JT CT
Journal of Telecommunication and Computer Technology
Vol. 1 | Issue 1 | 2026

A Review of Secure and Efficient Data Transmission in IoT Systems: Advances and Open Research Challenges

Mohammed Khudhair Abbas [1], Israa Mohammed Ahmed [2]

[1] College of Engineering, University of Information Technology and Communications (UOITC), Iraq
[2] College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq

ABSTRACT

The prompt reproduction of the Internet-of-Things (IoT) is used to convert communication networks by connecting billions of diverse devices, ranging from wearable sensors to made-up models. Ensuring the security and efficiency of data transmission in IoT communication networks poses a crucial challenge due to resource constraints, dynamic topologies, and diverse communication protocols. This review paper introduces a methodological analysis of state-of-the-art methods of secure IoT systems in communication networks, consisting of cryptography, approaches based on blockchain, and systems-based intrusion detection. This review paper is also used to examine some strategies for improving data efficiency, like edge computing, data aggregation, and AI-assisted routing protocols. Through estimating current solutions and summarizing such limitations, this review paper aims to differentiate research gaps. This review paper provides a powerful roadmap for researchers and practitioners seeking to build and design strong IoT systems able to support the shining future for the design of smart cities, healthcare systems, and commercial automation as well.

Keywords: *IoT security, data transmission efficiency, lightweight cryptography, blockchain IoT, AI-assisted routing.*

1. Introduction

The Internet of Things (IoT) has appeared as the most transformative criterion of the present-day digital community. Through interconnecting billions of diversified devices from wearable monitoring healthiness and home devices to vehicle-based autonomous

*** Corresponding Author: mohammed.abbas@uoitc.edu.iq**

and commercial sensors, IoT has redefined how the information is produced, conveyed, and used [1, 2]. Such devices sense, gather, and interchange information via spread communication networks, allowing a vast spectrum of smart usage in fields like healthcare, transmission, energy handling, agriculture, and commercial automation. Modern studies prophesy that the comprehensive number of linked IoT-devices will exceed 30 billion in the following years, generating data-based zettabytes which have to be transmitted efficiently, processed, and dealt with security [3, 4].

Both the dynamicity and the heterogeneity of IoT systems complicate the security tasks of data communication. IoT systems consist of many layers: the first layer is perception, including sensors, actuators, and RFID tags; the second layer is the network, including routing protocols in addition to communication protocols; and the third layer is application, including the end user services [5, 6]. Such layers present distinctive vulnerabilities. For instance, in the first layer, devices have been physically opened, making it critical to manipulate or reproduce them. The second layer, insecure due to the routing protocols, might allow selective forwarding or a sinkhole attack. Third layer, low authentication and low control access ease forbidden data-access and confidentiality infringements [7, 8].

Equally significant is the efficiency property of data communications. IoT-based devices generate a huge amount of redundant data, frequently informing interlock calculations from careful deployment [9]. With no efficient ingathering and compression mechanisms, such redundancy leads to too much energy exhaustion, congestion, and shortened device lifespan. Almost all IoT devices are battery-powered and hard to recharge following deployment, reducing energy spending through data transmission is crucial for combating network ageing. Besides, numerous applications based on IoT systems, like commercial monitoring, need close-by real-time transference, while delays due to ineffective routing or intensive cryptographic calculations may undermine both the reliability and the usability of such systems [10]. Consequently, modeling data communication protocols that achieve equilibrium, guaranteeing security-based efficiency restrictions, is expressed as the main challenge in IoT studies [11].

To handle such challenges, many hopeful directions have emerged in context. Cryptography remains the basis of IoT data security. Nevertheless, traditional cryptographic approaches like RSA and AES are computationally intensive for resource-limited IoT devices [12, 13]. Institutional cryptographic systems—mainly elliptic curve cryptography (ECC), uniform key encryption, and encryption features are explored for performing confidentiality and authentication in the absence of exhausting device resources [14, 15]. Almost all studies also combined steganographic strategies, used to embed encrypted

information in an image and/or video for hiding the communication from threats, thereby adding a further layer of defense. Whilst such strategies importantly support IoT security [16, 17].

At the same time, intrusion detection systems (IDSs) are gaining importance as the final solutions related to IoT security. Whilst both cryptography and blockchain primarily aim to deny unauthorized access, IDSs have been built for making detection for abnormal behavior once it occurs [18, 19]. Conventional IDSs are designed for maximum capacity servers. As a result, studies are focused on Network Intrusion Detection Systems (NIDSs), which hold machine learning (ML) and deep learning (DL) technologies for traffic analysis, identifying peculiarities, and classifying malicious activities [20, 21].

All of these technologies are converging—light encryption, blockchain, and machine learning-driven intrusion detection—a multifaceted effort to make IoT communications secure. Despite all this, the field continues to evolve. Many questions remain regarding interoperability based on protocols, scalability to include a vast number of IoT devices, and the integration of energy efficiency with security [22 – 24]. Therefore, it has become necessary to strike a balance between three fundamental goals: (1) ensuring security and privacy, (2) improving energy and communication efficiency, and (3) enabling scalability and interoperability across diverse environments.

Figure 1 presents the main structure of a secure and efficient data transmission-based IoT system. Such a figure shows the main interaction among the layers of Perception, Network, and Application, whereas all such layers play a distinct role in confirming data confidentiality, data integrity, and data reliability in transmission. In the perception layer, main sensors and actuators catch the physical information, which is transmitted securely via the network layer utilizing cryptography-based lightweight, verification-based blockchain, and mechanisms-based intrusion detection. Thus, the application layer is in charge of services-based user-level and analytics for emphasizing data usage with minimum latency and minimum consumption of energy. Such a diagram illustrates how combining security and efficiency in each stage shapes the backbone of a strong IoT system.

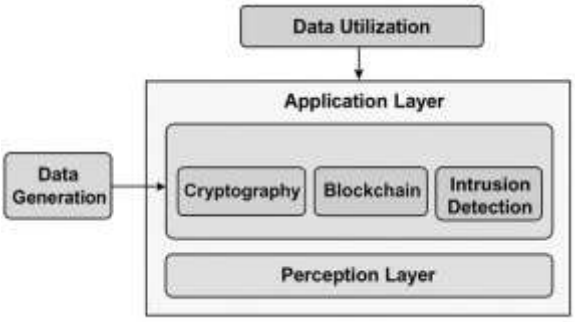

Figure 1: Secure and efficient data transmission diagram in IoT systems.

The expeditious adoption of IoT in crucial fields like healthcare, manufacturing, and intelligent cities is used to make high-security and efficiency-based data transmission a critical concern. Exposed devices can be exploited for large-scale threats, whilst resource restrictions deny the utilization of weighty security protocols. Consequently, researchers have been motivated to develop strategies that use to integrate robust protection-based lightweight functioning, stabilize security, and energy for efficient communication.

This review paper offers a systematic and comparative analysis of IoT data transmission approaches based on security and efficiency. Different from presenting surveys, this review combines several technologies consisting of cryptography, blockchain, intrusion detection systems, edge computing, and AI based on routing into a unified perspective. This review paper contributes to integrating security and efficiency techniques, comparative evaluation over several approaches, identifying challenges for combining over IoT layers, and provides future research roadmap directions.

The rest of this review article is organized as follows: Section 2 introduces the main review of challenging security approaches based on data transmission-based IoT. Section 3 presents efficiency-oriented methods, consisting of edge computing, data combination, and AI-assisted routing approaches. Section 4 demonstrates open challenges and research gaps which are used to persist despite the advancements. Finally, section 5 provides comprehensive conclusions of the review article via highlighting key findings and summarizing potential directions for future work.

2. Research Methodology

This review paper follows a structured methodology to guarantee both transparency and reproducibility. A systematic search was conducted over the main scientific databases, consisting of IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. The exploration focused on studies associated with IoT security and efficiency-based data transmission. The chosen process applied predefined implication and exception criteria. Only peer-reviewed papers published between 2016 and 2025 have been considered. Studies are needed for handling

at least one of the following: cryptography, blockchain, intrusion detection, edge computing, or AI routing-based IoT. A total of 54 papers were initially specified, out of which 30 papers have been finally selected subsequent to related titles, abstracts, and full methodological texts. See Table 1.

Table 1: Research Methodology.

Criteria Type	Description
Inclusion Criteria	IoT security, efficiency, peer-reviewed, English language
Exclusion Criteria	Duplicates, non-IoT studies, non-peer-reviewed
Databases Used	IEEE, Springer, ScienceDirect, Google Scholar
Time Range	2016–2025
Final Papers	30 papers

Figure 2 illustrates a structured process utilized for identifying, screening, and selecting associated studies for this review paper. It demonstrated the sequential steps from selecting a database and exploring a strategy to the final inclusion of the paper and comparative analysis.

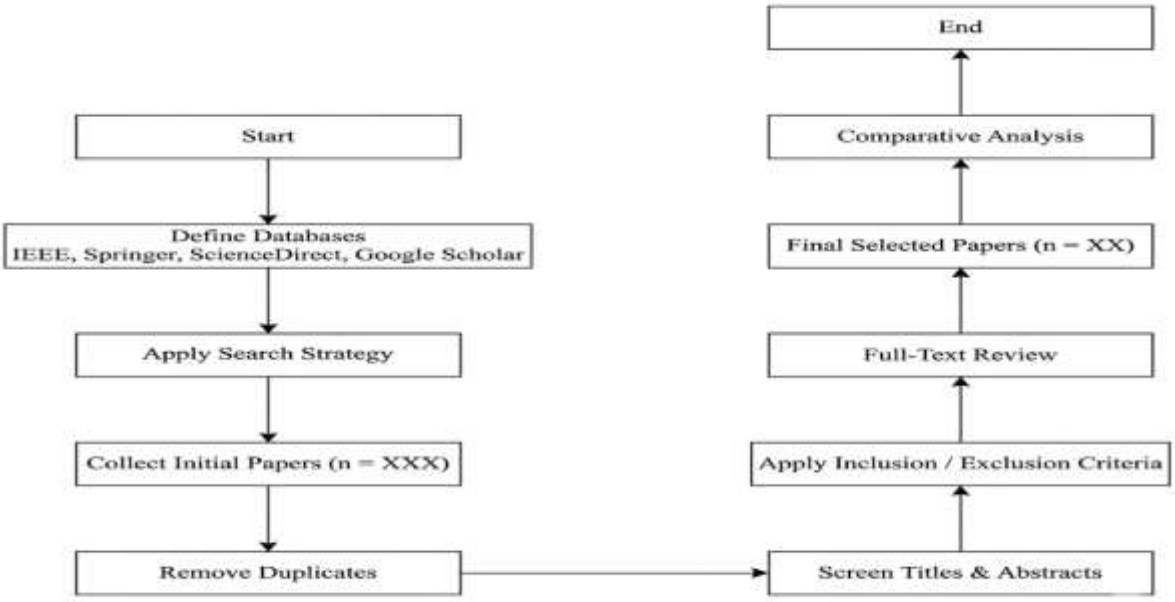

Figure 2. Systematic review flowchart for paper selection and analysis

3. Challenging Security Technologies for Data Transmission in IoT Systems

3.1. Cryptography-Based IoT Systems

Daniels et al. suggested the Security MicroVisor (SμV), an approach which utilized as a bridge between an operating system that isolates memory and verifies code execution to enhance IoT device security. Such an approach enhanced protection-based device-level whilst presented scalability and resource over related respects [25]. Banerjee et al. modelled a protocol-based, energy-efficient Datagram Transport Layer Security (eeDTLS) for IoT, which minimized energy consumption while conserving secure and reliable communication [26]. Nevertheless, such an approach faced restrictions in terms of flexibility when it was applied to various IoT conditions.

Manogaran et al. built an IoT-enabled healthcare framework based on medical sensors in addition to secure data communication, consisting of reliable and tolerant monitoring on a large scale [27]. Further, such a framework has a vulnerability and congestion when treating huge datasets. Sun et al. presented Cloud Eyes, which was used to encrypt traffic for IoT communication security [28]. However, practical in detection, which relies on dependent cloud connectivity, increases latency. Eventually, Khari et al. integrated Elliptic Galois Cryptography and Matrix XOR steganography, implanting medical IoT data with an image for robust confidentiality [29]. In spite of such robust protection, such a hybrid system suffers from computational complexity and notable image size. Table 2 summarizes the comprehensive comparison of all the mentioned studies.

Table 2: Cryptography-Based IoT Security Studies

Study	Method	Challenges	Issues
[25]	Security microvisor (SμV) middleware with code verification	Provides memory isolation and custom IoT security	Overhead and scalability limitations
[26]	Energy-efficient Datagram Transport Layer Security (eeDTLS)	Reduces energy cost while maintaining TLS-level security	Limited flexibility in diverse IoT networks
[27]	Body-embedded medical sensors with vital management security	Protects large-scale health data transmissions	Vulnerable to privacy leaks and network congestion
[28]	CloudEyes cloud-based anti-malware service.	Provides trusted IoT malware detection	Dependence on cloud connectivity and latency
[29]	Elliptic Galois Cryptography + Matrix XOR steganography with	Encrypts medical IoT data and hides it in images	Computational complexity and

Adaptive optimization	Firefly	image-size overhead

3.1. Blockchain-Based IoT Systems

Many studies have presented IoT systems based on blockchain and addressed some previous issues, such as reliability and complexity, but there are still some restrictions in context. Ahmed et al. suggested an Energy-Efficient Data Aggregation Mechanism (EEDAM) combined with blockchain for ensuring security and energy properties in IoT data communications [30]. Xu et al. demonstrate transparent tamper-proof traceability data based on high availability, and allow an automated regulatory-compliance checking and adaptation in scenario-based product traceability [31]. They illustrate an analysis-based qualitative and quantitative analysis of the software architecture of originChain. Though such a model faced challenges in managing a huge number of intelligent compact. Novo et al. introduced an IoT-based architecture for scalable entry management, which used blockchain for decentralized authentication [32]. However, such a method used to avoid central authorities, it requires a compound in cloud communication, network edge, and fog layers covering. Dorri et al. surveyed blockchain as a good solution in IoT trust systems and privacy metrics, illustrating that the decentralized ledgers are capable of combating manipulation [33]. However, such an approach forced complex computational costs in resource-restricted devices in IoT data transmission.

Götzinger et al. offer the Research on Self-Awareness (RoSA) system and its design principles. They utilized self-aware functionalities abstraction, data reliability, and confidence, which are currently given by RoSA, and are presented. Possible use cases of RoSA were also discussed [34]. Such research is promising that RoSA can serve as a common approach for self-aware frameworks and applications, and thus assists in exploring the vast design space of hierarchical agent-based systems with computational self-awareness. Whilst promising, ROSA is built for commercial circumstances, restricting such common applicability. Thus, Jiang et al. combined federated learning and blockchain for conserving privacy on IoT data participation [35]. Even with improved data privacy, such schemes suffer from high communication overhead. Eventually, Liu et al. suggested a lightweight blockchain intended for resource-constrained purposes of IoT conditions [36]. Even though such a model handled ledger scalability, some challenges persist in the steady state lightweight process and long-term model flexibility. Table 3 highlights the complete comparison of the above literature works.

Table 3: Blockchain-Based IoT Security Studies

Study	Method	Challenges	Issues
[30]	Energy-Efficient Data Aggregation Mechanism (EEDAM) with blockchain	Reduces redundancy and ensures secure aggregation	High complexity in clustering and scheduling
[31]	Blockchain-based smart contracts for medical data	Secure remote patient monitoring	Smart contract scalability
[32]	Blockchain with cloud, edge, and fog integration	Reduces centralization and latency	Synchronization and orchestration difficulties
[33]	Blockchain + smart contracts for IoT privacy	Strong authentication and privacy	Computational overhead for constrained devices
[34]	Route Optimization and Service Assurance (ROSA)	Low-latency IIoT communication	Limited to industrial scenarios
[35]	Edge-assisted federated learning with blockchain	Privacy and resource allocation	High communication overhead
[36]	Lightweight blockchain (LightBlock) for IoT	Resource-constrained IoT security	Blockchain ledger scalability

3.2. Intrusion-Detection for IoT Systems

Latif et al. applied a 6LoWPAN for IDS, which monitors IoT networks at low-power restrictions [37]. Although beneficial for certain attack protocols, its applicability is limited to 6LoWPAN scenarios. Thus, A. L. Buczak and E. Guven considered machine learning and data mining techniques in intrusion detection as a foundation for implementing analytics-based IoT privacy [38]. Therewith, such work underlined biases in utilized datasets in addition to the ML system complexity. In the same context, Fadlullah et al. modelled a deep learning based on IDS's ability to identify abnormality in IoT communication traffic through high accuracy [39].

Even with its performance, such a work requires considerable resources that are not always available at the same time in IoT apparatus. Therefore, Hodo et al. used a comparison of shallow and DNN technologies for detecting both the botnets and the malware in the IoT communication network system [40]. Their key findings offered enhanced detection, however, advanced attention on scalability in real-time deployment. That's what aids Zarpelão et al. to create a taxonomy of IDS in IoT data transmission, classify intrusion detection methods depending on their positioning and methodology [41].

Even so, such a survey requires confirmation on the machine learning combination. Ultimately, Pundir et al. supply a review of intrusion detection in IoT frameworks, summarizing challenges and standpoints for future exploration [42]. However thorough, such a study would be without actual validation, having gaps in real-time applicability. Table 4 highlights the comprehensive comparison of the literature works related to intrusion detection for IoT systems.

Table 4: Intrusion-Detection for IoT Security Studies.

Study	Method	Challenges	Issues
[37]	6LoWPAN-based IDS	Low-power IoT intrusion monitoring	Limited to a specific protocol (6LoWPAN)
[38]	Machine learning and data mining for IDS	Cyber analytics in IoT intrusion detection	Dataset bias and complexity
[39]	Deep learning IDS for IoT traffic	Improves anomaly detection accuracy	High computational demand
[40]	Shallow vs. deep neural IDS for IoT	Detects IoT botnets and malware	Scalability and deployment constraints
[41]	Taxonomy of IoT-specific IDS	Classifies IDS placement/detection methods	Lacks ML integration
[42]	IDS survey for IoT	Reviews intrusion detection in IoT architectures	Limited practical validation

4. New Trends in Data Transmission in IoT Systems

Figure 3 illustrates the expanded architecture in Figure 1, combining the new trends in secure IoT data transmission. In addition to the basis layers, this figure presents Edge Evaluation, Data Combination, and AI-Assisted Routing Protocols as derived improvements. Edge evaluation authorizes real-time processing of close-by data sources, importantly minimizing latency and congestion in the network.

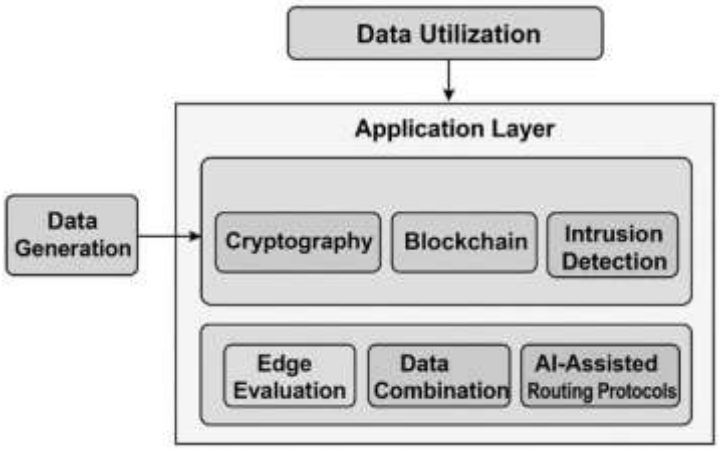

Figure 3. New trends in data transmission in IoT systems

The data aggregation (combination) enhances the efficiency of bandwidth and consumption of energy through decreasing redundant transmissions, at the same time as AI-assisted routing protocols give an adaptation, a smart communication root which used to optimize performance over dynamic IoT environments. As a result, such improvements express a shift toward more intelligent, context-aware, and efficient resource IoT systems. The main addition of these new trends confirms improved scalability, energy, and security, which make such a design a forward-looking diagram for next-generation IoT systems. These additions are detailed defined in the next sub-sections.

4.1. Edge Evaluation

Carvalho et al. studied the basic functions of edge calculation in IoT via classifying distinct frameworks like Fog, MEC, Cloudlet, and cloud computing of mobile communication systems, confirming the crucial demand for addressing scalability property, security scheme, and challenges of low-latency [43]. Based on such a study, da Silva et al. demonstrate a mechanism based on adaptive autoscaling that utilizes online machine learning for dynamically allocating resources on the edge, thereby qualifying the scalability restrictions specified in the Carvalho et al. study [44]. Enhancing such work, Agrawal et al. present a load-balancing and access-control approach dynamically, which harmonizes resource allocation between both the edge and the layers of fog for improving throughput property and data exchange security, illustrating how such an arrangement is able to enhance performance and confidentiality in IoT systems [45]. Lastly, Adhikari et al. suggest a machine learning-based, lightweight framework, such as Random Forest, on nodes of the edge for reducing upstream traffic and improving privacy during local analytics, thereby addressing both latency and security concerns previously [46]. As a whole, such studies emphasize how edge evaluation takes action as a crucial possibility of security and efficiency in IoT data transmission. Table 5 highlights the comprehensive comparison of the literature works related to intrusion detection for IoT systems.

Table 5: Comparison studies of edge evaluation for an IoT data transmission system

Study	Method	Key contribution	Limitation
[43]	Comprehensive taxonomy + qualitative comparison of	Clear taxonomy of MEC/Fog/Cloudlet, use-case mapping, open issues	Broad survey — limited experimental/quantitative evaluation.

	EC architectures	(scalability, privacy, low latency).	
[44]	Online ML for autoscaling edge resources	Practical autoscaling reduces latency and adapts to the workload at the edge.	Needs extensive training data; may be sensitive to concept drift.
[45]	Dynamic load balancing + optimized access control	Coordinated edge–fog–cloud placement improves throughput and access security.	Complexity of orchestration; overhead in control signaling.
[46]	Lightweight ML (Random Forest) on edge nodes	Demonstrates accurate local analytics and reduced upstream traffic.	Model update/model distribution costs; dataset heterogeneity challenge.

4.2. Data Combination

Abbasian Dehkordi et al. contribute a thorough taxonomy of data combination approaches, illustrating how integrating data at distinct layers in IoT systems minimizes consumption of energy and conveyance overhead, even with definite integrity and security [47]. W. Feng et al. expand such an idea by suggesting integration of the hierarchical assembling and network approaches, which removes redundant data and lengthens the lifetime of the network. [48]. Then, Naeem et al. present an SDN approach, where local integration and compression make the aggregation further programmability and adaptivity, bridging conventional clustering approaches beyond-generation software specified in communication networks [49]. To complement such methods, Ahmadvand et al. highlight the security and robustness concerns related to localized aggregation [50]. As a result, such contributions demonstrate that data combination works as a basis to enhance the efficiency of transmission in time, challenging accurate integration of protection-based security and privacy as well, a spectacle of complete alignment with the visualization of this proposed review paper for supporting the robustness property of IoT data transmission in a crucial estate. Table 6 summarizes all the related studies with the key comparison related to data combination for IoT systems.

Table 6: Comparison studies of data combination for an IoT data transmission system.

Study	Method	Key contribution	Limitation

[47]	Taxonomy of aggregation techniques across WSN domains	Systatic classification; discussion of applicability per scenario (terrestrial, underground, underwater, body) and energy/latency tradeoffs.	Survey-level: limited new algorithms; practical security solutions are not the primary focus.
[48]	In-network hierarchical aggregation	Reduces redundancy and uplink traffic; improves lifetime.	Vulnerable to aggregator failure; potential data distortion.
[49]	Gateway compression + SDN control	Shows how SDN can orchestrate where/when to combine data to optimize throughput.	Requires programmable infrastructure; controller overhead.
[50]	Data fusion with privacy/robustness discussion	Highlights privacy/robustness tradeoffs of aggregation and the need for secure aggregation.	Centralized aggregation risks (privacy/leak, single point of failure).

4.3. AI-Assisted Routing Protocols

Haseeb et al. illustrate how combining genetic methods-based authentication with inspection algorithms improves the efficiency of routing and the security functionality in IoT-based mobile communication networks, showing that the AI is able to optimize the communication networks' performance [51]. Qaffas et al. made more advances in such a trend by utilizing Vision Transformer and Temporal Convolutional Networks on the edge computation for managing traffic in an intelligent city, proving how the AI distribution is able to decrease central communication with minimizing latency [52]. Etengu et al. suggest a deep supplementing learning approach for efficient energy routing in integrating SDN with OSPF circumstances, displaying AI’s adaptation to topologies dynamically while constraining the resource networks [53]. Eventually, modern works of integrating RL with DQN extend such perception through introducing adaptive policies of routing effective of energy trade-off, latency, and reliability [54]. As a result, such studies expose that routing-based AI is an influential technique for performing secure, smart, efficient data communication, supporting such a trend discussed in this proposed review paper, positioning AI as a guide to the following generation in IoT systems. Table 7 demonstrates the key comparison between related studies in AI-assisted routing protocols for IoT systems.

Table 7: Comparison studies of **AI-assisted routing protocols** of an IoT data transmission system

Study	Method	Key contribution	Limitation
[51]	Genetic algorithm + gateway authentication + network audit	Demonstrates energy & throughput gains and integrated security auditing for mobile sensors.	Mobility and dynamic topology handling are still limited; gateway centralization overhead.
[52]	ViT + TCN hybrid models deployed at edge nodes	Hybrid vision & temporal models at the edge reduce central communication and latency for traffic control.	Model size and compute demands at the edge; dataset bias and privacy concerns.
[53]	Deep RL framework for energy-efficient routing/load balancing	Shows DRL can adapt routing under energy/QoS tradeoffs in SDN-enabled networks.	Requires large training episodes and online exploration risk in live networks.
[54]	DQN / policy gradient routing policies	Good at balancing conflicting objectives (energy, delay); enables adaptive routing.	Sample inefficiency, reward engineering, and safety during learning.

5. Open Challenges and Research Gaps

Even with the progress of security and efficiency in IoT systems, many open challenges continue to exist. Firstly, scalability and interoperability continue as a basis restriction across diverse IoT devices and various platforms that try to communicate in a secure manner over limited bandwidth. Secondly, cryptography-based lightweight and blockchain combination needs modern trade-offs among network evaluation, time latency, and storage, mostly in edge circumstances. Thirdly, dynamic management-based confidentiality in the decentralized environment and mobile IoT conditions continues to be underexplored, as current IDS and solutions-based blockchain have no ability to adapt quickly to advanced attacks. Besides, AI-assisted routing approaches issue a trade-off in energy–accuracy, while deep approaches maximize security and prediction precision while elevating computation and power utilization.

Figure 4 shows the comparison research progress under five main challenges: security, efficiency, scalability, interoperability, and intelligence. As important advances are being made in security and efficiency, such a figure shows that the scalability and interoperability continue to be smaller and remain crucial barriers for the general IoT system. The demand for a robust approach which is used to combines smart algorithms, encryption-based lightweight, and interoperable criteria for performing complete system flexibility. It mainly carries the case of driven AI and solutions-based edge

computation are crucial to bridge the main research gaps and emerging IoT communication across further independent and secure patterns.

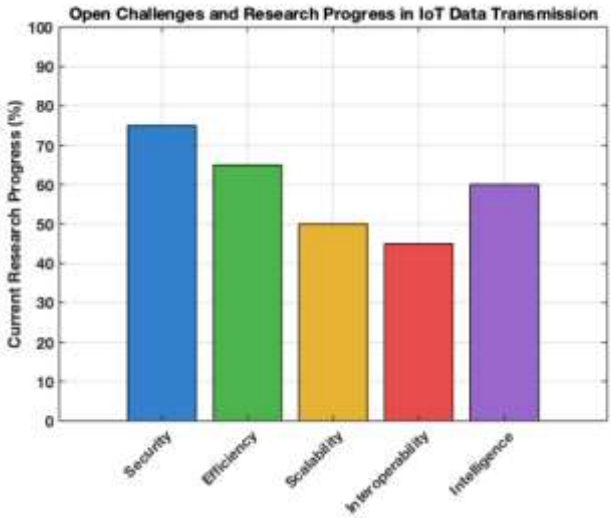

Figure 4: Open challenges and research progress in IoT data transmission.

The reviewed approaches have not been treated independently. An architecture-based unified IoT combines cryptography within data protection, blockchain-based confident management, threat detection-based IDS, low latency correlated to edge computing, and AI-based intelligent routing, as shown in Table 8.

Table 8: Integrated IoT Security Architecture

Layer	Technology	Role
Perception	Lightweight Cryptography	Data protection
Network	Blockchain + IDS	Trust + intrusion detection
Edge	Edge Computing	Low-latency processing
Application	AI Routing	Optimization

This integration enhances scalability, efficiency, and security simultaneously, handling fragmentation in current studies.

6. Conclusions

The expeditious propagation of IoT systems is basically transforming new communication networks, presenting opportunities and risks for data transmission. This review paper is used to analyze the main trends in security and efficiency of IoT communication systems, including cryptography-based lightweight, blockchain-based, and intrusion detection-based AI-driven techniques. Moreover, deriving patterns like edge evaluation, data combination, and AI-assisted routing has illustrated the possibility for enabling smart, adaptive, and scalable IoT systems. However, many research questions remain open. This review paper, for that reason, confirms that the road to the synergistic

interchange of security, smart, and efficiency, lays the path for the next generation of tough IoT systems. As future work, it has to emphasize combining efficient energy consumption-based security with diverse environments and devices of IoT systems, proving integrated interoperability protocols, and advancing self-learning adaptation embedding in security layers which integrate blockchain, edge-intelligence, and AI. In addition, IoT-based real-world approaches require evaluating the balance of security and efficiency across dynamically changing implementation environments. While IoT systems are progressing, moving toward 6G and an AI-standalone framework, future research directions have to strive for performing autonomous, security property, and context-based communication approaches that are able to self-based optimization, self-based healing, and confirming data integrity in real-time conditions. Key insights of this review paper include: security and energy efficiency trade-offs, scalability is still a main restriction, and integration over IoT layers remains immature. As a future research direction, it should focus on hybrid approaches integrating AI, blockchain, and edge computing, deployment based on performance evaluation in the real world, and standardized frameworks for interoperability.

Declaration of Competing Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Funding Information

No funding was received from any financial organization to conduct this research.

Author Contributions

Mohammed Khudhair Abbas: Experimental and simulation work, Investigation, Data collecting, Writing – review and editing, Test and correct the manuscript, supervision, Writing – review and editing. Israa Mohammed Ahmed: Writing – review and editing, Test and correct the manuscript.

Acknowledgments

The authors gratefully acknowledge the Department of Mobile Communications and Computing Engineering, College of Engineering, University of Information Technology and Communications, Baghdad, Iraq, and the College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq, for their academic leadership and institutional support throughout this work. Heartfelt thanks also go to colleagues and all the laboratory staff for their positive response and scientific support through the probabilistic–numerical framework model.

References

[1] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586
[2] E. J. Omol, "Organizational digital transformation: From evolution to future trends," *Digital Transformation and Society*, vol. 3, no. 3, pp. 240–256, 2024, doi: 10.1108/DTS-08-2023-0061.
[3] S. Ayyalasomayajula, "The dawn of big data: Origins and early promise of big data," in *AI and the Revival of Big Data*. IGI Global Scientific Publishing, 2025, pp. 1–22, doi: 10.4018/979-8-3693-8472-5.ch001.
[4] A. R. Santhi and P. Muthuswamy, "Industry 5.0 or industry 4.0 S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies," *Int. J. Interact. Des. Manuf.*, vol. 17, no. 2, pp. 947–979, 2023, doi: 10.1007/s12008-023-01217-8.
[5] K. Soni, M. Malik, D. Raval, U. Patel, and A. Patel, "An intelligent green controller for dynamic resource provisioning in heterogeneous cloud-edge IoT systems," 2026, doi: 10.21203/rs. 3. rs-8450394/v1.
[6] F. A. Alaba, "IoT architecture layers," in *Internet of Things: A Case Study in Africa*. Cham: Springer Nature Switzerland, 2024, pp. 65–85, doi: 10.1007/978-3-031-67984-1_4.
[7] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of Things: A general overview between architectures, protocols and applications," *Information*, vol. 12, no. 2, p. 87, 2021, doi: 10.3390/info12020087.
[8] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends," *Wireless Commun. Mobile Comput.*, 2018, Art. no. 5349894, doi: 10.1155/2018/5349894.
[9] U. Uyoata, J. Mwangama, and R. Adeogun, "Relaying in the Internet of Things (IoT): A survey," *IEEE Access*, vol. 9, pp. 132675–132704, 2021, doi: 10.1109/ACCESS.2021.3112940.
[10] B. Rana, Y. Singh, and P. K. Singh, "A systematic survey on Internet of Things: Energy efficiency and interoperability perspective," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 8, p. 4166, 2021, doi: 10.1002/ett.4166.
[11] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, "A cross-layer secure and energy-efficient framework for the internet of things: A comprehensive survey," *Sensors*, vol. 24, no. 22, p. 7209, 2024, doi: 10.3390/s24227209.
[12] D. Weng, "Performance and energy evaluation of lightweight cryptography for small IoT devices," in *Proc. IEEE UEMCON*, 2023, pp. 289–295, doi: 10.1109/UEMCON59035.2023.10316062.
[13] R. David and P. Deepalakshmi, "Internet of Things (IoT) devices encryption approaches: Enabling secure communication possible in low-resource settings," in *Proc. GINOTECH*, 2025, pp. 1–6, doi: 10.1109/GINOTECH63460.2025.11076617.
[14] A. E. Adeniyi, R. G. Jimoh, and J. Awotunde, "A review on elliptic curve cryptography algorithm for Internet of Things: Categorization,

application areas, and security," 2024, doi: 10.1016/j.compeleceng.2024.109330.
[15] S. Ullah, R. Z. Radzi, T. M. Yazdani, A. Alshehri, and I. Khan, "Types of lightweight cryptographies in current developments for resource-constrained machine-type communication devices: Challenges and opportunities," *IEEE Access*, vol. 10, pp. 35589–35604, 2022, doi: 10.1109/ACCESS.2022.3160000.
[16] Gurjot Singh Gaba, Gulshan Kumar, Tai-Hoon Kim, Himanshu Monga, Pardeep Kumar, "Secure Device-to-Device Communications for 5G enabled Internet of Things applications," in Computer Communications (Elsevier), vol. 169, pp. 114 – 128, March 2021. doi: 10.1016 /j.comcom.com com.2021.01.010
[17] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," *Symmetry*, vol. 15, no. 1, p. 152, 2023, doi: 10.3390/sym15010152.
[18] A. Heidari and M. A. J. Jamali, "Internet of Things intrusion detection systems: A comprehensive review and future directions," *Cluster Comput.*, vol. 26, no. 6, pp. 3753–3780, 2023, doi: 10.1007/s10586-022-03776-z.
[19] K. Vaigandla, N. Azmi, and R. Karne, "Investigation on intrusion detection systems (IDSs) in IoT," *Int. J. Emerg. Trends Eng. Res.*, vol. 10, no. 3, 2022, doi: 10.30534/ijeter/2022/041032022.
[20] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, p. 4150, 2021, doi: 10.1002/ett.4150.
[21] Z. Mustafa, R. Amin, H. Aldabbas, and N. Ahmed, "Intrusion detection systems for software-defined networks: A comprehensive study on machine learning-based techniques," *Cluster Comput.*, vol. 27, no. 7, pp. 9635–9661, 2024, doi: 10.1007/s10586-024-04430-6.
[22] A. Alfahaid, E. Alalwany, A. M. Almars, F. Alharbi, E. Atlam, and I. Mahgoub, "Machine learning-based security solutions for IoT networks: A comprehensive survey," *Sensors*, vol. 25, no. 113341, 2025, doi: 10.3390/s25113341.
[23] A. I. Mahameed, "A lightweight smart contract framework for behavior-based dynamic identity revocation in IoT systems," *J. Robot Control (JRC)*, vol. 6, no. 6, pp. 2799–2813, Nov. 2025, doi: 10.18196/jrc.v6i6.27204.
[24] S. B. Sharma and A. K. Bairwa, "Leveraging AI for intrusion detection in IoT ecosystems: A comprehensive study," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3550392.
[25] W. Daniels, B. B. Brumley, S. G. Chothia, and C. J. Mitchell, "Security MicroVisor: Efficient memory isolation and custom security services for IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017, doi: 10.1145/3154448.3154454.
[26] A. Banerjee, D. Vasisht, and R. Chandra, "Energy-efficient datagram transport layer security for IoT," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, 2018, doi: 10.1109/GLOCOM.2017.8255053.
[27] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, T. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for securing smart healthcare monitoring

system," *Future Gener. Comput. Syst.*, vol. 82, pp. 375–387, 2018, doi: 10.1016/j.future.2017.10.045.
[28] Y. Sun, Y. Zhang, G. Feng, and Y. Wu, "CloudEyes: Cloud-based malware detection with encrypted traffic for IoT," *Future Gener. Comput. Syst.*, vol. 72, pp. 344–356, 2017, doi: 10.1002/spe. 2420.
[29] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 73–83, Jan. 2020, doi: 10.1109/TSMC.2019.2903785.
[30] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An energy-efficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, pp. 11404–11417, 2022, doi: 10.1109/ACCESS.2022.3146295.
[31] X. Xu *et al.*, "Designing blockchain-based applications: A case study for imported product traceability," *Future Gener. Comput. Syst.*, vol. 92, pp. 399–406, 2019, doi: 10.1016/j.future.2018.10.010.
[32] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.
[33] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," *Comput. Commun.*, vol. 98, pp. 1–16, 2017, doi: 10.48550/arXiv. 1608.05187.
[34] M. Götzinger *et al.*, "RoSA: A framework for modeling self-awareness in cyber-physical systems," *IEEE Access*, vol. 8, pp. 141373–141394, 2020, doi: 10.1109/ACCESS.2020.3012824.
[35] W. Jiang, M. Chen, and J. Tao, "Federated learning with blockchain for privacy-preserving data sharing in Internet of vehicles," *China Commun.*, vol. 20, no. 3, pp. 69–85, Mar. 2023, doi: 10.23919/JCC.2023.03.006.
[36] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: A lightweight blockchain system for industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019, doi: 10.1109/TII.2019.2904049.
[37] S. Latif *et al.*, "Intrusion detection framework for the Internet of Things using a dense random neural network," *IEEE Trans. Ind. Informatics*, vol. 18, no. 9, pp. 6435–6444, Sep. 2022, doi: 10.1109/TII.2021.3130248.
[38] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.
[39] Z. M. Fadlullah *et al.*, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2432–2455, 2017, doi: 10.1109/COMST.2017.2707140.
[40] E. Hodo *et al.*, "Threat analysis of IoT networks using an artificial neural network intrusion detection system," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, 2016, pp. 1–6, doi: 10.1109/ISNCC.2016.7746067.
[41] B. B. Zarpelão, R. S. Miani, C. de Oliveira, and S. C. de Albuquerque, "A survey of intrusion detection in Internet of Things,"

J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017, doi: 10.1016/j.jnca.2017.02.009.
[42] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/ACCESS.2019.2962829.
[43] G. Carvalho, B. Cabral, V. Pereira, and J. Bernardino, "Edge computing: Current trends, research challenges and future directions," *Computing*, vol. 103, pp. 993–1023, 2021, doi: 10.1007/s00607-020-00896-5.
[44] T. P. da Silva, A. R. Neto, T. V. Batista, F. C. Delicato, P. F. Pires, and F. Lopes, "Online machine learning for auto-scaling in the edge computing," *Pervasive Mobile Comput.*, vol. 87, p. 101722, 2022, doi: 10.1016/j.pmcj.2022.101722.
[45] N. Agrawal, "Dynamic load balancing assisted optimized access control mechanism for edge-fog-cloud network in Internet of Things environment," *Concurrency Comput.: Pract. Exp.*, vol. 33, p. 6440, 2021, doi: 10.1002/cpe. 6440.
[46] M. Adhikari, M. Ambigavathi, V. G. Menon, and M. Hammoudeh, "Random forest for data aggregation to monitor and predict COVID-19 using edge networks," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 40–44, Jun. 2021, doi: 10.1109/IOTM.0001.2100052.
[47] S. Abbasian Dehkordi *et al.*, "A survey on data aggregation techniques in IoT sensor networks," *Wireless Netw.*, vol. 26, pp. 1243–1263, 2020, doi: 10.1007/s11276-019-02142-z.
[48] W. Feng *et al.*, "Joint energy-saving scheduling and secure routing for critical event reporting in wireless sensor networks," *IEEE Access*, vol. 8, pp. 53281–53292, 2020, doi: 10.1109/ACCESS.2020.2981115.
[49] F. Naeem, M. Tariq, and H. V. Poor, "SDN-enabled energy-efficient routing optimization framework for industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 17, no. 8, pp. 5660–5667, Aug. 2021, doi: 10.1109/TII.2020.3006885.
[50] H. Ahmadvand, C. Lal, H. Hemmati, M. Sookhak, and M. Conti, "Privacy-preserving and security in SDN-based IoT: A survey," *IEEE Access*, vol. 11, pp. 44772–44786, 2023, doi: 10.1109/ACCESS.2023.3267764.
[51] K. Haseeb, N. Islam, A. Almogren, and I. Ahmad, "AI-assisted energy-optimized sustainable model for secured routing in mobile wireless sensor networks," *IEEE Access*, vol. 8, pp. 21221–21233, 2020, doi: 10.1007/s11036-024-02327-7.
[52] A. A. Qaffas, M. Alhossani, and A. Almuflih, "AI-driven distributed IoT communication architecture for smart city traffic," *Sensors*, vol. 21, p. 2410, 2021, doi: 10.1007/s11227-025-07426-0.
[53] R. Etengu, S. C. Tan, L. C. Kwang, F. M. Abbou, and T. C. Chuah, "AI-assisted framework for green-routing and load balancing in hybrid software-defined networking: Proposal, challenges and future perspective," *IEEE Access*, vol. 8, pp. 166384–166441, 2020, doi: 10.1109/ACCESS.2020.3022291.
[54] R. A. Nazib and S. Moh, "Reinforcement learning-based routing protocols for vehicular ad hoc networks: A comparative survey," *IEEE*

Access, vol. 9, pp. 27552–27587, 2021, doi: 10.1109/ACCESS.2021.3058388.