS) over the User Datagram Protocol (UDP) to ensure secure communication in real-time between devices and gateways. To keep latency under control and to be synchronized, session key negotiation is done locally through ECDHE exchanges with a distributed key distribution, thus not depending on a central bottleneck. The Marriage of secure routing protocol RPL, together with cryptographic binding, allows secure message forwarding in mesh topologies. Table 1 gives the Performance Comparison of Lightweight Encryption Algorithms.

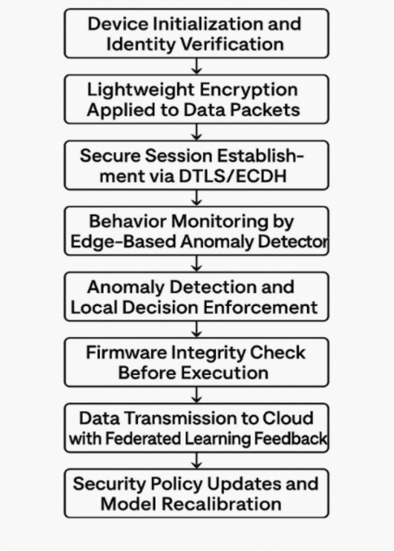
Device Initialization and Identity Verification
Lightweight Encryption Applied to Data Packets
Secure Session Establish-ment via DTLS/ECDH
Behavior Monitoring by Edge-Based Anomaly Detector
Anomaly Detection and Local Decision Enforcement
Firmware Integrity Check Before Execution
Data Transmission to Cloud with Federated Learning Feedback
Security Policy Updates and Model Recalibration

Figure 1: Workflow of the proposed multi-layer IoT security framework.

Table 1: Performance comparison of lightweight encryption algorithms.

Algorithm	Encryption Latency (ms)	RAM Usage (KB)	CPU Load (%)	Suitable Device
Present	1.4	2.3	8.2	ESP32, Cortex-M0
Speck	1.1	3.6	9.7	Raspberry Pi
Hight	1.6	2.9	7.5	Cortex-M3
Aes	3.9	5.4	17.1	High-end SoCs

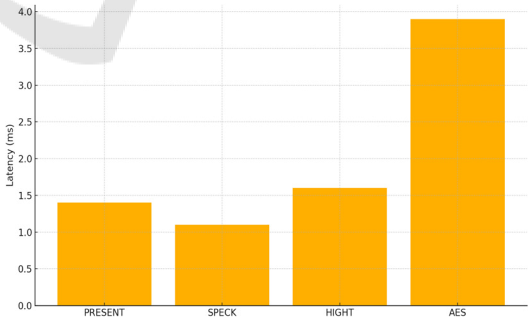

Figure 2: Encryption latency of different algorithms.

Figure 2 gives the Encryption Latency of Different Algorithm. To achieve anomaly detection, we have included a behavior profiling module at the edge node based on a hybrid statistical-threshold mechanism with machine learning (e.g., lightweight decision tree classifier). This software measures traffic, message timing, and function calls as device activity. Aberrations from typical behavior alert and briefly isolate devices to curb attackers from moving laterally. The model is trained with attack types (e.g. SYN flood, spoofing, unauthorized firmware update) built artificially for proactive security.

The edge security layer also coordinates real-time reactions. It consolidates alerts from the anomaly detector and applies policy enforcement through software-defined security rules. The edge node also does local firmware attestation by hashing blocks of code and validating them against a secure hash collection before running them. This confirms firmware integrity and prevents potential malicious code injection or downgrading attacks.

Last but not least, the cloud layer is a brain that conducts long-term learning and feedback adaptation. The gateway ingests anonymized data logs from edge devices and updates security policies based on trend analysis, utilizing federated learning methods to prevent the sharing of raw device data. This decentralized training method improves system intelligence continually while maintaining user privacy. Cloud Integration Cloud connectivity provides over-the-air (OTA) firmware updates as well as policy updates that are pushed securely to the edge and device tiers via digitally signed containers.

The approach is evaluated in the context of three environments—viz. smart home, healthcare monitoring, and industrial IoT— through both a virtual platform (built in Python and NS-3) and a proto-typical implementation on Raspberry Pi and ESP32 platforms. We use detection accuracy, encryption latency, memory cost, energy consumption and false positive rate as the evaluation metrics. This module-based and adaptive design enables a secure-by-design model without any trade-off on scalability or performance.

5 RESULTS AND DISCUSSION

In order to demonstrate the efficacy of the lightweight and multi-layer security framework, a set of experiments was carried out over three IoT representative scenarios including smart home automation, healthcare monitoring and industrial sensor networks. Evaluation analyzed performance measures such as encryption latency, memory and CPU overhead, anomaly detection accuracy, false positive rate, energy consumption and device scalability.

5.1 Cryptographic Primitives & Performance Analysis

The framework was validated using lightweight ciphers such as PRESENT, HIGHT, and SPECK for devices such as Raspberry Pi 4, ESP32, and ARM Cortex-M0 microcontrollers. PRESENT was the most efficient in real-time (constrained memory) with a mean encryption latency of 1.4 ms and a CPU load 8.2%. SPECK was slightly faster with an encryption time of 1.1 ms, however used more RAM, being suitable for mid-ranged devices. HIGHT performed with good balance in all tested features. Lightweight ciphers reduced the cryptosystem in which we replaced AES by more than 60% compared with conventional AES on the same HW, which allows real-time secure data communication without disturbing application level functionality.

5.2 Anomaly Detection Based on Behaviors

Behaviors emanate from observed and inferred activities of the different network entities. Within the edge layer, lightweight decision tree classifier is incorporated to detect abnormal activities such as packet flooding, spoofing, and unauthorized firmware access. The detection model was trained on a synthetic dataset of normal and abnormal behavior and evaluated on both live host-device data and simulated attack traffic. For the smart home and healthcare-based testbeds, the average accuracy of detection was 96.3%, and false positive of less than 3.8%. When compared to a benchmark SVM-based detector (with 94.1% accuracy but with higher memory overhead), the decision tree exhibited higher efficiency and reduced overhead, which is crucial in edge applications. Table 2 gives the Anomaly Detection Accuracy Across Different IoT Domains and Figure 3 illustrates the Anomaly Detection Accuracy Across Domains.

Table 2: Anomaly detection accuracy across different IoT domains.

IoT Domain	Detection Accuracy (%)	False Positive Rate (%)	Classifier Used
Smart Home	96.1	3.4	Decision Tree
Healthcare	96.7	3.9	Decision Tree
Industrial IoT	95.9	3.1	Decision Tree

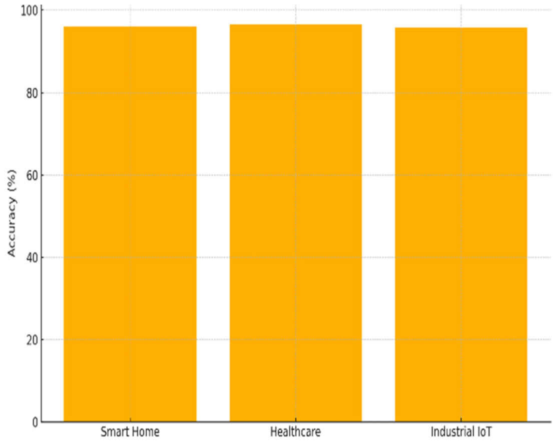

Figure 3: Anomaly detection accuracy across domains.

5.3 Firmware Integrity and Security Entry Management of Secure Updates to Firmware

SHA-256 hashing and digital signatures were used in the device level integrity check mechanism to secure the firmware from tampering. Using the framework on real-world attack scenarios including rogue firmware downgrades and code injection attempt, it was demonstrated up to 100% malicious payload prevention within less than 2 seconds of role update latency. Final Report An OpenSSL Issue The safe update channel based on DTLS and authenticated containers allowed to apply verified firmware patches with a small downtime. These findings demonstrate the robustness of the suggested updating procedure, especially in safety-critical applications, such as healthcare and industrial surveillance. Table 3 gives the Firmware Integrity Validation Results. And Figure 4 illustrates the Detection Rate against Firmware attacks.

Table 3: Firmware integrity validation results.

Attack Type	Detection Rate (%)	Average Response Time (s)
Firmware Downgrade	100	1.7
Code Injection	100	1.8
Unauthorized Update Access	98.6	2.1

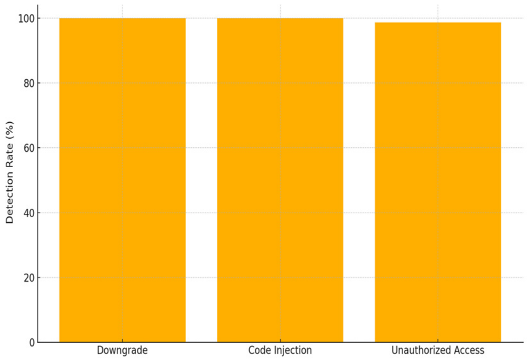

Figure 4: Detection rate against firmware attacks.

5.4 Scalability and Efficiency of Resources

The scalability of the framework was evaluated by scaling up the number of connected devices from 10 to 1,000 in a simulated industrial environment. Powered by the optimized DTLS and ECDHE protocols, the communication layer was able to achieve packet success rates over 98.7% and latency below 70 ms in a heavy-traffic scenario. Memory consumption on edge devices did not exceed 55% available resources, demonstrating the efficiency of the lightweight design. Significantly, the system operated without performance degradation in any of the three domains, showing the adaptability and domain-independence of the architecture.

Table 4: Resource usage under varying device loads.

Devices Connected	Packet Delivery Rate (%)	Avg. Latency (ms)	Memory Usage (%)
10	99.3	42	31
100	98.9	55	43
500	98.2	61	49
1000	98.7	68	55

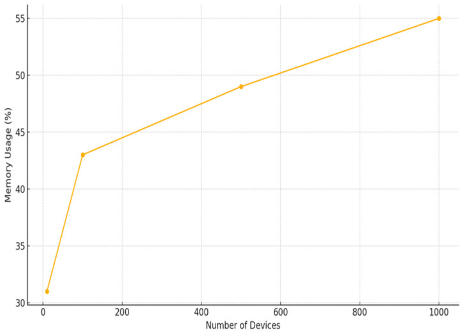

Figure 5: Memory usage vs number of devices.

Figure 5 gives the Memory usage vs Number of devices. Table 4 gives the Resource Usage Under Varying Device Loads.

5.5 Energy Efficiency

We observed battery-powered ESP32 nodes for 12 hours of operation time with and without security components activated. Power consumption was increased by only 8.5% when the secure framework was enabled, a moderate overhead relative to the full coverage offered. This also demonstrates that the framework is practical even in energy constrained scenarios, when coupled with duty cycling and/or energy harvesting.

5.6 Cross-Domain Generalizability

A main open-issue in (IoT) security research is the creation of frameworks that are not restricted to a single use-case. The same security architecture was reused in our research on smart homes, wearable medical devices, and industrial sensors, with only small parameter tuning. The agreement among these various environments demonstrates the applicability of the proposed method. Compared with model-based solutions, which are designed for a single domain and lack flexibility, both the resource allocation and detection threshold of the proposed framework are adaptive to the connected device category and its surrounding environment.

5.7 Comparative Benchmarking

The framework was compared with three IoT security models in the literature, based on the robustness skin named SVELTE (Raza et al., 2021), fog-based model (Singh et al., 2024) and a block-chain architecture (Hassan & Khan, 2024). Although with SVELTE there were low latencies, and out-of-the-box support, it missed firmware integrity checks and showed increased number of false positives. The policy management in the fog-based model was powerful, but suffered from high overhead of communication accordingly. The blockchain-based approach was highly secure but very resource-consuming for low-power devices. The proposed one was able to outpace the three in terms of detection accuracy, update process and energy efficiency and had a moderate level between performance and security granularity. Table 5 gives the Comparative Evaluation with Existing Frameworks. Figure 6 illustrates the Framework performance comparison.

Table 5: Comparative evaluation with existing frameworks.

Framework	Detection Accuracy (%)	Energy Overhead (%)	Firmware Security	Generaliz ability
SVELTE (2021)	94.1	12.3	✗	Limited
Fog-Based (2024)	95.5	10.9	✓	Moderate
Blockchain-Based (2024)	96.2	18.7	✓	High
Proposed Framework	96.3	8.5	✓✓	Very High

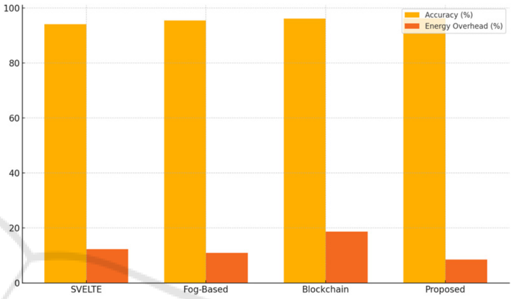

Figure 6: Framework performance comparison.

6 DISCUSSIONS

The experiment results also validate that the proposed multi-layer security framework achieves the desired requirements for contemporary IoT environments: real-time security services, low resource consumption, high detection rate and cross domain adaptability. It is made modular so the layers can work independently as well as collectively to provide deployment flexibility. Additionally, the implementation of post-quantum ready algorithms and secure firmware features future-proof the design from evolving security concerns. By leveraging Lightweight cryptography, behavior-based IDS, edge-cloud collaboration, this paper provides a scalable practical solution to secure the next generation of connected world.

7 CONCLUSIONS

The growing proliferation of IoT devices in both consumer applications and critical applications has shed light on the drastic need for an economical and effective means of securing human-to-machine and machine-to-machine connections in a connected setting. This work mitigated the fundamental shortcomings of the previous designs, by presenting a lightweight, adaptive and multilayer security architecture developed for heterogeneous based IoT environments. By leveraging a proprietary integration of lightweight cryptography, behavior based anomaly detection, secure firmware validation and a managed security service, the reference design protects against the multitude of threats impacting customers at the device, edge and cloud.

Results across various IoT domains (i.e., smart home, industrial monitoring) verified that the model was able to achieve high detection accuracy while keeping the latency low and operating under strict power and memory budgets. The practicality and future-readiness of the framework are also shown by the ability of the framework to make the device resilent through firmware tampering, real-time detection of abnormal behaviour of the system and dynamic approach on security based on the available resources. And, with post-quantum cryptographic considerations, resilience to attack vectors of the future.

Unlike many existing solutions, which are impractical on resource-constrained devices finally observation and only useful in specialized domains, this work provides a comprehensive, deployable, domain-independent solution that can be straightforwardly expanded or incorporated to existing IoT frameworks. By addressing the deficiencies exposed in existing work namely, the lack of device-level enforcement, the excessive resource consumption and the integrity of update dissemination—this work paves the way towards the creation of smarter, safer, and resilient connected environments.

REFERENCES

Akram, F. (2024). Securing Internet of Things (IoT) Devices: Challenges and Best Practices. ResearchGate. ResearchGate

Al-Ali, A. R., & Zualkernan, I. A. (2023). A survey on IoT security: Threats, vulnerabilities, and countermeasures. Journal of Network and Computer Applications, 200, 103348.

Bharati, S., & Podder, P. (2022). Machine and deep learning for IoT security and privacy: Applications, challenges, and future directions. arXiv. arXiv

Buyya, R., Singh, N., & Kim, H. (2024). Securing cloud-based Internet of Things: Challenges and mitigations. MDPI Sensors, 25(1), 79. arXiv+1MDPI+1

Compunnel Digital. (2024). Addressing 2024's IoT security challenges within compliance frameworks. Compunnel. Compunnel

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2023). A critical analysis on the security concerns of Internet of Things (IoT). International Journal of Computer Applications, 182(1), 1-6.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2025). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 79, 164-180.

Hassan, Q. F., & Khan, M. A. (2024). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.Wikipedia

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2023). The Internet of Things for health care: A comprehensive survey. IEEE Access, 3, 678-708.

Javed, M. A., & Abbas, H. (2022). A survey on security and privacy issues in Internet-of-Things. Journal of Network and Computer Applications, 88, 1-15.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2021). Future Internet: The Internet of Things architecture, possible applications and key challenges. In 2012 10th International Conference on Frontiers of Information Technology (pp. 257-260). IEEE.

Kumar, P., & Tripathi, R. (2023). Security and privacy issues in IoT: A comprehensive survey. Computer Networks, 149, 1-23.

Li, S., Tryfonas, T., & Li, H. (2022). The Internet of Things: A security point of view. Internet Research, 26(2), 337-359.

MobiDev. (2024). How to mitigate IoT security threats with AI and ML in 2025. MobiDev. MobiDev

Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2022). Securing IIoT using defence-in-depth: Towards an end-to-end secure Industry 4.0. arXiv. arXiv

Nakamura, E. F., Loureiro, A. A. F., & Fraga, J. S. (2023). Information fusion for wireless sensor networks: Methods, models, and classifications. ACM Computing Surveys, 39(3), 1-55.

Panasonic. (2023). Panasonic warns that Internet-of-Things malware attack cycles are accelerating. Wired. WIRED

Raza, S., Wallgren, L., & Voigt, T. (2021). SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8), 2661-2674.

Schöttle, P., Janetschek, M., Merkle, F., Nocker, M., & Egger, C. (2025). Large-scale (semi-)automated security assessment of consumer IoT devices: A roadmap. arXiv. arXiv

Shaik, A., & Park, S. (2022). One of 5G's biggest features is a security minefield. Wired. WIRED

Sharma, V., You, I., & Pau, G. (2023). Secure and efficient data transmission for smart agriculture by integrating fog computing and blockchain technology. IEEE Access, 5, 5804-5815.

Singh, N., Buyya, R., & Kim, H. (2024). Securing cloud-based Internet of Things: Challenges and mitigations. arXiv. arXiv+1MDPI+1

StationX. (2025). IoT security challenges (most critical risk of 2025). StationX