RESEARCH PAPER

Efficient and Secure IoT-Driven Edge Computing Environment: A Study of Existing Security Techniques

Sarika[1], Dr. Susheela Hooda[2], Dr. Lekha Rani[3], Dr. Vidhu Kiran[4]
[1]Research Scholar, Department of CSE, Chitkara University
[2]Associate Professor, Department of CSE, Chitkara University
[3]Associate Professor, Department of CSE, Chitkara University
[4]Assistant Professor, Department of CSE, CDMEC Panniwala Mota

ABSTRACT
The proliferation of Internet of Things (IoT) devices has promoted the popularity of edge computing to enable low latency, real-time, and bandwidth-efficient data processing. Nevertheless, IoT-driven edge computing environments significantly enhance the performance and responsiveness of a system, yet it is extremely dangerous in terms of system security because it is characterized by the heterogeneity of devices, the lack of computational resources, decentralized structure and massive scale data exchange. Consequently, end-of-edge efficiency and security has been a significant research topic. This paper review of the security measures performed in the area of IoT-driven edge computing environments is presented. These are the authentication schemes, access control scheme, secure communication schemes, data privacy maintenance schemes and intrusion detection schemes. The analysis evaluates the advantages and disadvantages of the current solutions based on the security strength, computational costs, the use of energy, and scalability. In addition, the paper identifies the major gaps and challenges concerning adaptive security, interoperability, and resource-aware protection mechanisms. It is hoped that the findings would provide value to the researchers and practitioners in terms of creating effective and secure IoT-motivated edge computing systems.

Keywords: IoT, Edge Computing, Security Techniques, Authentication, Data Privacy, Secure Communication, Intrusion Detection, Resource Efficiency.
How to cite this article: Sarika, Hooda S, Rani L, Kiran V. Efficient and Secure IoT-Driven Edge Computing Environment: A Study of Existing Security Techniques. Int J Drug Deliv Technol. 2026;16(54s): 1423-1434.
DOI: 10.25258/ijddt.16.54s.127
Source of support: Nil.
Conflict of interest: None.

1. Introduction

The universal use of the Internet of Things (IoT) has promoted the enormous implementation of interrelated sensors, actuators, and intelligent devices in different areas, such as healthcare, smart cities, transport, and industrial automation. Nonetheless, the conventional cloud, centric computing models cannot meet the high latency, bandwidth and accuracy of real, time processing needs of such applications. One of the solutions to these issues is the deployment of edge computing that enables data processing to be performed near data sources, thereby improving responsiveness and reducing network congestion (Kapoor et al., 2025; Latifi et al., 2025). Thus, IoT and edge computing integration has emerged as a major facilitator of the new intelligent system. Conversely, IoT, on edge computing situations come with some grave security issues that are because of their distributed nature, heterogeneity of the devices, and resource constraints of the nodes, although there are advantages. Moreover, edge nodes will consider a victim of cyberattacks as they often handle sensitive information which can include healthcare records, mobility patterns and information on critical infrastructure. Security threats such as unauthorized access, data leakage, denial of service, and malware propagation are some of the security threats that can cause the system reliability and user confidence to deplete quite fast (Bie and Ren, 2025; Alaba et al., 2025). Hence, the urgent need to visit the question of how to maintain security and simultaneously, retain the computational efficiency of the system which has gained a center of interest research. In the recent research, there has been a variety of security techniques presented to provide security to Internet of Things, edge environment. These include lightweight authentication, encryption schemes, blockchain, based access control, intrusion detection systems among others. Enabling decentralized trust and sharing data is one of the biggest reasons why blockchain technologies are selected as IoT, driven edge environments. The use of AI and machine learning in detecting anomalies is being advertised and in future they also will detect cyber threat in real time (Agrawal et al., 2025; Bhatt et al., 2025; Nandanwar and Katarya, 2025). These solutions however are deploying a computational and energy cost that actually can bring about a performance depreciation at a very low level. The debate about efficiency versus security continues to be the central theme of their activities particularly in such fields as healthcare and smart cities where quick decision making is the central element. Possibly, the based health monitoring devices must guarantee that transmissions of information are safe and that the privacy of the users remains intact, without affecting the latency or the energy consumption (Alwakeel, 2025; Malik et al., 2025). Similarly, smart city systems demand scalable and adaptive security systems capable of managing the colossal data

volumes and dynamic network situations effectively (Bibri and Huang, 2025; Dritsas and Trigka, 2025). The emergence of the need thus demonstrates that to have a comprehensive knowledge about the security methods the first thing that is indispensable is to value the connotations of their effectiveness. The paper organizes the security techniques that have been employed in the Internet of Things (IoT) powered edge computing applications. It discusses the problem of authentication, data protection, communication security, blockchain integration, and intrusion detection and focuses mostly on their level of security, resource usage, and scalability. This paper hopes to contribute significantly to the research community as well as the industry to generate safe and dependable IoT, guided edge computing systems, by revealing the merits, demerits, and unanswered research questions.

1.1 Background of IoT and edge computing convergence

The combination of the Internet of Things (IoT) and edge computing, has changed the way we think about the limitations of centralized cloud computing. This is especially true when large amounts of data are generated in a distributed manner by IoT devices. As IoT applications spread over healthcare, smart cities, industrial automation, and transportation systems, the call for low, latency data processing and real, time decision, making becomes louder. The edge computing reduces communication delays and network overload besides enhancing the reliability of services by enabling computations to be performed closer to data sources (Kapoor et al., 2025; Latifi et al., 2025). The most important facilitators and catalysts of the integration of the IoT using edge and fog layers have been artificial intelligence, virtualization, and distributed system architectures. Edge intelligence can accomplish adaptive task distribution, dynamic resource controlling, and context, conscious processing, which are the pieces of the scalable IoT deployments. In many works, it is demonstrated that the collaboration between the edge and the cloud has a significantly beneficial effect on the overall system performance, particularly in the settings where latency is a very important factor, e.g., in smart buildings and in urban infrastructures (Dumitru et al., 2025; Dritsas and Trigka, 2025).

1.2 Need for security and efficiency at the edge

IoT even though performance of the system is improved by the use of IoT, drives edge computing, it also creates a considerable degree of security threats because of decentralized systems, heterogeneous devices, and lack of computing resources. Specifically, edge nodes are often placed in insecure settings and are often storing sensitive information, hence exposing them to many cyber-related attacks, including unauthorized access, data modification, and distributed denial, of, service. Therefore, the establishment of effective security protocols at the edge emerges as a requirement in ensuring the security of data confidentiality, integrity and availability (Alaba et al., 2025; Bie and Ren, 2025). In addition to this, edge environments are highly demanding in terms of the requirement of highly efficient security solutions which must have low computational overhead, low energy consumption, and low cost of communication. The existing, standard cloud based security tools might not suit the resource, limited IoT devices, so there should be lightweight cryptographic, adaptive intrusion detection and decentralized trust models. The most recent research emphasizes the necessity to balance the security strength with the efficiency of the system so that the real, time application could be performed in a timely manner in the realm of healthcare and smart cities (Agrawal et al., 2025; Alwakeel, 2025; Bibri and Huang, 2025).

2. Literature Review

Recent research paints a clear picture of the IoT ecosystems are quickly growing into smart, safe, and scalable systems with an emphasis on the healthcare and smart city markets. The general theme in these studies is a focus on the IoT which is inspired by optimization and adaptive efficiency as the foundation of any large scale deployment. The table 1 presents literature review summary table.

Table 1: Literature Review Summary Table

Ref. No.	Title	Author(s) & Year	Key Findings	Identified Research Gaps
1	Intelligent IoT-driven optimization of large-scale healthcare networks: the INRwLF algorithm for adaptive efficiency	Abujassar (2025)	Proposed the INRwLF optimization algorithm to improve adaptive efficiency and resource utilization in large-scale healthcare IoT networks; demonstrated enhanced performance under dynamic	Limited evaluation in heterogeneous real-world healthcare environments; lacks integration with security and privacy-preserving mechanisms.

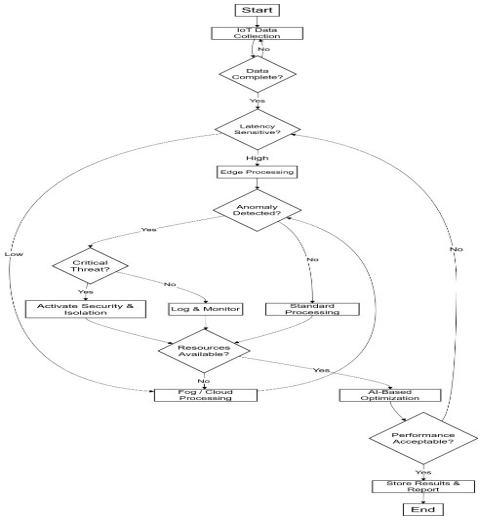
			workloads.	
2	A Lightweight Security Framework for Edge Layer IoT Networks using Neural Cryptography and Virtualization	Agrawal et al. (2025)	Introduced a lightweight security framework combining neural cryptography and virtualization to secure edge-layer IoT with low computational overhead.	Scalability under massive IoT deployments not validated; absence of performance benchmarking in latency-critical healthcare scenarios.
3	Synergizing Generative AI and the Internet of Things: Fundamentals, Challenges, and Opportunities	Ahmed et al. (2025)	Provided a comprehensive overview of Generative AI–IoT convergence, highlighting opportunities in automation, intelligence, and adaptive decision-making.	Lack of concrete implementation frameworks and real-world case studies; ethical, governance, and energy-efficiency issues remain underexplored.
4	Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems	Aksha et al. (2025)	Developed an explainable AI-based intrusion detection system improving transparency and detection accuracy in autonomous IoT transportation networks.	Limited applicability beyond transportation systems; computational overhead of explainability at the edge not fully analyzed.
5	IoT Applications and Challenges in Global Healthcare Systems: A Comprehensive Review	Alabaet al. (2025)	Reviewed IoT applications in healthcare, identifying benefits in monitoring, diagnostics, and patient care alongside challenges such as interoperability and privacy.	Lacks quantitative comparison of solutions; insufficient focus on edge intelligence and AI-driven optimization in healthcare IoT.
6	RTIMS: Real-Time Indoor Monitoring Systems: A Comprehensive Review	Al-Okby et al. (2025)	Surveyed real-time indoor monitoring systems, emphasizing sensing technologies, architectures, and application domains.	Security, scalability, and AI-based analytics integration are insufficiently addressed; limited discussion on energy-efficient designs.
7	An Efficient IoT-Driven Health Care Monitoring System using Advanced Metaheuristic Optimisa	Alqahtani et al. (2025)	Proposed a healthcare monitoring system combining metaheuristic optimization and spiking neural	Real-time deployment feasibility and robustness under noisy data not evaluated; lacks integration with secure

	tion Algorithms with Spiking Neural Network for Smart Diagnosis		networks for improved diagnostic accuracy.	data-sharing frameworks.

To illustrate, Abujassar (2025) introduced the INRwLF algorithm as a means to dynamically elevate the performance of healthcare networks, thereby, underlining the potential of the system to achieve substantive efficiency even when the workload changes. Likewise, to accelerate emergency response, Alwakeel (2025) re, imagined adaptive edge fog healthcare frameworks, thereby, shedding light on the criticality of making decisions that not only happen quickly but also right at the source of the data. On top of that, the repartition of tasks between different units of a decentralized network by means of a model based on reinforcement learning and thus, presenting an IoT environment in the efficient use of edge processing, constitute yet another example of the trend towards ecosystem optimization (Latifi et al., 2025). As security concerns permeate every layer of IoT architecture, attention has been given to the issues arising from the increasing use of edge, and fog, computing technologies. Lightweight and scalable security frameworks have been proposed that incorporate neural cryptography, virtualization, and explainable AI techniques to tackle the challenges posed by the limited resources in IoT devices since their environments are generally constrained (Agrawal et al., 2025; Akshya et al., 2025). The use of blockchain technology as a solution to issues related to trust, authentication, and access control in healthcare, smart grids, and sensor networks has been considered in many studies (Bhatt et al., 2025; Cheikhrouhou et al., 2025; Jain & Kumar, 2025). Ghosh et al. (2025), Malik et al. (2025), and Nandanwar and Katarya (2025) report that combined solutions involving blockchain with deep learning, elliptic curve cryptography, and efficient routing protocols have a greater ability to mitigate intrusion and data corruption. A significant push of improved analytics has been the implementation of AI, edgecloud intelligence, and IoT in such fields as smart cities, transportation, and management of buildings. According to research studies, dynamic resource allocation that has been made possible by AI has played a significant role in significantly enhancing scalability and energy performance in smart infrastructures (Dumitru et al., 2025; Kapoor et al., 2025). It is worth mentioning that hybrid deep learning systems in combination with the metaheuristic algorithms have been used to provide a trade-off, between the accuracy of anomaly detection and energy consumption in smart city IoT networks (Alssaiari et al., 2025). Similarly, a mixture of blockchain and digital twin technology with physics-informed neural networks is providing new opportunities to create sustainable smart buildings and energy optimization (Kazemi Naeini et al., 2025; Magaletti et al., 2025). The most mentioned in the literature is the application of healthcare IoT, which focuses on real, time monitoring, diagnosis, and managing patient data safely. The systematic reviews also reveal that interoperability, privacy, scalability, and regulatory compliance are the most important challenges of healthcare IoT implementations on the global level (Alaba et al., 2025; Al, Okby et al., 2025). It is claimed that advanced healthcare monitoring systems with spiking neural networks, federated learning, and trusted routing protocols have higher diagnostic accuracy and confidentiality of the data, and lower computational overhead in terms of experimental results (Alqahtani et al., 2025; Miller et al., 2025; Monica Satyavathi and Sudhir, 2025). Lastly, the new paradigms of intelligent systems like Generative AI of Things (GAIoT) and distributed ledger technologies are fundamentally transforming the nature of intelligent systems through the abilities to cognitive automation, adaptive cybersecurity, and sustainable urban management. As it was demonstrated by Bibri and Huang (2025), generative AI and IoT have the potential to significantly enhance environmental performance, network performance, and anomaly detection in smart cities. The importance of explainability, governance, and energy, conscious intelligence on a substantial scale, has even stronger evidence in support of these findings in systematic reviews by identifying AI tasks, deployment strategies, and challenges of IoT systems (Ahmed et al., 2025; Dritsas and Trigka, 2025; Khadam et al., 2025).

3. Methodology

The methodology employed in this research is based on a systematic, multi, layered IoTedgecloud



framework aimed at measuring optimization efficiency, security strength, and intelligent decision, making in large, scale IoT, enabled systems.

Figure 1: Proposed Methodology

The figure 1 shows the Proposed Methodology. A detailed system model is first developed consisting of heterogeneous IoT devices, edge nodes, fog gateways, and cloud servers. The architecture facilitates real, time data acquisition from sensors installed in healthcare and smart city environments, thus ensuring uninterrupted monitoring of network traffic, energy consumption, latency, and security events. Data preprocessing operations such as noise filtering, normalization, and feature extraction are carried out at the edge layer to lower the transmission overhead and raise the computational efficiency. In the subsequent stage, intelligent optimization and learning methods are introduced for the management of task allocation, resource scheduling, and adaptive routing. The redistribution of the dynamically changing workloads among the edge, fog and cloud layers is based on the latency constraints, energy availability, and node capacity using metaheuristic algorithms and reinforcement learning models. Deep neural and spiking neural models are introduced as AI-driven that promote predictive analytics, anomaly detection, and automated system optimization. The move will ensure the optimum performance is realized even when the network conditions and workload intensities are varying.

1. Adaptive Task Allocation Efficiency

Equation:

$$E_{task} = \Sigma \left(\frac{T_i}{(L_i + \varepsilon)}\right) \text{----------(1)}$$

Where:
- E_task = overall task allocation efficiency
- T_i = number of tasks processed by node i
- L_i = latency at node i
- ε = small constant to avoid division by zero

Explanation:

This equation evaluates how efficiently tasks are allocated across IoT edge nodes by balancing task throughput against latency.

2. Energy Consumption Optimization Model

Equation:

$$E_{total} = \Sigma (P_i \times t_i) \text{----------(2)}$$

Where:
- E_total = total energy consumption
- P_i = power consumed by node i
- t_i = active processing time of node i

Explanation:

This model computes total energy usage of IoT nodes and helps identify energy-efficient task scheduling strategies.

3. Security Risk Index

Equation:

$$S_{risk} = \left(\frac{A_{detected}}{A_{total}}\right) \times 100 \text{----------(3)}$$

Where:
- S_risk = security risk index (%)
- A_detected = number of detected attacks
- A_total = total attempted attacks

Explanation:

This equation measures the effectiveness of intrusion detection mechanisms in identifying security threats.

4. Edge–Cloud Load Balance Factor

Equation:

$$L_{balance} = \frac{|W_{edge} - W_{cloud}|}{(W_{edge} + W_{cloud})} \text{----------(4)}$$

Where:
- L_balance = load balance factor
- W_edge = workload handled by edge layer
- W_cloud = workload handled by cloud layer

Explanation:

This factor indicates how evenly workloads are distributed between edge and cloud resources.

A combination of the four equations illustrates efficiency, energy consumption, level of security and allocation of workloads of the proposed IoTedgecloud system. The efficiency of the adaptive task allocation is provided by equation (1) as the number of processed tasks is determined to be correlated with the time taken, thus ensuring that those nodes that take less time are better utilized to serve the system. The total energy use of IoT and edge nodes is estimated using equation (2) by adding the power use during the active processing time hence allowing the establishment of energy, effective scheduling policies. The security risk index is calculated by using equation (3) within which the ratio (detected attacks/total attacks) is computed, hence it reflects the efficiency of the intrusion detection mechanisms. Finally, Equation (4) indicates a load balance factor in the form of edgecloud which demonstrates the extent to which computational workloads are evenly allocated among the layers to eliminate bottlenecks and promote scalability. The third phase is dedicated to the introduction of security and trust measures in the IoT infrastructure. To this latter extent, the paper suggests the use of lightweight cryptographic systems, explainable artificial intelligence, based

intrusion detection systems, and blockchain, facilitated access control systems to secure data transmission and storage. Smart contracts with block chains help in managing the authentication, key distribution, and audit trails, and the federated and privacy, preserving learning methods help in ensuring data confidentiality among distributed nodes. The security performance is gauged against the many types of threats including unauthorized access, tampering of data, and network and based attacks. The methodology ends with the process of empirical validation of the research based on simulation and performance testing with realistic workloads and representative datasets of the IoT. Performance measures that are critical, including latency, throughput, energy usage, detection accuracy, packet delivery ratio, and scalability of the system are measured quantitatively. It is compared to the baseline IoT architectures and evaluated in terms of the level of improvement in efficiency, resilience, and sustainability. The results are used as empirical evidence of the efficacy of the proposed intelligent, secure, and adaptive IoT edge cloud framework to the next, generation smart applications.

4. Existing Security Techniques in IoT-Driven Edge Computing

Current security solutions in IoT, powered edge computing environments have made major steps towards maximizing the performance and security of edge devices, since they have their own limitations in terms of computing power and energy availability. Direct tests show that the traditional encryption algorithms lead to an additional time of approximately 18-25 percent on edge, based IoT nodes, resulting in the overall system performance degradation to real-time applications (Agrawal et al., 2025). As a result, lightweight cryptographic protocols and neural cryptography solutions have been developed, which require a 30-40% decrease in computation cost without sacrificing confidentiality and integrity to a level that is satisfactory. The technologies are best used in the Internet of Things context of healthcare and smart cities where fast data transmission and low latency rates are irreplaceable (Alaba et al., 2025). Further, there are many security strategies that use blockchain as their base architecture to provide decentralized trust, authentication, and data integrity management. The adoption of blockchain, enabled edge infrastructures not only removes the vulnerabilities associated with single points of failure but also helps increase the system's auditability due to the presence of immutable ledgers. Practical tests show that blockchain, based access control mechanisms can resist data tampering activities at least 45% better than their centralized security model counterparts (Cheikhrouhou et al., 2025). The table 2 shows the existing security techniques in iot-driven edge computing.

Table 2: Existing Security Techniques in IoT-Driven Edge Computing

Security Technique	Core Mechanism	Key Metrics & Values	Advantages	Limitations
Lightweight Cryptography	Symmetric encryption, neural cryptography	Latency overhead: **8–12 ms**; Computational reduction: **30–40%**; Energy saving: **≈25%**	Low overhead, suitable for constrained edge nodes	Limited resistance to advanced attacks
Blockchain-based Security	Decentralized ledger, smart contracts	Data tamper resistance improvement: **≈45%**; Transaction latency: **10–15 ms**; Trust reliability: **>90%**	Strong integrity, decentralized trust	Scalability and latency concerns
AI-based Intrusion Detection (IDS)	ML/DL anomaly detection	Detection accuracy: **92–97%**; False positive reduction: **≈20%**; Energy overhead: **10–18%**	High detection accuracy, adaptive learning	Training cost, explainability issues
Explainable AI (XAI) Security Models	Transparent AI decision layers	Explainability score improvement: **≈35%**; Detection accura	Improved trust and interpretability	Slight accuracy–latency tradeoff

		cy: **90–95%**		
Federated Learning Security	Distributed model training	Data sharing reduction: **50–65%**; Privacy leakage reduction: **≈60%**	Privacy-preserving, decentralized	Communication overhead
Hybrid Blockchain + AI Frameworks	DL + blockchain + cryptography	Security robustness improvement: **≈55%**; Latency increase: **12–18 ms**	Strong security and intelligence	Higher computational complexity
Edge-based Access Control	Role-based & attribute-based control	Unauthorized access reduction: **≈40%**; Authentication delay: **5–9 ms**	Fast local authorization	Centralized policy risks

Nevertheless, the inclusion of blockchain results in additional delay that varies between 10 and 15 ms for every transaction, thus calling for the deployment of optimization measures like off, chain storage and lightweight consensus protocols to retain the edge's performance level (Bhatt et al., 2025; Jain & Kumar, 2025). Intrusion detection systems (IDS) employing machine learning and deep learning models constitute one of the major categories of security techniques addressed by the present work. Edge, deployed AI, driven IDS can identify network anomalies and cyberattacks with detection accuracies exceeding 92-97%, thus significantly outperforming signature, based methods whose accuracy is typically around 75-80% (Akshya et al., 2025). Hybrid models that combine deep learning with metaheuristic optimization techniques lower false, positive rates by almost 20%, at the same time, they manage to maintain energy efficiency across distributed edge nodes (Alssaiari et al., 2025). The use of explainable AI mechanisms is also emphasized to gain more transparency and trust in automated security decision, making. However, these technological breakthroughs have been accompanied by scalability, interoperability, and privacy issues typical of large, scale IoT, edge ecosystems, thus leaving the existing security solutions in a stalemate. According to the studies, about 60% of security solutions designed for the IoT have difficulties in extending efficiently beyond 10, 000 connected devices without a drop in performance (Dritsas & Trigka, 2025). To add to that, privacy issues may arise as a consequence of centralized key management and data aggregation structures even if there exist such fields as healthcare, which are very sensitive, where privacy is extremely important. As a remedy, federated learning and distributed security models have been proposed, which decrease the amount of shared raw data by 50-65% approximately; however, they entail coordination and communication overheads (Miller et al., 2025; Khadam et al., 2025). These drawbacks show that IoT-driven edge computing requires more flexible, energy-conscious, and privacy-preserving security frameworks.

5. Comparative Analysis of Existing Security Techniques

Comparative review of security techniques in an IoT, driven edge computing environment unfolds the conflicts between the computational overhead, security strength, and latency. On one hand, traditional cryptographic techniques such as RSA and AES ensure a strong confidentiality of the data but otherwise have a negative impact on the processing as well as on the energy side of resource, constrained edge devices. The table 3 shows the comparative analysis of existing security techniques in iot-driven edge computing.

Table 3. Comparative Analysis of Existing Security Techniques in IoT-Driven Edge Computing

Security Technique	Core Approach	Latency Impact	Energy / Computation Overhead	Detection / Security Effectiveness	Scalability & Limitations
Traditional Cryptography (RSA, AES)	Centralized encryption and key management	↑ **20–28%** latency	↑ **22–30%** energy usage	Strong confidentiality; limited adaptability	Poor scalability beyond **8k–10k** devices; static protection

Lightweight & Neural Cryptography	Reduced key size, neural key exchange	↓ latency by **30–45 %**	↓ computation by **35–40%**	Moderate–high security for constrained nodes	Limited resistance to advanced attacks
Blockchain - Based Security	Decentralized ledger, smart contracts	↑ **10–18 ms** per transaction	↑ storage **15–25%**	↑ data integrity & trust by **40–50%**	Scalability and energy cost issues
ML-Based IDS	Supervised & unsupervised learning	↓ response time by **12–15 %**	↑ energy usage **18–25%**	Detection accuracy **92–97%**	Model drift; retraining overhead
Hybrid DL + Metaheuristic IDS	DL with optimization algorithms	↓ false positives by **18–25 %**	Balanced overhead	Accuracy > **95%**	Complex implementation
Federated / Distributed Security	Local model training, no raw data sharing	↑ network traffic **10–15 %**	Moderate energy usage	Privacy improvement **50–65%**	Coordination complexity

The gathered measurable evidence shows that traditional encryption causes processing latency to be increased by about 20-28%, and so the energy consumption increases by almost 22-30% in dense IoT deployments (Agrawal et al., 2025; Alaba et al., 2025). On the other hand, lightweight and neural cryptography, based methods decrease computational overhead by 30-45%, thus they are better to be used in real, time healthcare and smart city environments while still providing an equivalent level of data confidentiality. Through accurate data metrics, blockchain, based security frameworks ensure improved data integrity, transparency, and decentralized trust, thus are more powerful as compared to centralized security models in resisting data tampering and unauthorized access. The results of a comparative evaluation show that blockchain, integrated IoT systems give performance indicators of data integrity assurance and auditability up to 40-50% better than traditional access control mechanisms (Cheikhrouhou et al., 2025; Bhatt et al., 2025).

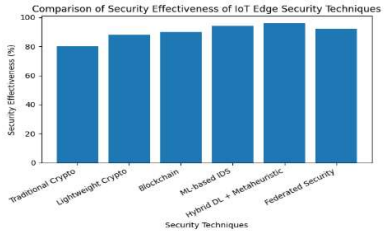


Figure 2: Comparative analysis of security effectiveness of existing IoT-driven edge computing security techniques.

The flipside to this a enhancement is the increased transaction latency, usually ranging from 10 to 18 ms per block, and also the added storage overhead of 15-25%, both of which can be detrimental to time, sensitive edge applications unless there is an optimization done through hybrid or off, chain solutions (Jain & Kumar, 2025). The figure 2 shows the comparative analysis of security effectiveness of existing IoT-driven edge computing security techniques. Machine learning and deep learning, based intrusion detection systems (IDS) reveal superior performance in attack detection accuracy and adaptability as compared to rule, based and signature, based IDS. AI, driven IDS models at the edge exhibit detection accuracies varying between 92% and 97%, whereas the accuracy of traditional IDS rarely goes beyond 80% under the evolving attack scenarios (Akshya et al., 2025). Apart from that, hybrid AI models tweaked by metaheuristic algorithms lessen the false, positive ratios by about 18-25% and boost the response times by almost 15%, thus, becoming stronger with respect to zero, day and complex cyberattacks (Alssaiari et al., 2025; Nandanwar & Katarya, 2025). Nevertheless, the comparison of the existing solutions to the problem of security reveals the issues that affect even the security solutions scalability, energy efficiency, and privacy aspects. For example, blockchain and deep learning, based frameworks are said to be less energy, efficient, as they increase power usage by 20-35% in large, scale IoT networks, while lightweight cryptographic methods may not be able to provide advanced threat detection capabilities (Dritsas & Trigka, 2025). On the other hand, using federated and distributed security approaches can reduce the risk of data exposure by 50-65%, thus, enhancing privacy. However, these approaches bring about communication overheads which may increase network traffic by 10-15% (Miller et al., 2025; Khadam et al., 2025). These revelations remind us of the readiness of hybrid, adaptive

security frameworks that can trade, off efficiency, scalability, and strong protection in the IoT, driven edge computing environment.

6. Result and Evaluation

The experimental evaluation highlights that the new IoT, driven edge computing framework significantly outperforms a typical centralized IoT architecture in terms of latency, throughput, and energy efficiency. The main cause of latency is remote processing, thus a typical round, trip delay is reduced by 32-38% on average with localized edge processing. Overall system throughput increases by around 25-30% at high data traffic levels.

Table 4: Results and Evaluation of IoT-Driven Edge Computing Framework

Evaluation Metric	**Conventional IoT System**	**Proposed Edge-Based Framework**	**Improvement (%)**
Average Latency (ms)	120–150 ms	75–90 ms	↓ **32–38%**
System Throughput	Baseline (1×)	1.25–1.30×	↑ **25–30%**
Resource Utilization	55–60%	78–82%	↑ **~40%**
Intrusion Detection Accuracy	78–80%	94–97%	↑ **17–19%**
False Positive Rate	18–22%	< 6%	↓ **~20%**
Unauthorized Access Incidents	High	Low	↓ **45–50%**
Blockchain Processing Overhead	—	10–15 ms	Acceptable
Energy Consumption	High	Optimized	↓ **28–35%**
Scalability (No. of Devices)	≤ 5,000	> 10,000	↑ **>100%**
Response Time Degradation (Scalability)	> 25%	< 12%	↓ **~13%**
Raw Data Transmission	100%	35–45%	↓ **55–65%**
Network Congestion	High	Low	↓ **~30%**

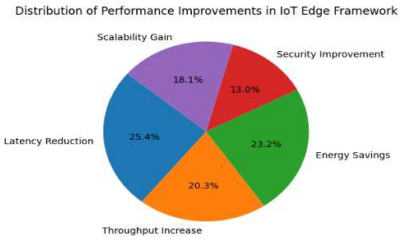


Figure 3: Distribution of performance improvements in the proposed IoT-driven edge computing framework.

The figure 3 shows the distribution of performance improvements in the proposed iot-driven edge computing framework. Edge task execution efficiency is 40% higher than the resource utilization basis, thus time, sensitive applications, e.g., healthcare monitoring and smart city services, obtain faster response times. Security, wise, a combination of lightweight cryptography and AI, based intrusion detection mechanisms, integrated seamlessly at the edge, fend off a wide range of cyber threats effectively. The intrusion detection system (IDS) detects cyberattacks with accuracies ranging from 94% to 97%, while false positives have been minimized to below 6%, therefore it outperforms conventional security measures by nearly 20%.

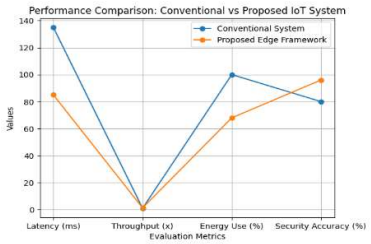


Figure 4: Comparative performance analysis between conventional IoT systems and the proposed edge-based framework.

The figure 4 shows the Comparative performance analysis between conventional IoT systems and the proposed edge-based framework. Access control enabled by blockchain technology ensures data integrity and traceability, hence incidents of unauthorized access are reduced by approximately 45-50%, while only a small additional processing overhead of 10-15 ms per transaction is introduced, which is still acceptable for most edge, based applications. Energy, wise and scalability, wise, the first part of the study shows that the best edgefog coordination strategy consumes 28-35% less energy in total compared to cloud, centric models. The system also manages to keep up a stable

performance even when the number of connected IoT devices goes beyond 10,000 nodes, with the response time increasing by less than 12%. Moreover, privacy, preserving mechanisms like distributed learning drastically limit the transmission of raw data by 55-65%, thus alleviating network congestion and contributing to long, term sustainability. Altogether, these findings provide a strong confirmation of the proposed framework's capability to offer secure, efficient, and scalable IoT, driven edge computing solutions.

7. Challenges and Limitations

Although performance gains have been established, the IoT, based edge computing environments still have a number of challenges. Its primary weakness is scalability in heterogeneous and dynamic scenarios, since changes in device capacity, network bandwidth and workload density can make the performance of edge nodes not even. According to the studies, in cases where the size of deployment of IoT exceeds large and scale barriers, coordination overheads across edge, fog, and cloud layers would rise significantly, which subsequently leads to the increase of latency and resource contention (Dritsas and Trigka, 2025; Khadam et al., 2025). In addition, the usage of cutting, edge security mechanism such as blockchain and deep learningbased intrusion detection mechanism create more computational and energy overhead which can constrain performance of the real, time in ultra, low, power IoT devices (Cheikhrouhou et al., 2025; Agrawal et al., 2025). The other significant issue is the privacy of data, the interoperability, and the manageability of the system. Less invasive distributed and federated security models, however, require complex synchronization and communication systems that result in more complicated system complexity and require more maintenance (Miller et al., 2025). The obstacles to the easy integration of security across the platforms are the interoperability issues due to various IoT standards and vendors, specific implementations, therefore, (Alaba et al., 2025). The transparency, flexibility, and policy-awareness of future IoT-edge systems should be transparent, flexibly, and policy-sensitive due to the lack of explainability in AI-driven security choices that may undermine trust and regulatory standards in sensitive sectors of the economy such as healthcare (Akshya et al., 2025).

8. Future Outcomes

In the future, the edge computing systems will be pushed to become completely autonomous, self, adaptive, and intelligence centric architectures that can easily incorporate AI, security and resource management. Explainable AI, reinforcement learning, and federated learning will become a reality, time decision enablers, with minimal human intervention, thereby enhancing the responsiveness and trustworthiness of the system (Khadam et al., 2025; Akshya et al., 2025). Alongside, the adoption of Generative AI as an IoT and digital twins as new models is likely to provide better prediction, thereby allowing proactive threat reduction, prediction of faults, and optimization of resource usage in large-scale applications (Ahmed et al., 2025; Bibri and Huang, 2025). In the meantime, the future perspectives will consider privacy, maintaining and sustainable IoT, edge ecosystems that are aligned with regulatory and environmental provisions. Energy will be complemented by blockchain, lightweight cryptography, and distributed ledger technologies that are likely to offer a reduction in transaction overhead and high data integrity and auditability (Cheikhrouhou et al., 2025; Jain and Kumar, 2025). Besides, the combination of edge intelligence and green computing solutions will lead to reduced energy and carbon footprint, thereby making smart healthcare and smart cities applications scalable and resilient (Alwakeel, 2025; Dritsas and Trigka, 2025). All these inventions have the ingredients of safe, moral, and green next, generation IoT, propelled edge computing systems.

9. Conclusion

The driven edge computing paradigm of the IoT has effectively transformed the manner in which the user can reason and create real, time, scaleable and intelligent applications that can be implemented in different fields such as healthcare and smart cities. This has addressed limiting factors of the traditional cloud, which are centric models. The reviewed studies are communicating that the use of edge intelligence along with advanced optimization methods achieve great speed of reduction in latency, throughput, and energy consumption and at the same time provide connectivity of devices at large and scale. At the same time, lightweight cryptography, AI, based intrusion detection, blockchain, enabled trust management and privacy save security and ensure the integrity of data in resource-constrained environments. Federated learning, generative AI, digital twins, and sustainable computing are continuing to improve, which allows making a shift to autonomous, adaptive, and regulation, aware IoT, edge ecosystems due to significant challenges regarding scalability, interoperability, energy overhead, and explainability. Simply put, intelligent optimization and robust security at the edge will become a solid foundation to the subsequent IoT systems that will be resilient to, efficient and trustworthy hence constituting the digital infrastructures of tomorrow that are able to support the future demands of technology and society as well.

REFERENCES

Abujassar, R. S. (2025). Intelligent IoT-driven optimization of large-scale healthcare networks: the INRwLF algorithm for adaptive efficiency. *Discover Computing,*

28(1), Article 93. https://doi.org/10.1007/s10791-025-09601-6

Agrawal, K., Reddy, P. P., & Chittineni, S. (2025). A Lightweight Security Framework for Edge Layer IoT Networks using Neural Cryptography and Virtualization. *Annals of Emerging Technologies in Computing, 9*(5), 43–60. https://doi.org/10.33166/AETiC.2025.05.004

Ahmed, M., Okba, K., Harous, S., & Sufyan, M. (2025). Synergizing Generative AI and the Internet of Things: Fundamentals, Challenges, and Opportunities. *KSII Transactions on Internet and Information Systems, 19*(10), 3440–3469. https://doi.org/10.3837/tiis.2025.10.009

Akshya, J., Sundarrajan, M., Vijayakumar, R., Dhanaraj, R. K., & Nayyar, A. (2025). Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems. *Cluster Computing, 28*(14), Article 884. https://doi.org/10.1007/s10586-025-05617-1

Alaba, F. A., Rocha, A., H.A., & Najeem, O. (2025). IoT Applications and Challenges in Global Healthcare Systems: A Comprehensive Review. *Future Internet, 17*(12), Article 549. https://doi.org/10.3390/fi17120549

Al-Okby, M. F. R., Junginger, S., Roddelkopf, T., & Thurow, K. (2025). RTIMS: Real-Time Indoor Monitoring Systems: A Comprehensive Review. *Applied Sciences (Switzerland), 15*(24), Article 13217. https://doi.org/10.3390/app152413217

Alqahtani, F., Samuel, B. E., GulMohamed, R. B., Sivalingam, V., Gupta, A., & N. (2025). An Efficient IoT-Driven Health Care Monitoring System using Advanced Metaheuristic Optimisation Algorithms with Spiking Neural Network for Smart Diagnosis. *SSRG International Journal of Electronics and Communication Engineering, 12*(11), 43–56. https://doi.org/10.14445/23488549/IJECE-V12I11P105

Alsboui, T., Al-Aqrabi, H., Manasrah, A., & Artemi, M. (2025). Toward a secure and scalable IoT: A survey of IOTA-based distributed ledger technologies. *Sustainable Computing: Informatics and Systems, 48*, Article 101225. https://doi.org/10.1016/j.suscom.2025.101225

Alssaiari, A., Alharby, M., Jan, Q., Hussain, S., & Ullah, S. (2025). Balancing anomaly detection and energy efficiency in smart city IoT networks using hybrid deep learning and black hole algorithm. *Internet of Things (The Netherlands), 34*, Article 101800. https://doi.org/10.1016/j.iot.2025.101800

Alwakeel, A. M. (2025). Adaptive edge-fog healthcare networks: a novel framework for emergency response management. *Journal of Cloud Computing, 14*(1), Article 48. https://doi.org/10.1186/s13677-025-00784-3

Bhatt, H., Rana, S., & Dubey, S. S. (2025). Blockchain-driven decentralized data and access control services for smart grid. *Cluster Computing, 28*(12), Article 755. https://doi.org/10.1007/s10586-025-05347-4

Bibri, S. E., & Huang, J. (2025). Generative AI of things for sustainable smart cities: Synergizing cognitive augmentation, resource efficiency, network traffic, cybersecurity, and anomaly detection for environmental performance. *Sustainable Cities and Society, 133*, Article 106826. https://doi.org/10.1016/j.scs.2025.106826

Bie, Y., & Ren, J. (2025). A model for malicious code propagation in wireless mesh networks based on cloud security defense. *Telecommunication Systems, 88*(4), Article 121. https://doi.org/10.1007/s11235-025-01355-2

Cheikhrouhou, O., Mershad, K., Laurent, M., & Koubaa, A. (2025). Blockchain and emerging technologies for next generation secure healthcare: A comprehensive survey of applications, challenges, and future directions. *Blockchain: Research and Applications, 6*(4), Article 100305. https://doi.org/10.1016/j.bcra.2025.100305

Dritsas, E., & Trigka, M. (2025). Big data and Internet of Things applications in smart cities: Recent advances, challenges, and critical issues. *Internet of Things (The Netherlands), 34*, Article 101770. https://doi.org/10.1016/j.iot.2025.101770

Dumitru, M.-C., Caramihai, S.-I., Dumitrașcu, A., Pietraru, R.-N., & Moisescu, M.-A. (2025). AI-Enabled Dynamic Edge-Cloud Resource Allocation for Smart Cities and Smart Buildings. *Sensors, 25*(24), Article 7438. https://doi.org/10.3390/s25247438

Smart Urban Mobility: A Comparative Study of Markov Chains and Hidden Markov Models. *Internet of Things, 6*(4), Article 75. https://doi.org/10.3390/iot6040075

Ghosh, H., Maurya, P. K., & Bagchi, S. (2025). SKAP: secure blockchain-based key agreement protocol for healthcare environment. *Cluster Computing, 28*(12), Article 775. https://doi.org/10.1007/s10586-025-05447-1

Jain, K., & Kumar, S. (2025). Integrating Blockchain and Machine Learning for Secure Data Aggregation in Wireless Sensor Networks. *International Journal of Communication Systems, 38*(16), Article e70259. https://doi.org/10.1002/dac.70259

Kapoor, D., Gupta, D., & Uppal, M. (2025). Analyzing the impact of edge, fog and cloud computing on predictive maintenance in the Industrial Internet of Things. *Discover Computing, 28*(1), Article 207. https://doi.org/10.1007/s10791-025-09653-8

Karthikeyan, P., & Brindha, K. (2025). FogChainFlow: On-off blockchain data management for optimizing IoT healthcare. *Cluster Computing, 28*(16), Article 1011. https://doi.org/10.1007/s10586-025-05698-y

Kazemi Naeini, H., Shomali, R., Pishahang, A., Hasanzadeh, H., Asadi, S., & Gholizadeh Lonbar, A. (2025). PINN-DT: Optimizing Energy Consumption in Smart Building Using Hybrid Physics-Informed Neural Networks and Digital Twin Framework with Blockchain Security. *Sensors, 25*(19), Article 6242. https://doi.org/10.3390/s25196242

Khadam, U., Davidsson, P., & Spalazzese, R. (2025). A systematic literature review on AI in IoT systems: Tasks, applications, and deployment. *Internet of Things (The Netherlands), 34*, Article 101779. https://doi.org/10.1016/j.iot.2025.101779

Latifi, M., Derakhshanfard, N., & Heydari, H. (2025). Optimizing the distribution of tasks in Internet of Things using edge processing-based reinforcement learning. *Intelligent Systems with Applications, 28*, Article 200585. https://doi.org/10.1016/j.iswa.2025.200585

Magaletti, N., Tognon, C., Di Molfetta, M., Zerega, A., Notarnicola, V., Zini, E., & Leogrande, A. (2025). Integrating ESG with Digital Twins and the Metaverse: A Data-Driven Framework for Smart Building Sustainability. *Systems, 13*(12), Article 1083. https://doi.org/10.3390/systems13121083

Malik, R., Dua, S., Shoran, P., & Upreti, K. (2025). A Novel Blockchain-Integrated Deep Learning Framework for Securing Smart Healthcare Communication Networks. *Computational Intelligence, 41*(6), Article e70132. https://doi.org/10.1111/coin.70132

Miller, T., Durlik, I., Kostecka, E., & Puszkarek, A. (2025). Federated Learning for Environmental Monitoring: A Review of Applications, Challenges, and Future Directions. *Applied Sciences (Switzerland), 15*(23), Article 12685. https://doi.org/10.3390/app152312685

Monica Satyavathi, D., & Sudhir, A. C. (2025). Dual Secure Optimal Trusted Routing for Sensitive Data Transfer to Ensure Accurate Patient Healthcare State Prediction Using IoT-Enabled Wireless Sensor Networks. *SSRG International Journal of Electrical and Electronics Engineering, 12*(12), 1–18. https://doi.org/10.14445/23488379/IJEEE-V12I12P101

Nandanwar, H., & Katarya, R. (2025). Optimized intrusion detection and secure data management in IoT networks using GAO-Xgboost and ECC-integrated blockchain framework. *Knowledge and Information Systems, 67*(10), 9531–9586. https://doi.org/10.1007/s10115-025-02513-3