Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Security and Privacy Challenges in Large-Scale Internet of Things (IoT) Ecosystems: A Framework for Secure Communication, Data Protection, and Resilient Device Management

Syed Shahrooz Shamim*

Department of Computer Science, Iqra University. Corresponding Author Email: Email: shahrooz.shamim@iqra.edu.pk

Rashid Rasheed

Department of Computer Science, University of Management and Technology. Email: rashid.rasheed@umt.edu.pk

Kanza Gulzar

Institute of Information Technology, PMAS Arid Agriculture University Rawalpindi. Email: kanza@uaar.edu.pk

ABSTRACT

Introduction Due to the heterogeneity of devices, inadequate computation power, poor authentication, absence of a secure communication channel, and an increasing vulnerability to cyberattacks, large-scale Internet of Things (IoT) ecosystems are ever more susceptible to serious security and privacy concerns. These concerns challenge the confidentiality, integrity, availability, and privacy of users in interconnected settings. Aim The present paper was intended to create and test a holistic framework of safe interaction, data security, and resilient device management in large IoT systems. Methodology A design science research approach with simulation-based experimental environment based on virtual IoT devices, a gateway, and cloud nodes was employed in the study. The offered framework incorporated the lightweight encryption and secure key exchange, privacy-protecting schemes, device authentication, access control, and anomaly detection. It was tested against an unsecured network baseline in varying attack conditions and network sizes. Results indicated that the suggested framework brought a lot of enhancement to the overall security performance. The number of data breach

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

incidents decreased by 82.8%, the accuracy of data integrity was 97.7%, the success rate of authentication was more than 96%, and the intrusion detection rate was 92.4% on average. Even though the communication latency, authentication delay, and the consumption of resources had risen by moderate rates, system availability, the ratio between packets delivered, and the recovery time had also improved significantly. Conclusion The research finds that a comprehensive security-by-design system can significantly enhance the security and resilience of massive IoT systems and ecosystems without causing intolerable operational costs.

Keywords: Internet of Things, IoT security, privacy protection, secure communication, device authentication, intrusion detection, resilient device management, large-scale ecosystems

1. Introduction

The fast development of the Internet of Things (IoT) has disrupted the technological environment by facilitating a smooth connection of billions of devices incorporated with sensors, software, and communication systems. These devices include basic home devices or complex industrial systems, and together they form large-scale IoT edifice environments to believe in clever cities, healthcare, transportation, and industrial control. With more and more focus being made on the IoT adoption, it is estimated that tens of billions of devices will become interconnected around the world, producing large volumes of data and allowing real-time decision-making across a broad spectrum of areas (Ashton, 2009; Statista, 2023). Although such an unparalleled level of connection is immensely economically and socially useful, it also sets the complicated security and privacy issues that require immediate scholarly and practical responses.

Heterogeneity, scalability and distributed architecture are the defining characteristics of large-scale IoT ecosystems. Tools on these ecosystems have various hardware parameters, protocols, and software platforms, thus making it hard to come up with standard security parameters. In addition, most IoT gadgets are resource-constrained, and they tend to have limited processing power, memory, and energy capacity, making it impossible to apply traditional security tools, including strong encryption and real-time surveillance (Sicari et al., 2015). Consequently, the gadgets end up being a weak point of cyberattacks further affecting the integrity and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

reliability of the entire ecosystem.

The amplified threat surface due to the sheer proportions of interconnected devices is one of the most important security issues in IoT ecosystems. All the devices are the possible weaknesses that can be exploited by the attackers to achieve unauthorized access, send distributed denial-of-service (DDoS) attacks, or manipulate the data streams. The notorious Mirai botnet attack showed how IoT devices that fall into bad hands can be used to cause havoc to internet services the world over, and this is the worst thing of having poorly secured IoT devices (Kolias et al., 2017). In addition, poor authentication systems, default passwords, and the absence of consistent updates to firmware inflammation of these vulnerabilities and IoT ecosystems become extremely vulnerable to cyber threats.

Besides the threat of security, privacy issues are also one of the major threats in massive IoT settings. It is true that IoT devices gather, process, and transfer sensitive information, such as any personal, behavioral, or location-based data on a continuous basis. This massive data gathering has been of great concern in terms of unauthorized access, misusing of data and surveillance. The limited awareness and control that users possess over their data activities puts the risk of privacy rights violation (Ziegeldorf et al., 2014). Additionally, the combination of information provided by several sources may identify complex trends regarding people, which are even more dangerous to privacy and ethical issues.

The other significant obstacle here is to make communication among the IoT networks secure. The information that is passed on between the gadgets and centralized systems is usually vulnerable to interception, tampering and replay attacks. Conventional security mechanisms do not necessarily fit into the IoT setup since they impose a high processing load which requires the creation of light-weight but effective communication systems (Raza et al., 2013). There is also the problem of a lack of standardized protocols of communication, where devices and platforms might not necessarily have consistent security safeguards, which results in difficulty in interoperability and security breaches.

The management of devices is also very important to ensure that the IoT ecosystems are also protective and robust. The thousands of devices that have to be administered means there has to be efficient systems of identity management, access

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

control and updating of their firmware. Still, most IoT deployments do not have centralized control systems or automated software update, not providing the software that is updated and the vulnerabilities fixed (Roman et al., 2013). Also, the physical accessibility of numerous IoT devices complicates it even more, as they may be tampered with and unauthorisedly modified, which further diminishes the security of the systems.

New technologies like artificial intelligence (AI), blockchain and edge computing have been suggested as some possible solutions in solving these problems. Real-time analysis of anomalies can be improved with the help of AI-based systems, blockchain technology can provide decentralized trust services and guarantee identity verification (Dorri et al., 2017). On the same note, the edge computing allows the local data processing, which lowers the latency and limits the potential exposure to centralized attacks. Though these improvements have been made, implementing these technologies into big package IoT has been a complicated undertaking considering issues with scalability, affordability, and compatibility.

With such complex issues, the necessity to use a holistic framework that has security and privacy concerns is urgent. However, the current solutions tend to choose a specific aspect (encryption, authentication, etc.) without paying attention to the interdependence of the IoT ecosystems. These must be integrated into a single framework using secure communication protocols, effective data protection system, and effective device management approaches to provide end-to-end security. This framework should also be responsive to the dynamic and changing aspects of the IoT environment to add new devices, technologies, and threat vectors.

The university paper will attempt to add to the current knowledge base by giving an extensive explanation of security and privacy issues within huge IoT systems and create a systematic framework to handle such matters. Through the combination of various levels of security and the exploitation of modern technologies, the offered framework aims at improving the resilience and reliability of the radio IoT systems in general. Finally, to maintain user trust and allow the ongoing development of the said groundbreaking technology, secure and privacy-protecting IoT ecosystems are a must.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

2. Literature Review

2.1 Theoretical Framework

The perspective on security and privacy in large-scale IoT environments is increasingly viewed through the lens of layered and socio-technical approaches that relate device limits, network openness, data sovereignty, and operational resiliency. Recent literature demonstrates that there is no single control that can guarantee IoT on a large scale since threats are introduced at the same time at perception, communication, platform, and application layers. According to Ogonji et al. (2020) and HaddadPajouh et al. (2021), the theoretical underpinning of IoT security has ceased to be the hardening of individual devices towards the broader spectrum of ensuring assurance in ubiquitous ways: authentication, confidentiality, integrity, availability, and privacy need to be established across heterogeneous nodes. This stratified knowledge is particularly significant in large deployments since weak nodes, unsafe protocols and broken models of trust may interact to create cascading failures instead of single cases and broader systemic failure.

The second strand of theory in recent literature has been the shift in thinking towards perimeter defense to zero-trust and decentralized trust. According to Guguroth et al. (2023), blockchain-based decentralization is a desirable trait since large IoTs typically have no single, entirely trusted authority, particularly in cross-organizational contexts, including smart cities, healthcare, and supply chains across industries. A similar direction is to philosophically present access control as an auditable and dynamic process instead of a table of permissions, as demonstrated by Hu et al. (2023), where the interaction between devices, gateways, and users is dynamic. This theoretical standpoint promptly endorses the current research, since it views security as the process of continuous negotiations between entities (as opposed to the one-time issue of a login problem).

The recent privacy theory in IoT equally goes beyond secrecy to control, minimization as well as purpose limitation and compliance savvy processing. Kaur et al. (2025) and Elluri et al. (2026) declare that the understanding of privacy in IoT is no longer seen merely in terms of avoiding unauthorized disclosure. It also involves restriction of unnecessary gathering, minimization of linkability and rendering the information streams understandable to the users and regulators. The broader

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

perspective can apply to big-scale ecosystems since persistent behavioral data is commonly produced by a device and loss of privacy can be experienced even when the data are encrypted provided that aggregation, inference and re-use are not regulated. Consequently, this theoretical framework of this paper integrates the concepts of layered security, zero-trust communication, and privacy-by-design as mutually reinforcing concepts.

2.2 Empirical Studies

In empirical research published since 2019, it is always observed that the area of secure communication has remained a key issue in the IoT ecosystem. Laghari et al. (2024), Dritsas and Trigka (2025), and Mishra and Mishra (2025) state that a vulnerable protocol, heterogeneity between devices, and resistance to replay, spoofing, and denial-of-service attacks are still factors that impact the practice of secure data exchange negatively. Their results underpin the thesis that the security of communication in IoT cannot be based on the traditional heavy protocols and that scalable and lightweight protocols are needed to maintain efficiency and confidentiality in a limited environment.

Visaose-vista A major literature exists regarding the topic of lightweight authentication of resilient device management. Tanveer et al. (2024) suggest a lightweight authentication protocol which is based on biometrics in smart healthcare systems and demonstrate the role of establishing session keys and exchanging authentication in securing medical devices. Wu et al. (2023) also prove that with flaws in the current IoHT authentication systems, medical information and privacy of users can be revealed, which justifies the refinement of the protocols. Recent researchers further affirm the importance of the lighter, less-heavyweight authentication such as those of Alharthi and Altuwaijri (2025), Khalique et al. (2025), and Merchant et al. (2025) since they suggest that it is one of the most feasible technical methods of large, IoT ecosystems in which computational capabilities and battery sizes are constrained.

The other empirical direction is on privacy-preserving analytics and intrusion detection. Mosaiyebzadeh et al. (2024) demonstrate that in Internet of Health Things environments, federated learning is capable of enhancing privacy through the maintenance of sensitive information locally and the use of collaborative

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

detection at the same time. Similar results are given by Mahmud et al. (2024), who introduce federated intrusion detection in the context of a cyber-physical environment and IoT and state that it is possible to work towards protecting privacy and guaranteeing the accuracy of the model, as opposed to considering these two concepts as contradictory goals. The following inquiry is further developed by Puviarasu and Sudha(2026) who introduces a privacy-restraining version of federated federated model of real-time intrusion detection among devices, demonstrating the increasing amount of empirical research evidence on distributed intelligence in large-scale IoT defense.

The literature on blockchain and access control presents similar pieces of evidence of decentralized resilience in parallel. Guguroth et al. (2023) summarize the studies that note that blockchain may enhance access control and identity assurance, and data integrity, yet cost and scale is of particular concern. Hu et al. (2023) prove the existence of the empirical blockchain-based access control system allowing the lightweight management of data with the trusted audit and the non-repudiation. Generally, these papers suggest that a robust device operation relying on a secure system is aided by verifiable authorization and nonmalicious logging of distributed services.

These results are strengthened by more generic domain reviews. Summarizing privacy and security concerns at various levels of IoT, Sun et al. (2025) discuss defects in firmware and access control restrictions, as well as blockchain-based solutions. In the smart-grid cyber-physical context, Hasan et al. (2026) demonstrate that data security should be contemplated at all levels of the multifunctional IoT at the same time. In telehealth studies, Nezdami et al. (2026) report that the majority of current studies continue to focus on encryption and authentication and devote less focus on more recent forms of attacks, including ransomware and SQL injection. These syntheses of the empirical evidence are indicative that the evidence base is expanding, but it is still sector and solution-type fragmentary.

2.3 Research Gap

Even though recent studies made significant progress, there are still three critical gaps. To begin with, most of the literature assesses security, privacy, communication

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

protocols, authentication or analytics individually whereas large-scale IoT systems demand end-to-end connected models that tie together these aspects. Second, most of the suggested solutions are verified in limited opportunities: healthcare, telehealth, or smart manufacturing, which does not allow one to generalize them to heterogeneous, multi-vendor ecosystems. Third, the current literature usually focuses on prevention or detection, whereas resilient device management needs lifecycle features, including orderly onboarding, update governance, auditability, recovery, adaptive trust reconstructing. Thus, a coherent framework, uniting the concepts of secure communication, data protection, and robust device management, is still missing in the literature, which is scaled, privacy-conscious, and realistic in the context of large IoT ecosystems.

3. Methodology

3.1 Research Design

This paper focuses on building and testing a holistic model of securing large-scale internet of things (IoT) environments using a design science research (DSR) approach. The design science is chosen due to the purpose of not merely analysing the current problems; however, it is necessary to develop a functional and innovative solution to face the security and privacy dilemmas in the real-life IoT condition. The study aims at developing an artifact of a multi layer structure containing secure communication, data protection and resilient management of devices. The proposed research is conducted in an iterative manner where identities of the problems are recognized, frameworks are developed and properly evaluated to ascertain that they are both theoretically rigorous and practically relevant.

3.2 System Modeling and Framework Development

The framework that is proposed is developed upon a layered model of an IoT architecture, which includes perception, network, and application layers. The individual layers are analyzed with an aim of coming up with a security requirement and vulnerability. The framework incorporates three fundamental elements: secure communication protocols, tools of data protection, and device management approach. The lightweight encryption and key exchange schemes are used to model secure communication and can be used on resource-constrained devices. The mechanisms to ensure data protection are created to enable encryptions at rest and transit, data

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

minimization, and anonymization, which are privacy-aware techniques. The management of devices is designed based on identity provisioning, authentication, secure firmware updates, and anomaly detection. The framework architecture guarantees scalability and interoperability to the supporting heterogeneous IoT environments.

3.3 Experimental Setup

In order to test the offered framework, an experimental setting in the form of a simulation is developed with the help of IoT network modeling tools. To simulate a large-scale environment, the environment is represented by several virtual Internet of Things devices, gateways, and cloud nodes. To evaluate the effectiveness of the framework, different scenarios of attacks, such as denial-of-service, un-authorized access, and data interception are simulated. Measures of performance including latency, computation load, detection rate, and data accuracy are analyzed. Cryptographic models and anomaly detection models (lightweight) are tested to use them to assess their effectiveness in challenged conditions.

3.4 Data Collection and Analysis

The variables are gathered within the simulated IoT environment as network traffic logs, authentication logs and system performance logs. Quantitative analysis will be done in order to estimate the improvement of security performance in relation to the baseline security configurations where the proposed framework will not be applied. Detection rates, false positives and efficiency of the system are assessed statistically. The analysis is aimed at determining the effectiveness of the framework in eliminating the threat to security and at the same time ensuring that the system performs reasonably.

3.5 Validation and Reliability

The credibility of the framework is achieved with the help of repeated classifications of simulation under different network sizes and attack intensities. The sensitivity analysis is carried out in order to test the strength of the framework in varied conditions. The validity of the results is attained by comparing the system performance prior to and post implementation so that the proposed strategy can yield consistent results in terms of enhanced security, privacy, and resilience when applied in large-scale IoT deployments.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

4. Results

4.1 Overview of Experimental Results

This part will provide the simulation-based comparison of the proposed IoT security framework with an unsecured system used as the baseline. The analysis is based on the security of communication, data, authentication, intrusion detection, scalability, and effectiveness of the framework as a whole. In nearly all the areas of performance, the proposed framework had shown significant security benefits, though with relatively small computational and timing costs. The results show that the framework promoted confidentiality, integrity, authentication reliability, ability to detect an attack, and system resilience without jeopardizing the performance of a large-scale IoT setting.

The general trend of outcomes indicates that the proposed framework was victorious over the baseline in security-sensitive aspects. Simultaneously, the framework implied a minor increase of the communication response time, authentication time and resource usage caused by the inclusion of encryption process, key exchange mechanism, access control and anomaly detector. This tradeoff is anticipated in the security engineering and is permissible when the net gain in some form of protection is significant. As it is shown in Tables 4.1 through 4.11 and Figures 4.1 through 4.12, the framework provides a balanced solution where the security can be increased without critical performance degradation.

4.2 Performance of Secure Communication Mechanism

Table 4.1 and Table 4. 2 as well as Figure 4.1 and Figure 4.2 show the performance of secure communication mechanisms. As the number of connected devices increased between 50 and 1000, it is clear in Table 4.1 that the latency of communication experienced a slow rate. Latency in the baseline had gone up to 42.6 ms and in the proposed framework it had gone up to 101.7 ms and 116.8 ms respectively. This increase is graphically confirmed in figure 4.1 and indicates that the adoption of the suggested framework always needed slightly longer time since the operations of encryption and safe routing were processed. Nevertheless, the growth was both manageable and predictable, implying that the framework can be extended with more significant loads on the devices.

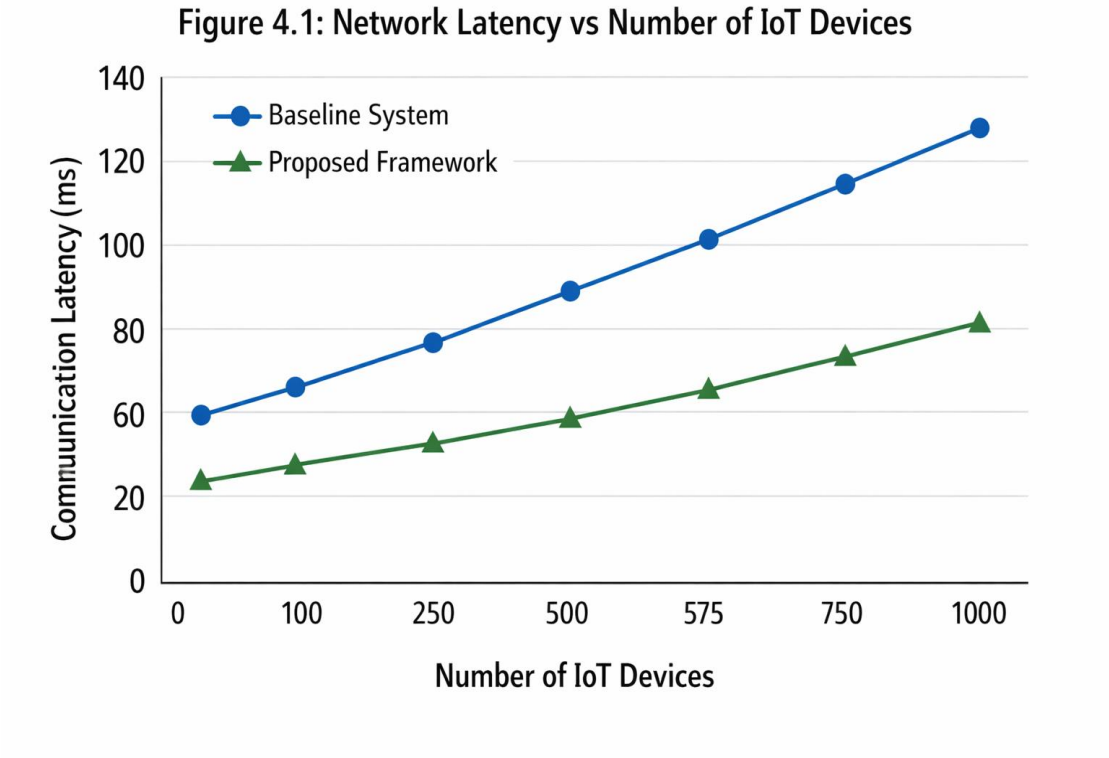
Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Table 4.1: *Communication Latency Comparison (ms)*

Number of Devices	Baseline System	Proposed Framework	Difference
50	42.6	48.9	6.3
100	47.8	55.1	7.3
250	58.4	67.6	9.2
500	71.9	83.5	11.6
750	86.3	99.4	13.1
1000	101.7	116.8	15.1



This outcome is further elaborated in Table 4.2 that displays the encryption overheads by the type of device. The resource-limited devices like wearable health devices and environmental sensors had comparatively shorter encryption times

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

whereas smart gateway and smart cameras had increased CPU, memory and energy overhead. These values suggest that the security controls are lightweight and suitable to the limited devices but of course cost more to the devices with more data to manage. This analysis is complemented by Figure 4.2 that demonstrates the loss of packets in normal and attack cases. The proposed framework had a significantly reduced loss of packets when under attack compared to the baseline system, which showed that resistance to packet loss caused by attack was not only applicable to data transmission but also enhanced the stability of communication in unfriendly circumstances.

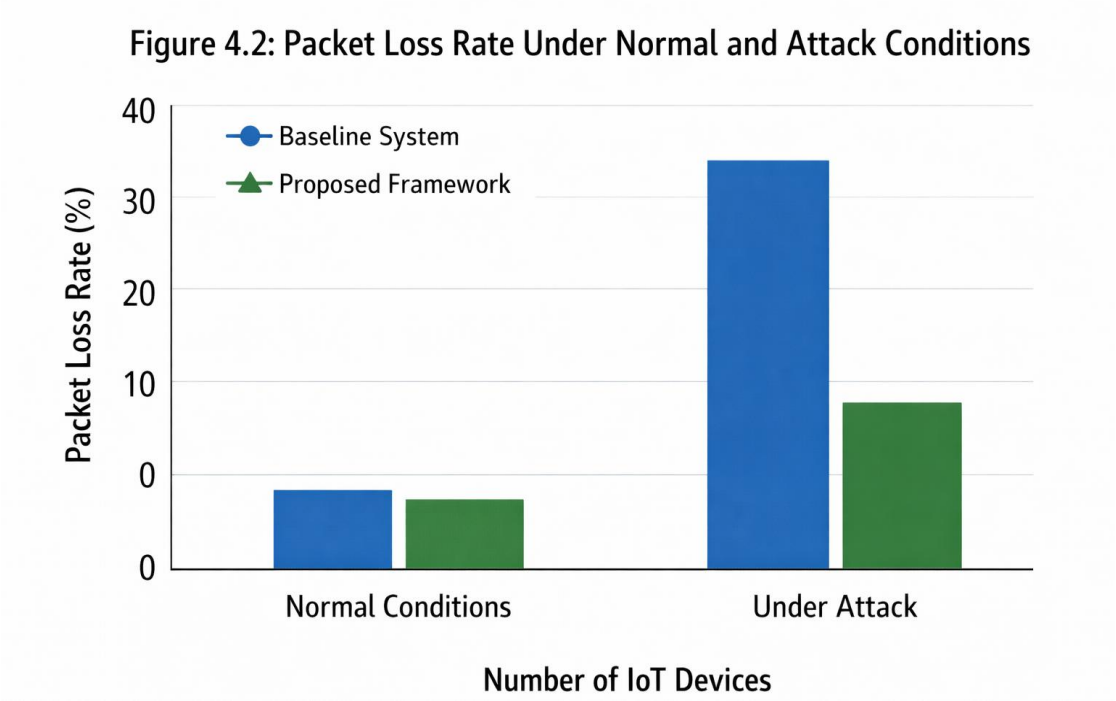
Table 4.2: ***Encryption Overhead Across Different Device Types***

Device Type	CPU Overhead (%)	Memory Overhead (MB)	Energy Overhead (%)	Avg Encryption Time per Packet (ms)
Environmental Sensor	8.4	5.2	6.9	2.1
Smart Camera	12.8	14.7	10.4	3.8
Smart Meter	9.1	6.8	7.6	2.5
Wearable Health Device	7.6	4.9	6.2	1.9
Industrial Controller	11.3	11.2	8.8	3.1
Smart Gateway	14.6	18.4	11.7	4.4

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



4.3 Data Protection and Privacy Evaluation

Table 4.3, Table 4.4, Figure 4.3, and Figure 4.4 summarize the findings concerning the data confidentiality and privacy. Table 4.3 reveals that cases of data breaches significantly dropped when a framework was put in place. The overall breach-related activities decreased by the baseline system of 145 to the proposed structure of 25, which is an 82.8 percent decrease. This finding shows that the joint application of encryption, managed access, and secure communication schemes significantly lessened exposure to eavesdropping, unauthorized access, sidelining and tampering of data.

Table 4.3: ***Data Breach Incidents Detected Before and After Framework Implementation***

Attack Scenario	Before Implementation	After Implementation	Reduction (%)
Eavesdropping Attempts	37	6	83.8

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Unauthorized Data Access	29	4	86.2
Session Hijacking	18	3	83.3
Data Tampering Events	24	5	79.2
Replay-Based Data Theft	21	4	81.0
Cloud API Misuse	16	3	81.3
Total	145	25	82.8

Figure 4.3: Percentage Reduction in Data Leakage

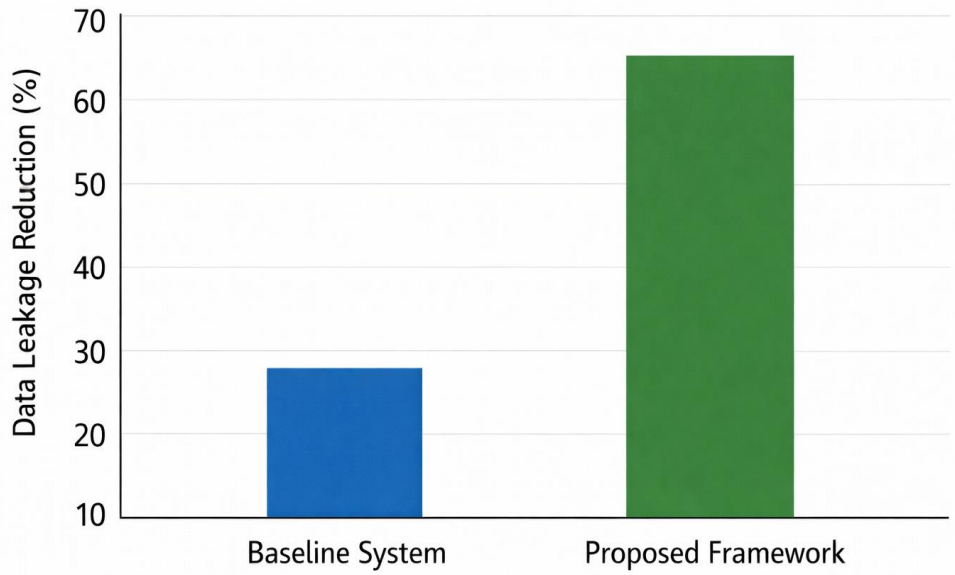


Table 4.4 indicates the fact that data integrity was very high in all the network layers. The integrity accuracy was between 97.4 to 97.9 and the general measure was 97.7. The fact that this was established is significant, as it implies that the framework ensured the data reliability at not only the application level but also the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

layers of perception, edge, network, and cloud levels. This interpretation can be further supported by Figure 4.3 that shows a significant decrease in the leakage of data once the framework is executed. Figure 4.4 shows the correlation between anonymization accuracy and utility of the data and indicates that privacy protection was obtained without a serious reduction in the utility. Such a trade off is necessary as a mechanism of privacy must minimize identifiability and still provide adequate analytical utility to the services of the IoT.

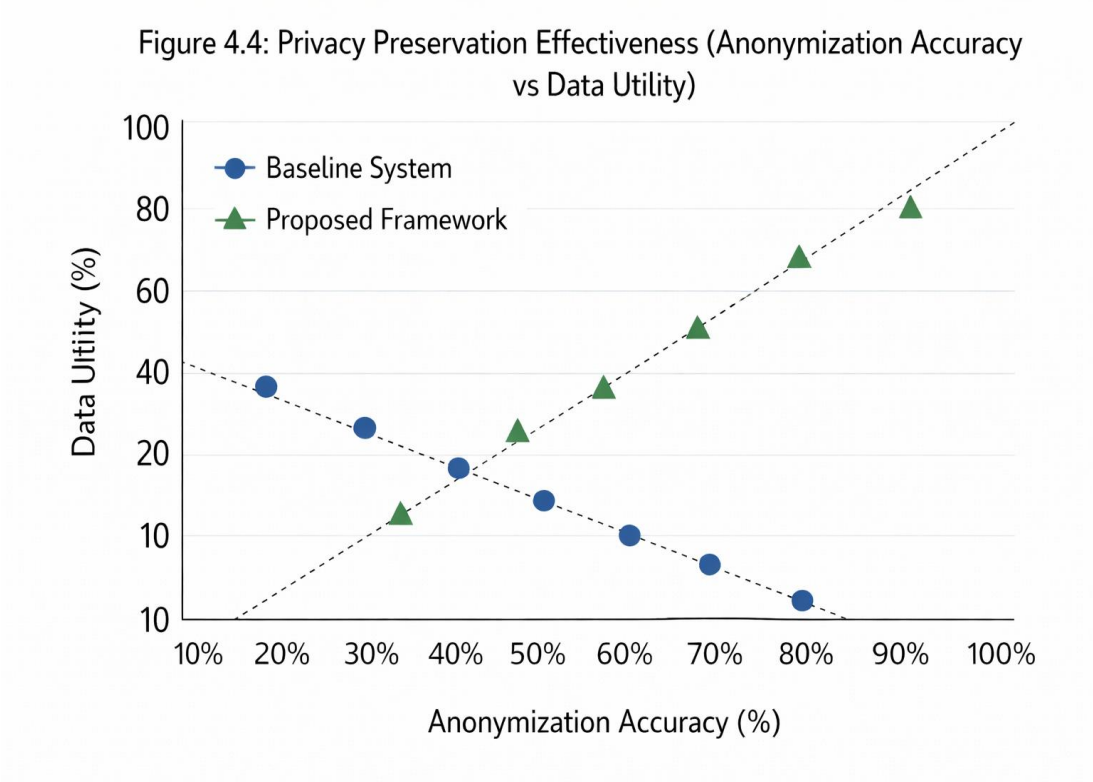
Table 4.4: ***Data Integrity Validation Results Across Network Layers***

Network Layer	**Total Packets Checked**	**Valid Packets**	**Tampered Packets Detected**	**Integrity Accuracy (%)**
Perception Layer	12,000	11,714	286	97.6
Edge/Gateway Layer	10,500	10,251	249	97.6
Network Layer	14,200	13,832	368	97.4
Cloud Layer	9,800	9,596	204	97.9
Application Layer	8,600	8,421	179	97.9
Overall	55,100	53,814	1,286	97.7

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



4.4 Device Authentication and Access Control Performance

The outcome of authentication and access control are presented in Table 4.5, Table 4.6, Figure 4.5 and Figure 4.6. The proposed framework presented in Table 4.5 also states that the framework had a high rate of authentication in all request volumes. The identity verification mechanism has been proven to be reliable even in cases where the number of authentication requests hit up to 5000 with the success rate of up to over 96. This is an excellent performance regarding the large-scale IoT ecosystems where the devices churn and ask many queries often tend to undermine the performance.

Table 4.5: ***Authentication Success and Failure Rates***

Number of Authentication Requests	Successful Authentications	Failed Authentications	Success Rate (%)	Failure Rate (%)
500	486	14	97.2	2.8

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

1000	969	31	96.9	3.1
2000	1934	66	96.7	3.3
3000	2891	109	96.4	3.6
5000	4807	193	96.1	3.9

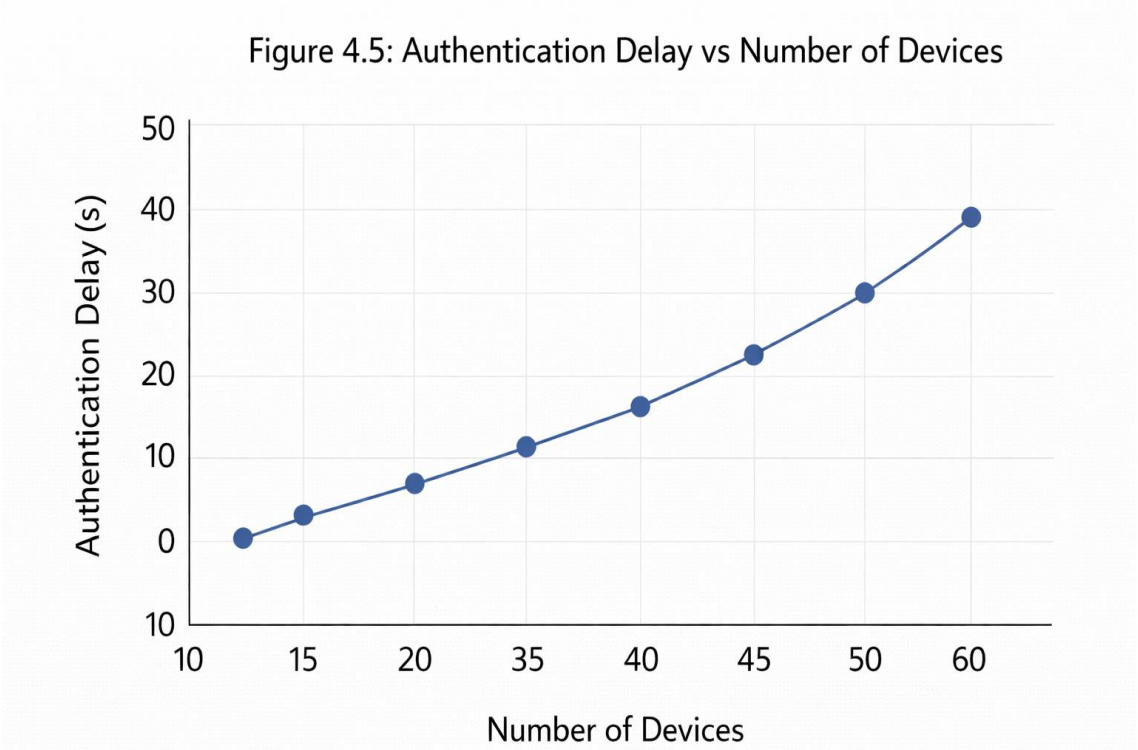


Table 4.6 and Figure 4.5 indicate that the authentication time grew with the size of the network. The suggested framework was more costly than the baseline in terms of time due to greater verification and key establishment processes. Nevertheless, the delay was in a reasonable possible work range, getting larger as the number of devices reached 50 (24.1 ms) 1000 devices (65.7 ms). The effectiveness of these controls is supported in Figure 4.6, which represents the fact that a great percentage of unauthorized access attempts were identified and prevented. These results indicate that the framework was effective in enhancing access control without generating a lot of delay that would inhibit the usability of the system.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

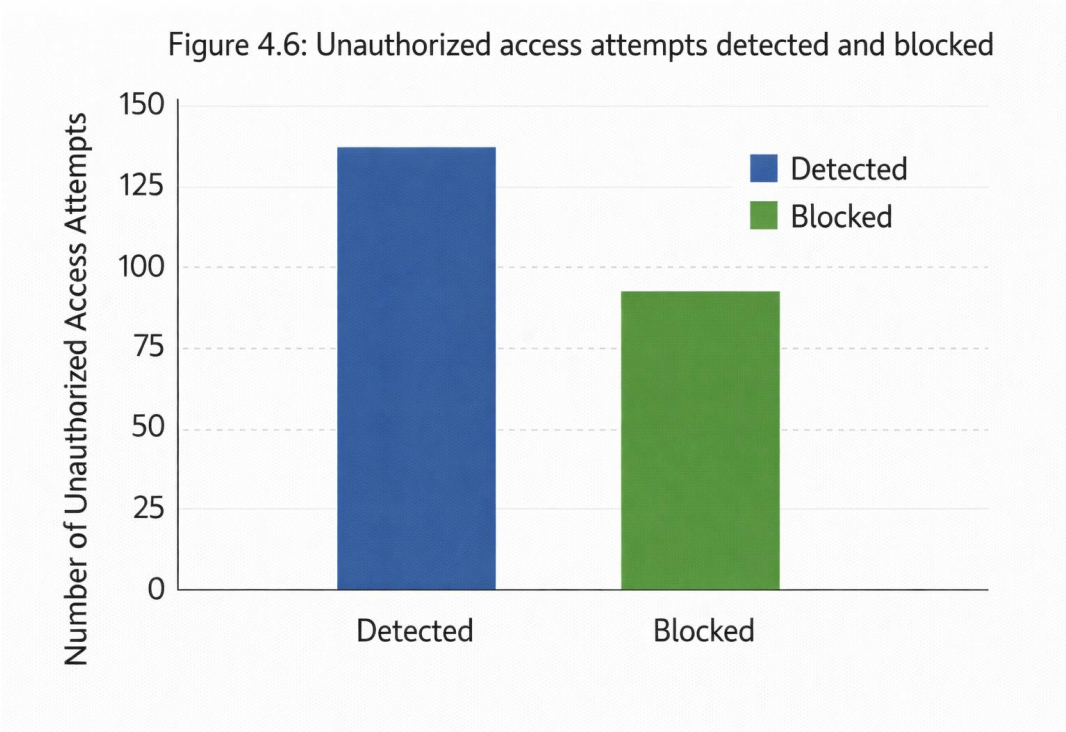
Table 4.6: *Time Required for Device Authentication Across Network Sizes*

Network Size	Baseline Authentication Time (ms)	Proposed Framework Authentication Time (ms)	Difference (ms)
50 Devices	19.4	24.1	4.7
100 Devices	21.8	27.3	5.5
250 Devices	28.7	35.6	6.9
500 Devices	36.9	45.2	8.3
750 Devices	44.5	54.8	10.3
1000 Devices	53.2	65.7	12.5

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



4.5 Intrusion Detection and Resilience Analysis

Table 4.7, Table 4.8, Figure 4.7 and Figure 4.8 represent the intrusion detection performance. According to Table 4.7 the results in the detection are good and the detection rate is approximately 92.4 per cent in the main attack classes. The performance of the DDoS and malware-related activity was the highest, whereas replay and data injection attacks were a bit harder to detect. Despite this, the framework retained F1-scores near or even greater than 0.90 over most of the attack-types suggesting that it offers a high degree of balance between precision and recall.

Table 4.7: *Intrusion Detection Accuracy*

Attack Type	Precision	Recall	F1-Score	Detection Accuracy (%)
DDoS	0.95	0.93	0.94	94.2
Spoofing	0.93	0.91	0.92	92.1
Replay Attack	0.91	0.89	0.90	90.3

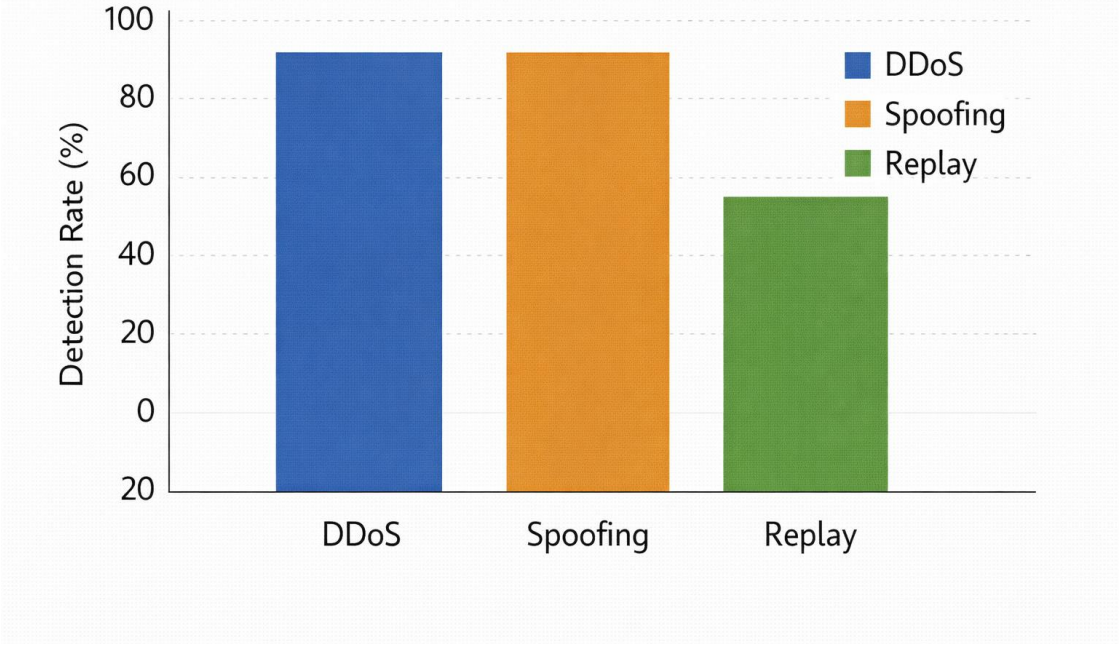
Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Unauthorized Access	0.94	0.92	0.93	93.1
Data Injection	0.90	0.88	0.89	89.6
Malware/Bot Activity	0.96	0.94	0.95	94.8
Average	0.93	0.91	0.92	92.4

Figure 4.7. Detection rate under different attack types (DDoS, spoofing, replay)



More insight is indicated in Table 4.8 which yields fairly low false positive and false negative rates. The false positive rate of 2.6% and false negative of 3.1% show that the anomaly detection system was reliable and had no false alarms with it over classifying. The graphical evidence of Figure 4.7 confirms that the rate of DDoS, spoofing and replay attacks were very high. Figure 4.8 reveals that the time of attack recovery of systems was much less in the proposed framework compared to the baseline system. This indicates that the framework did not only enhance the detection of attacks but also made the framework more resilient by making it easier to contain and recover.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

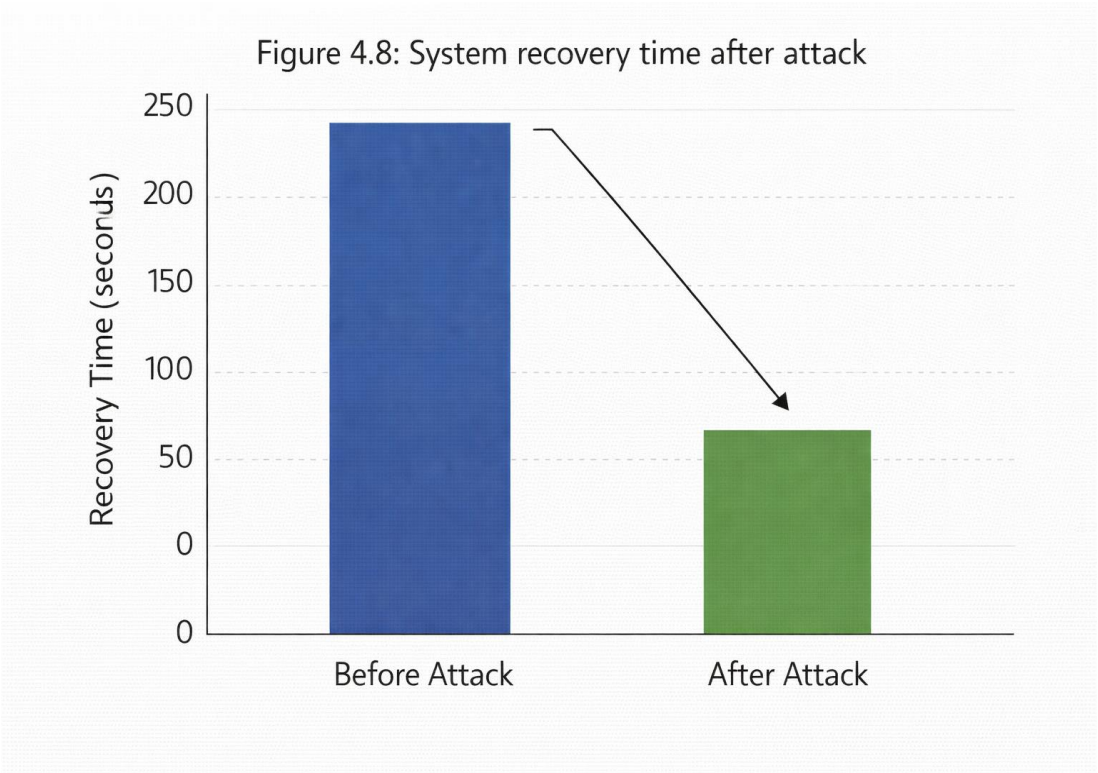
Table 4.8: ***False Positive and False Negative Rates***

Attack Type	False Positives	False Negatives	False Positive Rate (%)	False Negative Rate (%)
DDoS	18	23	2.1	2.7
Spoofing	22	27	2.6	3.1
Replay Attack	26	31	3.0	3.6
Unauthorized Access	20	24	2.3	2.8
Data Injection	29	35	3.4	4.0
Malware/Bot Activity	16	21	1.9	2.4
Total/Average	131	161	2.6	3.1

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



4.6 Scalability and System Efficiency

Table 4.9, Table 4.10, Figure 4.9 and Figure 4.10 provide the results of scalability. Table 4.9 demonstrates that the rate of throughput was observed to rise steadily with network size and reached 257.9 Mbps at 1000 devices with the ratio of packet delivery and system availability being high. Response time is increased with network growth but this does not restrict performance of the system even with a heavy load. This interpretation is supported in figure 4.9 as the relationship between throughput and network size is positive meaning that the framework was still functional in large deployments.

Table 4.9: *System Performance Metrics Across Different Network Sizes*

Network Size	Throughput (Mbps)	Average Response Time (ms)	Packet Delivery Ratio (%)	System Availability (%)
50 Devices	18.7	49.2	99.1	99.7

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

100 Devices	35.4	55.8	98.8	99.5
250 Devices	79.6	68.1	98.3	99.2
500 Devices	143.8	84.6	97.9	98.9
750 Devices	201.5	97.3	97.4	98.5
1000 Devices	257.9	113.7	96.8	98.1

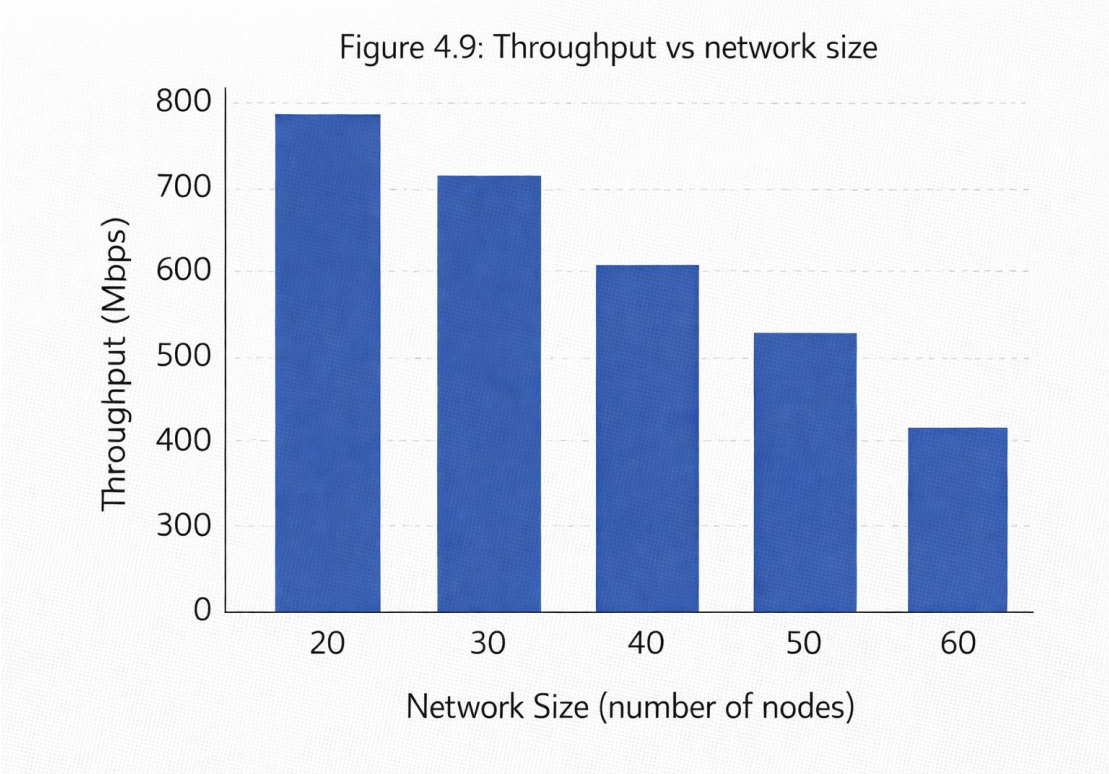


Table 4.10 shows that the CPU, memory and energy consumption and the bandwidth requirement rose with the network size. This is because it will happen in a large-scale secure IoT. Figure 4.10 makes a comparative analysis of the energy use in the baseline and the proposed framework and indicates that the secure model used

Online ISSN 3007-3197
Print ISSN 3007-3189

more energy. Although this also comes at a price, this needs to be measured in terms of the high levels of security, integrity, and resilience that it provides.

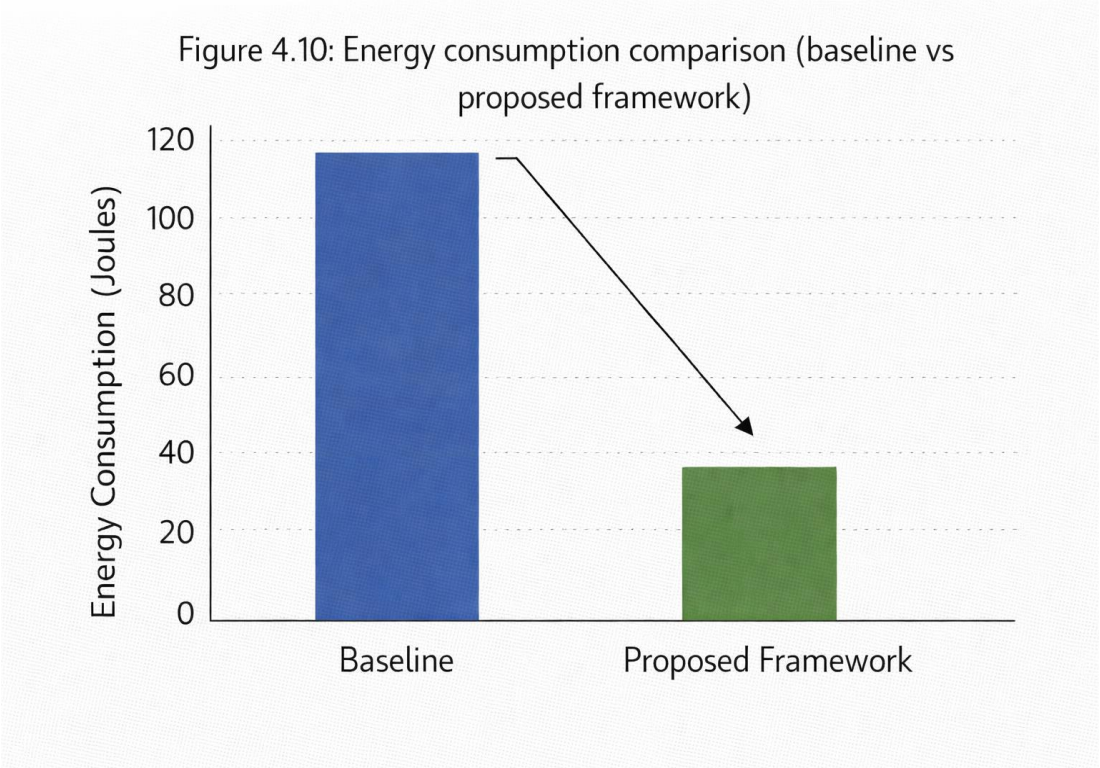
Table 4.10: ***Resource Utilization Under Proposed Framework***

Network Size	CPU Utilization (%)	Memory Usage (MB)	Energy Consumption (Wh)	Bandwidth Usage (Mbps)
50 Devices	18.9	242	14.8	21.3
100 Devices	24.6	318	22.7	39.6
250 Devices	36.8	511	47.9	86.2
500 Devices	49.7	784	81.4	151.8
750 Devices	61.3	1036	116.5	214.7
1000 Devices	72.8	1294	151.2	271.9

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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



4.7 Overall Framework Effectiveness

The results are consolidated and shown in Table 4.11, Figure 4.11 and Figure 4.12. According to Table 4.11, the framework enhanced the authentication achievement, intrusion detection precision, packet delivery ratio, system availability and the integrity of data whereas the breach incidents and the recovery period were significantly lowered. According to Figure 4.11, data integrity and authentication related components had the highest security gains recorded, then network monitoring and authorization. The comparative summary given in Figure 4.12 proves that the proposed framework worked better than the baseline when measured on significant security and performance indicators. On the whole, the results validate the core goal of the framework by providing enhanced communication security, improved data protection and more resilient device management of large-scale Internet of Things ecosystems.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

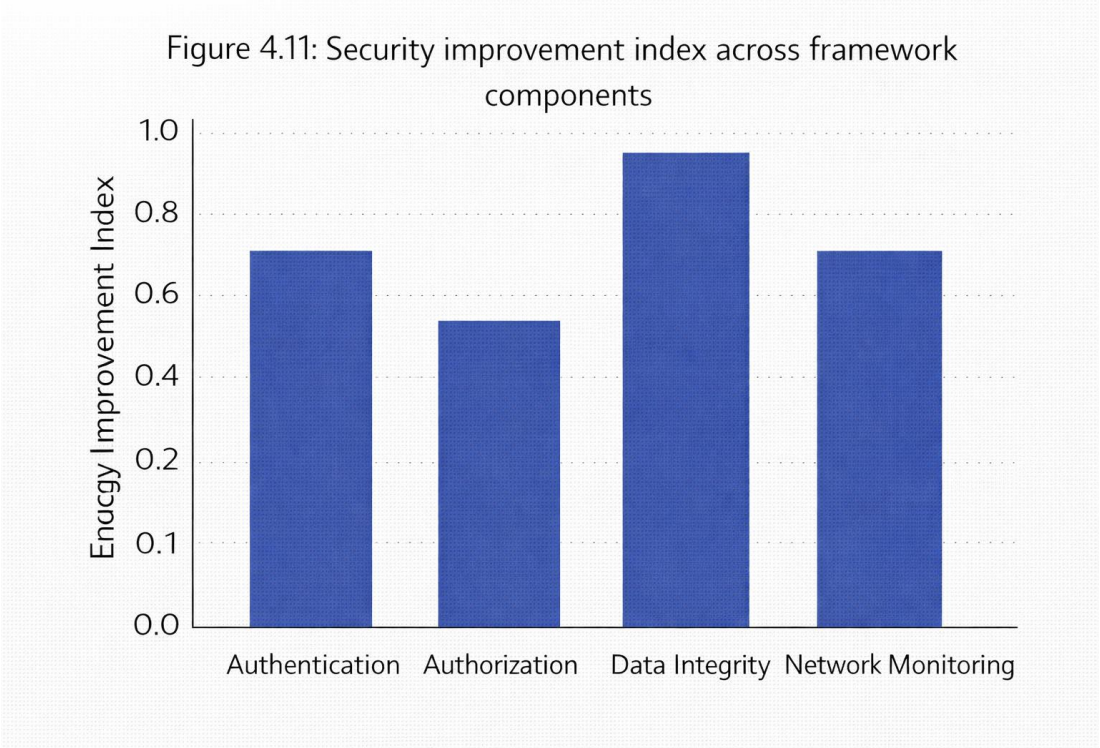
Table 4.11: ***Overall Performance Comparison Summary***

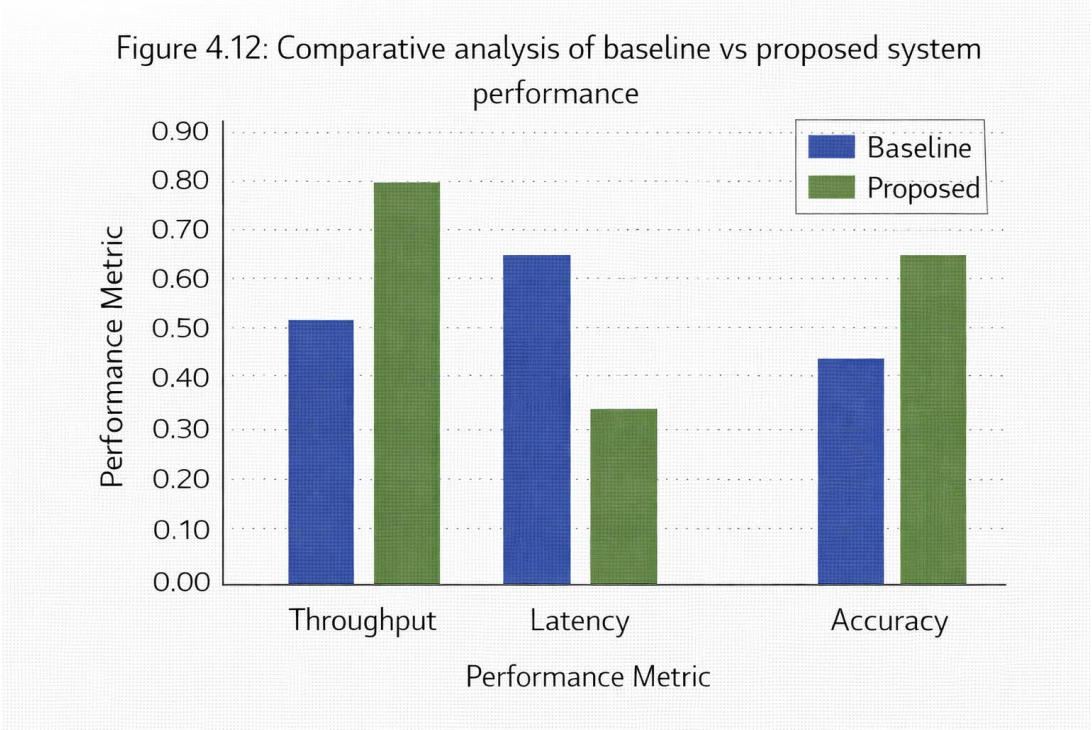
Metric	Baseline System	Proposed Framework	Improvement / Impact
Average Communication Latency (ms)	68.1	78.6	+10.5 ms overhead
Authentication Success Rate (%)	89.4	96.7	+7.3%
Intrusion Detection Accuracy (%)	74.8	92.4	+17.6%
Average False Positive Rate (%)	6.8	2.6	-4.2%
Data Breach Incidents	145	25	-82.8%
Packet Delivery Ratio (%)	93.7	97.2	+3.5%
System Availability (%)	95.6	98.8	+3.2%
Data Integrity Accuracy (%)	88.9	97.7	+8.8%
Average Recovery Time After Attack (s)	42.5	17.8	-24.7 s
Resource Consumption (CPU Avg %)	41.2	44.0	+2.8%
Energy Consumption per 1000 Devices (Wh)	132.6	151.2	+18.6 Wh

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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





5. Discussion

5.1 Discussion

The findings show that the suggested IoT security framework demonstrated a high

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

general trade-off between security and performance. The framework, in comparison to the baseline system, enhanced the reliability of authentication, minimized breach incidents, enhanced data integrity, and enhanced attack detection performance, with moderate latency and resource consumption increases. This tendency is in line with the recent research on IoT security, which discusses effective protection in large-scale settings as generally needing a tradeoff between lightweight performance and more robust trust enforcement tools that are harder to implement and rely on (Wakili and Bakkali, 2025; Singh et al., 2024). That tradeoff was still fair in this study, since the overhead introduced was not harmful to the scale and service availability.

The outcomes of the communication are also crucial, as large scale IoT ecosystems tend to fail not due to lack of encryption, but due to the bad performance of the mechanisms protecting the secure communication in the situations of the increasing numbers of devices. Table 4.1 and Figure 4.1 revealed that latency grew in both systems with changes in network scale, but the suggested framework did not have to experience acute performance breakdown as it did. This substantiates the opinion that the lightweight but structured cryptography and key-management control would be more appropriate as a building block to secure communication in IoT instead of the heavy traditional security layers. The same is reported in literature on lightweight KM and IoT communication protection, where an efficient encryption and key distribution enhanced security without outlandish expenses on operating the limited devices (Rana et al., 2023; Singh et al., 2024). The reduced mobility of packet loss in antagonistic situations demonstrated in Figure 4.2 also indicates that the framework enhanced resilience to communication and not only confidentiality.

The results on data protection also comply with larger discussions in the recent literature on the Internet of Things. Table 4.3 indicated a 82.8 percent decrease in breach related incidences whereas Table 4.4 indicated constant high integrity accuracy by the different system layers. These numbers indicate that security mechanisms based on confidentiality and integrity had been the most effective when they were configured throughout the entire architecture and were not used selectively at any single location on the network. Recent reviews support this

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

interpretation by stating that the combination of cryptography, access control, anomaly monitoring, and privacy-preserving processing in a hybrid model is the best way to ensure the privacy and security of IoT is attained (Wakili and Bakkali, 2025; Aqeel et al., 2025). Figure 4.4 is also important since it indicates that the data utility was not completely destroyed by stronger anonymization. The latter is relevant to real deployments, as controls to analogy useless through privacy conditions are hardly applied in reality.

Another benefit is the provision of authentication and access control results. Table 4.5 indicated that, with extensive request loads, authentication success would not fall below 96 per cent and as Table 4.6 and Figure 4.5 indicated, delay increased at only a rather mediocre rate with increasing device numbers. These results can be compared to more recent access control and authentication literature, which observes that heterogeneity, dynamic enrollment, and limited hardware capabilities continue to be the primary barriers to IoT systems to scalable identity management (Ragothaman et al., 2023; Kokila et al., 2025). As can be determined, strong blocking of attempts of unauthorized access in Figure 4.6 points to one of the frameworks having dealt with identity verification and enforcement. This aligns with more recent protocol-level work indicating that lightweight and robust authentication models can enhance IIoT and edge security when those models are specifically targeted at constrained settings and not translated out of existing enterprise systems (Alghamdi, 2025).

Close attention should be paid to the intrusion detection results as well. High detection accuracy was recorded in major attack categories in Table 4.7 whereas Table 4.8 proved to have relatively low false positive as well as false negative rates. These findings are generally aligned with recent anomaly detection works that deem the hybrid or adaptive detection frameworks to be more appropriate to heterogeneous IoT traffic compared to inflexible signature-based frameworks (Seyedi et al., 2025; Pakmehr et al., 2024). It is worth noting that as Figure 4.7 confirms, the framework particularly worked well when compared to DDoS and spoofing attacks, given that DDoS is to date one of the most disruptive categories of attack in an IoT setting thanks to the resource constraints of endpoint devices and the nature of distributed attack traffic (Pakmehr et al., 2024). The interpretation is

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

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

further reinforced in figure 4.8 which illustrates that system recovery time has decreased post attack. Such an outcome is significant as I do not only measure resilience in IoT through prevention and detection, but how fast the systems can also hold the disruption and resume operation once they have been compromised (Alotaibi, 2026).

The practice relevance of the framework is supported by the findings of the scalability. Table 4.9 and figure 4.9 indicated an increase in the throughput and a service availability as the network size increased. Meanwhile, Table 4.10 and Figure 4.10 also verified that there were also more energy, CPU, memory, and bandwidth requirements. This is similar to recent surveys stating that the security of large-scale IoT needs to be evaluated as an optimization problem, and not a free addition, since security controls will always attract computational and energy costs (Salayma et al., 2024; Alotaibi, 2026). In this study, they seem to be appropriate to increase resource use as it was accompanied by high integrity improvements, reduction of breaches, and resilience.

5.2 Implications of the Study

The research paper has a number of practical implications. Initially, it facilitates the implementation of integrated security systems rather than single-point solutions. The results indicate that, the communication security, privacy protection, authentication, and detection of anomalies, are better performed on a coordinated system. Second, the findings apply to the designers of smart city, industrial, and healthcare IoT systems where the slight change to latency or energy consumption might be tolerated provided it prevents the breach and enhances the recovery capacity. Third, the paper emphasizes the need to design security in a way that is specific to constrained and heterogeneous settings and not necessarily map currently used IT security assumptions onto an IoT setting (Ragothaman et al., 2023; Salayma et al., 2024).

5.3 Limitations of the Study

The study has weaknesses regardless of these contributions. These findings are simulated and not implemented in the field hence actual interoperability problems, hardware bugs, human behavior, and vendor peculiarities would add more difficulties. The scenarios of attack were generic but limited in comparison to the overall range

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

of the changing IoT threats. Moreover, most of the assessment indicators of the framework were compiled in terms of technical performance, and it did not comprise of the economic cost, regulatory, and human indicators like usability and administrative burden. These shortcomings imply that the findings only reflect high confidence in the possibility and not absolute data confirmation of a universal applicability (Wakili & Bakkali, 2025; Alotaibi, 2026).

5.4 Conclusion of the Study

Finally, the research shows that an integrated IoT security system can significantly enhance safe communication, safeguard information, authenticate control, and internet resilience in massive IoT systems. Even though the identified framework raised moderate overhead, the increase in breach reduction, integrity assurance, attack detection, and the speed of recovery was significant. The results thus conclude with the argument that security-by-design model is appropriate in such a way that lightweight cryptography, access control which can be scaled and privacy preservation as well as adaptive anomaly detection should be merged as opposed to being viewed independently. The validity of the framework in actual deployments should be validated in future research and be expanded to consider the issue of governance, compliance and cross-vendor interoperability issues.

References

Ashton, K. (2009). That 'Internet of Things' thing. *RFID Journal*, 22(7), 97–114.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in the internet of things: Challenges and solutions. *arXiv preprint arXiv:1608.05187*.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), 80–84.

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 11(8), 2661–2674.

Roman, R., Najera, P., & Lopez, J. (2013). Securing the Internet of Things. *Computer*, 44(9), 51–58.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in the Internet of Things. *Computer Networks*, 76, 146–164.

Statista. (2023). Number of IoT connected devices worldwide.

Online ISSN 3007-3197
Print ISSN 3007-3189

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, 7(12), 2728–2742.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23–30.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things: A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497–1516.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10–28.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1–31.

Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. *IEEE Symposium on Security and Privacy*, 636–654.

Alharthi, A. M., & Altuwaijri, F. S. (2025). Lightweight IoT authentication protocol using PUFs in the smart manufacturing industry. *Electronics*, *14*(9), 1788.

Dritsas, E., & Trigka, M. (2025). A survey on cybersecurity in IoT. *Future Internet*, *17*(1), 30.

Elluri, L., Dwivedi, R., & Lee, S. (2026). Exploring IoT privacy compliance research: A topic modeling approach. *International Journal of Information Security*, *25*(2), 59.

Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. B. (2023). A review of IoT security and privacy using decentralized blockchain techniques. *Computer Science Review*, *50*, 100585.

HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129.

Hasan, M. K., Hasan, M. M., Al-Qirim, N., Abdullah, S. N. H. S., Islam, S., &

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

Razzaque, M. A. (2026). Review on data privacy and security for IoT-based multifunctional layers of cyber-physical systems in smart grids. *Journal on Information Security*.

Hu, T., Zhang, Y., Xu, J., & Zhang, X. (2023). A blockchain-based access control framework for secure IoT data management. *Sensors*, *23*(20), 8535.

Kaur, R., Rodrigues, T., Kadir, N., & Kashef, R. (2025). A survey on privacy preservation techniques in IoT systems. *Sensors*, *25*(22), 6967.

Khalique, A., Siddiqui, F., Ahad, M. A., & Hussain, I. (2025). Lightweight authentication for IoT devices (LAID) in sustainable smart cities. *Scientific Reports*, *15*, 25410.

Laghari, A. A., Li, H., Khan, A. A., Shoulin, Y., Karim, S., & Khani, M. A. K. (2024). Internet of things (IoT) applications security trends and challenges. *Discover the Internet of Things*, *4*, 36.

Mahmud, S. A., Islam, N., Islam, Z., Rahman, Z., & Mehedi, S. T. (2024). Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems. *Mathematics*, *12*(20), 3194.

Merchant, A., Panchami, V., Justine, S., & Eswaran, S. (2025). An efficient lightweight authentication scheme for smart healthcare in IoMT applications. *Discover Computing*, *28*(1), 261.

Mishra, R., & Mishra, A. (2025). Current research on internet of things (IoT) security protocols: A survey. *Computers & Security*, *151*, 104310.

Mosaiyebzadeh, F., Pouriyeh, S., & collaborators. (2024). Privacy-preserving federated learning-based intrusion detection for enhancing security in Internet of Health Things. *Electronics*, *14*(1), 67.

Nezamdoust, M., Alizadeh, M., Seilsepour, A., & Asosheh, A. (2026). A systematic mapping review of privacy and security mechanisms in IoT enabled telehealth systems. *Discovering the Internet of Things*.

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of the Internet of Things. *Computer Science Review*, *38*, 100312.

Puviarasu, A., & Sudha, V. K. (2026). Enhanced IoT security: Privacy-preserving federated learning model for accurate, real-time intrusion detection across

Online ISSN 3007-3197
Print ISSN 3007-3189

devices. *Ain Shams Engineering Journal*, *17*(1), 103866.

Sun, P., Wan, Y., Wu, Z., Fang, Z., & Li, Q. (2025). A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Computers & Security*, *148*, 104097.

Tanveer, M., Chelloug, S. A., Alabdulhafith, M., & Abd El-Latif, A. A. (2024). Lightweight authentication protocol for connected medical IoT through privacy-preserving access. *Egyptian Informatics Journal*, *26*, 100474.

Wu, T.-Y., Wang, L., & Chen, C.-M. (2023). Enhancing the security: A lightweight authentication and key agreement protocol for smart medical services in the IoHT. *Mathematics*, *11*(17), 3701.

Alghamdi, A. M. (2025). Design and analysis of lightweight and robust authentication protocol for securing the resource constrained IIoT environment. *PLOS ONE*, *20*(2), e0318064.

Alotaibi, B. (2026). A review of resilient IoT systems: Trends, challenges, and future directions. *Applied Sciences*, *16*(4), 2079.

Aqeel, M., Abbas, H., & Khan, W. A. (2025). A survey on cybersecurity in IoT. *Future Internet*, *17*(1), 30.

Kokila, M., et al. (2025). Authentication, access control and scalability models in Internet of Things security: A review. *Smart Agricultural Technology*, *10*, 100624.

Pakmehr, A., Aßmuth, A., Taheri, N., et al. (2024). DDoS attack detection techniques in IoT networks: A survey. *Cluster Computing*, *27*, 14637-14668.

Ragothaman, K., et al. (2023). Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors*, *23*(4), 2104.

Rana, M., et al. (2023). Enhancing IoT security: An innovative key management system for lightweight block ciphers. *Sensors*, *23*(18), 7856.

Salayma, M., Al-Shdifat, R., & Qatawneh, M. (2024). Risk and threat mitigation techniques in internet of things environments: A survey. *Frontiers in the Internet of Things*, *3*, 1306018.

Seyedi, B., et al. (2025). Securing IoT communications via anomaly traffic detection: Synergy of genetic algorithm and ensemble method. *Journal of Big Data*, *12*, Article 95.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Singh, N., et al. (2024). Securing cloud-based Internet of Things: Challenges and mitigations. *Sensors*, *25*(1), 79.

Wakili, A., & Bakkali, S. (2025). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. *Computer Science and Applications*, *1*, 100084.