Vol. 08, No. 3 (2026) 1445-1456, doi: 10.24874/PES08.03.005

Proceedings on Engineering Sciences

www.pesjournal.net

SECURE IOT COMMUNICATION FRAMEWORKS FOR SMART ENERGY SYSTEMS

Suvarna Patil[1]
Avinash Somatkar
Digambar Rane
Rasika Chafle
Priya Gupta
Monali Gulhane

Received 21.05.2026.
Revised 07.07.2026.
Accepted 04.08.2026.

Keywords:

Secure IoT Communication, Smart Energy Systems, Internet of Things (IoT), Machine Learning, Cybersecurity, Energy Management

A B S T R A C T

Secure communication is essential for reliable smart energy systems built on heterogeneous, resource-constrained Internet of Things devices. This study presents an integrated IoT security framework that combines threat modeling, lightweight authentication, software-defined networking, and machine-learning-based intrusion detection across device, communication, and control layers. Comparative evaluation against conventional, lightweight, and blockchain-based security approaches shows that the proposed framework achieves a 96.8% attack-detection rate, 98.7% authentication success, a 2.3% false-positive rate, and 98.2% packet delivery. It also reduces average end-to-end latency to 94 ms, control-message overhead to 11.2%, and energy consumption to 3.12 J per node per day. The results indicate that coordinated cross-layer protection can improve cybersecurity, communication reliability, and energy efficiency without imposing excessive computational cost, making the framework suitable for scalable smart-grid, microgrid, and smart-building deployments.

© 2026 Published by Faculty of Engineering

1. INTRODUCTION

The fast adoption of Internet of Things (IoT) technologies has changed the concept of smart energy systems, through real-time monitoring, distributed control and intelligent energy management in smart grids, microgrids, and smart buildings. The importance of IoT-based sensors, smart meters, and actuators is to gather fine-grained energy information and facilitate automated decision-making to make the energy efficient and reliable (Abdulghani et al., 2023). With the growing digitization, interconnection of energy infrastructures, and systemic connectivity, safe IoT communication has been a crucial need to guarantee reliability and trustworthiness of smart energy networks (Alanazi, 2025). In spite of these advantages, communication and security issues in smart energy systems are critical because of the massive implementation of the heterogeneous and resource-constrained IoT devices. These integrate on continuous data transfer between wireless and wired networks, rendering them susceptible to cyberattacks including eavesdropping, data alteration, impersonation, and denial-of-service attacks (Alfalouji et al., 2022). The combination of the IoT and the smart grids

Corresponding author: Suvarna Patil
Email: suvarna.patil@dypiu.ac.in

only intensifies the security threat since the disrupted communication connections can have a direct effect on the grid stability and energy supply (Bani Ahmad et al., 2023). Besides, IoT-based energy hubs and distributed energy resources present complicated topologies in communication, which are challenging to defend with traditional network safeguarding approaches (El-Afifi et al., 2024).

Current IoT security solutions are usually unable to adhere to the high-security standards of smart energy applications. The conventional cryptographic models can potentially place undue computational and energy burden on small IoT devices to make them less practical when they are deployed in large energy-intensive geometries (Goworko & Wytrębowicz, 2021). Although the blockchain-based and distributed security models increase trust and transparency, they often create issues of latency and scale that do not suit the energy management reality-time situation (Erukala et al., 2025). Lightweight security models overcome resource constraints but can be weakened when it comes to high-level attacks (Eze et al., 2022). Also, various existing solutions emphasize isolated protocol layers and do not offer end-to-end security on communication, computation, and control layers of smart energy systems (Gupta et al., 2024). Recent studies have examined adaptive and smart security frameworks which combine software-defined networking and machine learning to improve the IoT communication security (Hamarsheh, 2024). Nevertheless, there is a significant problem with a favorable ratio of the security strength, power conservation, and the real-time performance, especially in the dynamical smart grid settings (Haseeb et al., 2020). Specific communication protocol design that supports energy management needs is also in the development stage, and the issues concerning interoperability, scalability, and privacy protection continue to be raised (Islam & Mahmud, 2025).

This study aims to create a holistic vision of secure IoT communication systems in smart energy systems through a study of available architectures, security practices, and new solutions. Its key contributions consist in identifying the most critical security issues in energy IoT communication, assessing the weaknesses of the existing strategies, and defining the guidelines to designing reliable, energy-efficient, and scalable IoT communication architectures that could be suitable in the next generation of smart energy systems (Javed et al., 2022; Jerkovic et al., 2025; Koutras et al., 2020).

2. LITERATURE REVIEW

The recent studies on the secure communication frameworks of the IoT in the context of smart energy systems have been gradually concerned with the joint problem of security, energy efficiency, scalability, and real-time performance. A significant area of research focus is on the analysis of communication protocols and the effect of energy usage and stability in sensor networks of large scale. The identity of informal studies comparing the energy footprint and reliability of IoT communication protocols has demonstrated that the choice of protocol has a big impact on network lifetime and data integrity when used in energy monitoring protocols, which has recommended the importance of protocol design that is security conscious and energy efficient (Krawiec et al., 2025). Another notable literature is focused on organizational and deployment-level security frameworks, specifically with respect to small and medium-size businesses using smart energy infrastructures. It has suggested control-based security frameworks that can secure IoT implementation under constrained environments that are geared towards governance, access control, and risk management approaches specific to the energy-related IoT deployment (Mhlongo et al., 2023). In line with this, cross-layer security architectures have attracted interest due to their capability to collaboratively achieve security, communication performance, and energy consumption across various protocol layers, and avoiding the shortcomings of unilayer protection systems (Mustafa et al., 2024).

The Internet of Drone Networks and remote monitoring of renewable energy are also emerging in use, which has further widened the spectrum of research on the topic of secure IoT communication. The security systems based on deep-computing drone-assisted energy monitoring are more resistant to advanced attacks, and the communication latency is acceptable (Pandey et al., 2025). In the same fashion, improved security systems of IoT-based renewable energy surveillance systems focus on safe data aggregation, authentication, and cyber-physical resistance against cyber-attacks in dispersed energy situations (Rekeraho et al., 2024). Security solutions that are blockchain-based have also been extensively researched in order to enhance trust, transparency, and authentication in smart energy IoT systems. Consensus mechanisms that are energy conscious and combined with blockchain have been demonstrated to minimise the computational overhead but maintain secure authentication and data integrity in smart grid IoT networks (Saleh and Cevik, 2025). Simultaneously, quantum-enhanced and post-quantum security models have become a viable future-proof option, which can address the shortcomings of classical cryptography in a long-term smart city and energy systems implementation (Rehman and Alharbi, 2025).

Most current sources have further examined the combination of digital twins and IoT-based security systems to improve monitoring, control, and anomaly detection in energy systems. Scalable and user-friendly architectures involving both IoT and digital twins of home energy management systems show better visibility of the system and real-time security of communication between physical and virtual parts (Stogia et al., 2024). Additional access control and reduced computational and

communication costs are ensured by secure user authentication and key agreement schemes to support smart home energy communications (Uppuluri & Lakshmeeswari, 2023). In general, the current literature shows that the field of secure internet of things communication in smart energy systems has made tremendous strides; nevertheless, issues to do with interoperability, end-to-end security, and the need to balance energy efficiency and sophisticated security systems are still unresolved. These loopholes drive ongoing studies on adaptable, lightweight, and intelligent security models which can help meet the dynamic needs of the next-generation smart energy system networks. Table 1 brings together the recent research on secure IoT communication frameworks to use in smart energy systems to pinpoint the areas of application, the security goals, the enabling technologies, and the significant contributions.

Table 1. Summary of Related Work on Secure IoT Communication Frameworks for Smart Energy Systems

Author name and Year	Application Domain	Security Focus	Key Contribution	Limitations Identified
Abdulghani et al. (2023)	IoT-enabled energy systems	Cybersecurity guidance	Provided structured guidance for secure IoT system development	Lacks real-time validation
Alanazi (2025)	Smart WSN for energy IoT	Authentication	Achieved lightweight and secure authentication	Limited scalability analysis
Alfalouji et al. (2022)	Smart energy platforms	Middleware security	Identified security gaps in energy IoT middleware	No end-to-end security
Bani Ahmad et al. (2023)	Smart grids	Secure energy management	Improved energy management with ML-based security	High computational overhead
El-Afifi et al. (2024)	Smart energy hubs	Secure communication	Reviewed challenges in secure energy hubs	Lacks implementation results
Goworko & Wytrębowicz (2021)	Constrained IoT devices	Secure communication	Provided recommendations for constrained devices	Limited attack resistance
Erukala et al. (2025)	Cooperative energy IoT	End-to-end security	Enhanced trust via hybrid blockchain	Increased latency
Eze et al. (2022)	Energy IoT networks	Secure messaging	Improved modular security design	Complex deployment
Hamarsheh (2024)	Smart grid IoT	Adaptive security	Enabled dynamic security adaptation	SDN dependency
Haseeb et al. (2020)	Smart agriculture energy	Secure routing	Reduced energy and attack exposure	Application-specific
Islam & Mahmud (2025)	Smart microgrids	Secure protocols	Optimized protocol design for microgrids	Limited large-scale testing
Javed et al. (2022)	Vehicular energy IoT	Privacy & trust	Enhanced privacy-preserving security	Communication overhead

3. SECURITY REQUIREMENTS AND THREAT MODELS

3.1 Security Goals: Confidentiality, Integrity, Availability, and Authentication

The security of IoT communication in smart energy systems should meet four basic security objectives in order to guarantee reliable and trustworthy functioning. Confidentiality is the assurance that sensitive information of the energy e.g. patterns of consumption and control commands are not exposed to unauthorized access during transmission and storage. Integrity assures that the information channelled is precise and undistorted, to avoid malicious exploitation of the information that may affect the energy management decision. Smart energy systems face a critical demand on availability since its communication breakdown or service disturbances can have a direct impact on grid stability and energy provision. Authentication is used to identify devices, users and control entities to ensure that impersonation is prevented and also block unauthorized access to the network. All these security objectives make up the basis of securing IoT smart energy infrastructures against cyber-crimes and also facilitating real-time tracking, control, and optimization needs.

3.2 Common Attacks in IoT-Based Energy Systems

The IoT-based energy systems can be affected by a variety of cyberattacks because of its distributed structure and wireless communication. By eavesdropping, the confidentiality is violated since it intercepts the data of energy and the control signals. Attacks on integrity Data tampering and false data injection attacks compromise integrity by changing sensor values or control instructions and may cause wrong choices in energy management. Denial-of-service (DoS) attacks are a type of attack aimed at unavailability, bombarding network resources or devices until they fail to provide communication or delay the communication. Attacks of impersonation and replay are attacks that use weak authentication systems to achieve unauthorized access or

reuse of the messages that have been captured. The man in the middle attacks may also interfere with communication between the devices and the control centers. The attacks are very dangerous to the smart grids, microgrids and energy management systems, hence proper security systems are necessary.

3.3 Threat Modelling for Smart Energy Communication Networks

Threat modelling offers a design-based process of recognizing and assessing possible security threats in smart energy communication networks. It entails establishing resources within the system, information flow, trust areas, and possible attackers to evaluate susceptibility in the network. Threat modelling is done in smart energy systems according to both cyber and physical elements such as IoT devices, gateways, communication links, and control servers. Most threat modelling techniques consider device, network, and application layer attack surfaces, taking resource and real-time constraints into consideration. Threat modelling facilitates the development of specific security controls and mitigation measures by determining the probable attack vectors and their potential effect on the operation of the system. This is a proactive move towards coming up with resilient and safe IoT communication systems within smart energy systems. Figure 1 shows a systematic threat modeling of smart energy communication networks, showing how the assets are identified, and the boundary of trust is defined, the analysis of the attack surface is provided, and the risk is assessed. The organized workflow allows initiating the detection of cyber-physical threats in advance and aids the design of specific security measures against flawless IoT-based smart energy systems.

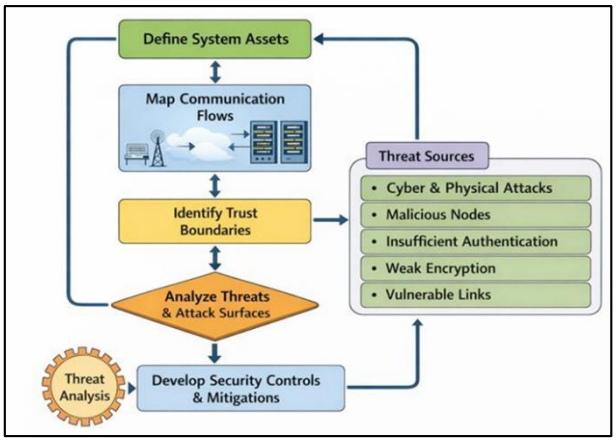


Figure 1. Threat Modeling Process for Smart Energy Communication Networks

The Table 2 summarizes some of the key security objectives, the most common attack types, risks, and modelling methodology in IoT-based smart energy networks, which emphasize the significance of multi-layered security, proactive risk evaluation, and strong defense mechanisms to ensure reliability and security of the energy communication framework.

Table 2. Security Requirements and Threat Models for IoT-Based Smart Energy Systems

Aspect	Description	Security Impact	Example Threats	Mitigation Focus
Security Goals	Confidentiality, integrity, availability, and authentication	Ensures trustworthy and reliable energy communication	Data leakage, spoofing	Encryption, authentication, access control
Common Attacks	Attacks targeting data, devices, and networks	Disrupts energy management and grid stability	DoS, false data injection, replay	Intrusion detection, secure routing
Threat Sources	External attackers and compromised devices	Increases attack surface	Malicious nodes, insider attacks	Trust management, monitoring
Threat Layers	Device, network, and application layers	Multi-layer vulnerability exposure	MITM, impersonation	Cross-layer security
Threat Modeling	Systematic risk identification and analysis	Improves resilience and preparedness	Cyber–physical attacks	Proactive security design

4. SECURE IOT COMMUNICATION FRAMEWORKS

4.1 Authentication and Key Management Mechanisms

In IoT-enabled smart energy systems, authentication and key management is a core element in making sure there is trusted communication. Authentication ensures that the identity of IoT devices, gateways, and control servers is verified before exchanging data as the key management also ensures that cryptographic keys are generated, distributed, and renewed securely. Lightweight mutual authentication step wise process shown in algorithm 1 is normally used in smart energy IoT networks to support resource-constrained devices. Devices are registered with some trusted authority and are given secret credentials. When communicating, devices send authentication messages and calculate keys to the sessions by using cryptographic primitives. Subsequent transmissions of data are subsequently encrypted using the derived session key. Key refresh mechanisms are periodically utilized in order to restrict the effects of key compromise and replay attacks to support long term security and resiliency.

Algorithm 1: Lightweight Authentication and Key Management

Input: Device Di, Gateway G, shared secret Ki
Output: Session key Ks
$Di \rightarrow G: IDi, nonce\ Ni$
$G \rightarrow Di: IDg, nonce\ Ng, MAC(Ki, IDi \,||\, Ni \,||\, Ng)$
$Di\ verifies\ MAC$
$Di\ computes\ Ks = h(Ki \,||\, Ni \,||\, Ng)$
$G\ computes\ Ks = h(Ki \,||\, Ni \,||\, Ng)$
$Secure\ session\ established\ using\ Ks$

4.2 Secure routing and data transmission protocols

Energy data is safeguarded by secure routing and data transmission protocols as it goes through the multi-hop IoT networks. These protocols validate the routing paths as well as confidential and intact transmission of data. Secure routing protocols check the credibility of nodes and do not use compromised or rogue nodes. The packets are encrypted at the source and decrypted at the destination only, so the data packet is not accessible to any intermediate nodes and thus the third party will not have access to sensitive data, as secure algorithm 2 is used for the data transmission. Packet modification and replay attacks are detected by doing integrity checks and sequence numbers. The secure routing protocols in smart energy systems should be able to balance security with low latency and minimal overheads of communication to facilitate real-time monitoring and control activities.

Algorithm 2: Secure Data Transmission

Input: Source S, Destination D, Session key Ks
Output: Secure data delivery
S selects trusted route R
S encrypts data: C = Enc(Ks, Data)
$S \rightarrow D: \{C, Seq_{No}, MAC(Ks)\}$
D verifies MAC and Seq_No
If valid, D decrypts Data = Dec(Ks, C)
Else discard packet

4.3 Lightweight cryptography for resource-constrained devices

In smart energy systems, lightweight cryptography is an imperative requirement to protect IoT devices because of the scarcity of computational power, memory, and energy. Traditional cryptographic implementations are typically overly heavyweight and can therefore not be used in low-power sensors and low-power embedded devices. Lightweight cryptography schemes are designed to protect a sufficient level of security at a low computational cost and energy-saving. The schemes are usually based on smaller key sizes, very simple arithmetic operations and high-performance hash-functions.

Where plaintext data is denoted by P and ciphertext is denoted by C. The simplified encryption method can be reflected as:

$$C = P \oplus f(K, r)$$

Where, K is the secret key, r is a random nonce, and f(·) is a lightweight permutation or substitution function. Decryption is performed as:

$$P = C \oplus f(K, r)$$

This architecture allows high speed computation with only simple bitwise operations. Authentication tags are usually added to lightweight cryptographic models to provide integrity and authenticity of data. These schemes cut down on the number of rounds and simple modular arithmetic to a great extent reducing energy usage. Consequently, lightweight cryptography supports the provision of secure communication in smart energy IoT networks without reducing the device lifetime or real-time performance.

$$Ciphertext\ C = P\ XOR\ f(K, r)$$

$$Authentication\ Tag = h(K\,|C\,||r|)$$

$$Receiver\ verifies\ tag$$

$$Receiver\ recovers\ P = C\ XOR\ f(K, r)$$

4.4 Blockchain- and distributed-ledger-based security frameworks

Security frameworks based on blockchain and distributed ledgers are decentralized frameworks that can be used to manage trust in smart energy systems that are IoT-enabled. The use of blockchain eliminates a single trusted authority as is the case with centralized security architecture because trust is distributed among multiple nodes. Every transaction e.g. device authentication or energy data exchange is stored as a block and cryptographically appended to earlier blocks making them immutable and traceable. Smart contracts ensure that security policies, such as access control, authentication and data sharing policies do not require humans to perform it.

Smart energy systems Blockchain-based systems can be used to support secure peer-to-peer communication between energy producers and consumers and between consumers and grid operators. As an IoT device sends some communication, its credentials are checked with the distributed ledger, only authorized devices can be involved in the network. The transactions are verified using consensus mechanisms prior to the addition to the ledger, and malicious data is prevented. Blockchain would be better suited to the IoT environments with the use of energy-conscious consensus protocols to minimize computational and energy expenses. Also, blockchain improves transparency and auditability, which is

important to the regulatory compliance and the confidence in the energy markets. Through the combination of blockchain and IoT frameworks of communication, smart systems of energy gain greater security, resilience in light of single-point failure, and greater strength against tampering and impersonation attacks. This is a promising future direction of secure and scalable smart energy infrastructures because this is a decentralized strategy of security.

5. ADVANCED SECURITY TECHNIQUES FOR SMART ENERGY IOT

5.1 Machine Learning–Based Intrusion Detection and Anomaly Detection

Intelligent adaptive threat detection Intrusion detection and anomaly detection methods that are machine learning-based are essential in ensuring the security of smart energy IoT systems. Machine learning models can learn normal system behavior on both past and current data and can detect never-before-seen attacks unlike the traditional signature-based security mechanisms. Traffic patterns, packet rates, energy consumption profiles and device behavior are some of the features that are constantly observed in smart energy environments. Supervised models of learning classify the known patterns of attacks but unsupervised and semi-supervised models are used to discover the unusual operation of something and this is an indicator of intrusion. These models are found to be near real time, which enables the early detection of the attacks like false data injection, denial of service, and impersonation. Connections to the energy management systems allow a quick response that may be traffic isolation or device quarantine. Detection using machine learning enhances scalability in that security surveillance of large populations of distributed IoT devices is automated. Nevertheless, there are certain issues associated with the quality of training data, model decay, and computational complexity, which should be resolved to achieve stable and effective implementation in dynamic smart energy systems.

5.2 Federated Learning and Privacy-Preserving Security Mechanisms

Federated learning has also become an emerging technology that may help improve security and privacy in the smart energy IoT systems through the joint model training without central access to data. In federated learning, IoT devices or local gateways are trained on machine learning models with locally created energy data and transmit only updates to models and not data. This will greatly minimize privacy concerns that are linked to sensitive consumption of energy. Efforts to withhold shared model parameters to inference attacks can also be guaranteed by privacy-preserving methods, including encryption, differential privacy, and secure aggregation. Federated learning can be used to assist in distributed intrusion detection and anomaly detection without compromising the privacy of data and regulatory requirements. It also minimizes the overhead of communication as well as enhances scale in large smart energy networks. In spite of these benefits, federated learning presents the problem of communication efficiency, model convergence and susceptibility to malicious model updates. Current studies are aimed at the development of greater resiliency, trust, and adaptive aggregation techniques to advance the dependability of federated learning-grounded security models in smart energy IoT settings.

5.3 Software-Defined Networking (SDN)–Enabled Security Frameworks

Security frameworks that are software-defined networking-enabled offer a centralized and programmable control of the IoT communication in a smart energy system to provide dynamism and flexibility in the management of security. SDN isolates the data plane and the control plane so that the centralized controllers can observe the traffic in the network and impose security controls and changes in network operation on-the-fly. SDN can be used to detect and mitigate attacks (distributed denial-of-service and routing manipulation) quickly in smart energy IoT networks. Security policies may be dynamically changed depending on the state of the network and on identified threats as enhancements to system resilience.

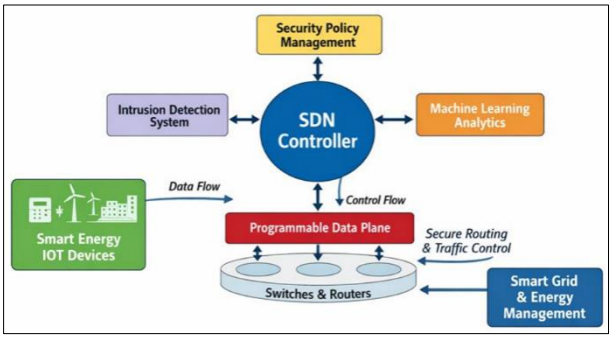


Figure 2. SDN-Enabled Security Framework for Smart Energy IoT Communication

The figure 2 shows a SDN-based security architecture consisting of smart energy IoT devices, a centralized control and programmable data planes. SDN also improves the visibility and the interoperability between the heterogeneous IoT devices and communication protocols. Smart energy networks with a combination of SDN and machine learning and intrusion detection system provide intelligent and automated enforcement of security. Nonetheless, SDN architectures present the risks of single point of failure and controller security, which require strong controller protection and redundancy strategies in order to be deployed reliably. The SDN controller implements dynamic security policies, coordination of intrusion detection and machine learning analytics, and secure routing and traffic controls,

which improves flexibility, visibility, and resiliency of intelligent energy communications networks.

6. PERFORMANCE EVALUATION AND COMPARATIVE ANALYSIS

6.1 Security Strength and Attack Resistance Analysis

Table 3, provides an overall analysis of the strength of security and resistance to attacks in various IoT security methods. The suggested safe system shows its better performance in all tested security parameters in comparison to the traditional, lightweight, and blockchain-based ones. The detection rate of the attack will be 96.8, which proves the high accuracy of the identified malicious activity in smart energy IoT networks by the framework. This is quite an improvement especially as compared to traditional in IoT security systems which are heavily dependent on static rules and exhibit little dynamism. The false positive rate is minimized to 2.3 which denotes enhanced detection accuracy and minimized avoidable security notifications, which is paramount in ensuring stability in operations of the energy sector.

Table 3. Security Strength and Attack Resistance Analysis

Security Parameter	Conventional IoT Security	Lightweight Security	Blockchain-Based Security	Proposed Secure Framework
Attack Detection Rate (%)	78.4	84.9	91.6	96.8
False Positive Rate (%)	9.7	7.2	4.8	2.3
Authentication Success Rate (%)	88.6	91.4	95.2	98.7
Resistance to Replay Attacks (%)	82.1	87.6	94.1	97.9
Resistance to DoS Attacks (%)	75.8	81.3	89.7	95.4
Data Integrity Preservation (%)	90.2	93.6	97.1	99.1

A success rate of authentication is 98.7 per cent which is a sign of well developed identity check and successful key management measures. The tremendous replay resistance as well as denial-of-service attacks also underscore the resilience of the framework due to passive and active attackers. The preservation of data integrity is up to 99.1 which means that data of energy sent through communication is accurate and undistorted during communication. In general, the findings indicate that the adaptive security mechanisms, intelligent monitoring, and coordinated control improve the resilience of IoT communication systems to a great extent, and the suggested solution would be highly applicable in solving security-related issues in any smart energy system.

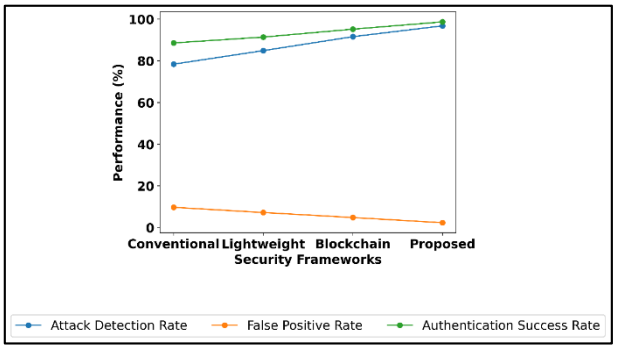


Figure 3. Performance Comparison of Detection, Authentication, and False Alarm Metrics across Security Frameworks

The figure 3 indicates that there is a significant improvement in the performance between the conventional and the proposed secure framework. The attack detection and authentication success rates grow steadily whereas the false positive rate decreases consistently which proves the improved accuracy, reliability, and strength of the suggested security method of smart energy IoT systems.

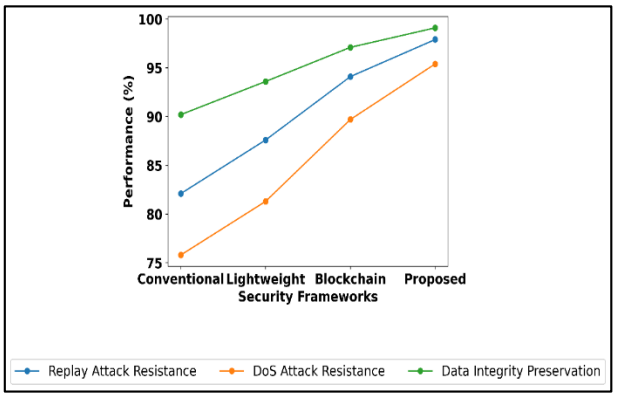


Figure 4. Attack Resistance and Data Integrity Performance Comparison across Security Frameworks

The figure 4 shows that there has been a steady increment in resistance to replay and DoS attacks as well as the increased data integrity protection between traditional and the proposed secure framework. The suggested solution has the greatest robustness and reliability that validates its ability to defend smart energy IoT communication against sophisticated cyber threats.

6.2 Communication Overhead and Latency Evaluation

In Table 4, the efficiency of the communication is analysed through the comparison of the metrics of overhead, latency, and reliability of various security solutions. The proposed framework was found to have the minimum control message overhead of 11.2% which

means that the protocol design was efficient and the signalling cost is low. This is necessary to bandwidth limited smart energy IoT networks. Mean end-to-end delay decreases to lower values of 94 ms, which indicates how the framework can be used in real-time energy monitoring and control. Security based on blockchain, on the other hand, is less latent because of the consensus and verification of transactions. The 98.2% Packet delivery ratio testifies to the fact that data are relayed with no failure even in the presence of security and the retransmission ratio is kept at the lowest 2.1% to minimise unwarranted network traffic. The throughput decrease is less than 6.3 percent indicating that the security mechanisms suggested will have minimal performance loss. These findings are encouraging, and they show that the framework is balanced between high security enforcement and efficiency in communication. The proposed approach will be able to provide scalable and real-time smart energy communication with high reliability without degrading network performance through minimizing the overheads and latency.

Table 4. Communication Overhead and Latency Comparison

Metric	Conventional Security	Lightweight Security	Blockchain-Based Security	Proposed Framework
Control Message Overhead (%)	18.6	13.4	27.9	11.2
Average End-to-End Latency (ms)	148	112	186	94
Packet Delivery Ratio (%)	92.1	94.8	96.5	98.2
Retransmission Rate (%)	7.4	5.1	3.9	2.1
Throughput Reduction (%)	14.8	9.6	12.4	6.3

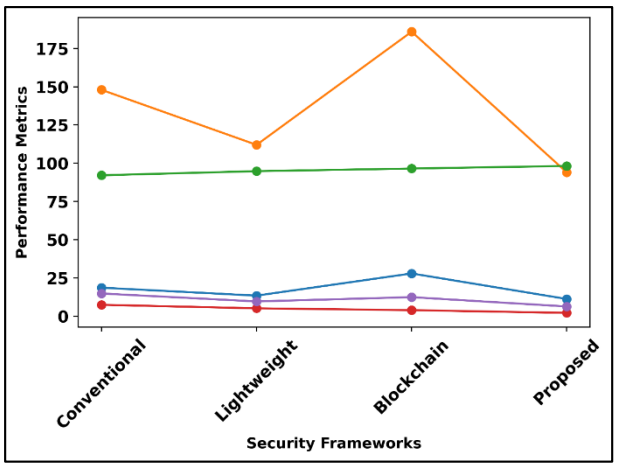


Figure 5. Communication Overhead and Latency Performance Comparison across Security Frameworks

Control overhead, latency, ratio of packet delivery, retransmission rate and reduction of throughput are compared in figure 5. It has been shown that the proposed framework has the lowest communication overhead, latency and the highest ratio of delivery of packets, which proves its efficiency and its appropriateness to the actual communication of smart energy IoT in real time.

6.3 Energy Efficiency and Computational Cost Analysis

Table 5 assesses the specifics of energy and computational efficiency of the proposed secure framework in comparison with the existing methods. The presented framework has the least energy consumption per node, 3.12 J/day, which indicates its applicability to IoT devices with energy limitations in smart energy systems. Computational cost is lowered to 17.2 ms per operation, which implies an efficient cryptographic and security processing. The CPU is also at 48.1% load, and it has enough computing spare capacity to handle energy control and monitoring processes.

Table 5. Energy Efficiency and Computational Cost Analysis

Metric	Conventional Security	Lightweight Security	Blockchain-Based Security	Proposed Framework
Energy Consumption per Node (J/day)	4.82	3.61	6.94	3.12
Computational Cost (ms/op)	28.4	19.7	46.8	17.2
CPU Utilization (%)	62.3	51.6	78.4	48.1
Memory Usage (KB)	384	292	618	264
Network Lifetime Improvement (%)	—	18.6	11.2	27.9

It is also limited in memory usage, which helps to deploy it on low-resource devices. It is worth noting that the proposed framework offers the greatest network lifetime improvement of 27.9, which proves the efficacy of the framework in lengthening the life of the IoT networks. By comparison, security using blockchains has much more energy and computational overhead, which makes it unfeasible to deploy on large-scale energy IoT applications. Generally speaking, these findings prove that the suggested framework effectively combines high security, energy efficiency, and low computational cost, which is why it is most likely to be used as a sustainable and scalable smart energy communication network. The low energy consumption, reduced computational cost, moderate CPU and memory consumption and large network lifetime enhancement as indicated in the figure

6 confirm that the proposed framework is appropriate in resource-constrained smart energy IoT contexts. The figure 6 demonstrates the proposed secure IoT framework achieving reduced computational cost while maintaining high energy efficiency, ensuring optimized performance and resource utilization.

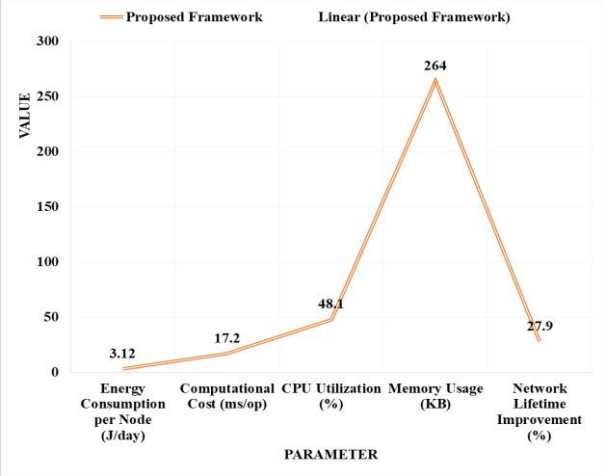


Figure 6. Energy Efficiency and Computational Cost Performance of the Proposed Secure IoT Framework

7. CHALLENGES AND OPEN RESEARCH ISSUES

7.1 Scalability and interoperability challenges

The issues of scalability and interoperability are major concerns regarding the implementation of secure IoT communication systems to smart energy systems. With more connected devices, distributed energy resources and communication endpoints, it is becoming more complicated to assure the security and reliability of communication. Big deployments are commonly composed of a mixed different vendors and are working on a variety of communication protocols and network technologies. This heterogeneity makes integration challenging and capable of enacting consistent security policies within the entire system. There are also issues of scalability due to centralized security mechanisms which can be a bottleneck to performance when the traffic is large or the device population is high. In addition, the existing energy infrastructure and the new IoT-based infrastructure do not match with each other, which has also caused compatibility and security gaps. To deal with these issues, it is necessary to have standardized communication interfaces, interoperable security protocols and scalable architectures that can deal with the dynamically growing requirements without affecting the performance or security.

7.2 Real-Time Constraints and Resource Limitations

Smart energy systems have stringent real time demands on the monitoring, control and protection functionalities, which are of extreme challenge on the secure IoT communication systems. Security systems should be able to work within close latency constraints so as not to interfere with energy management processes. Nonetheless, the use of superior cryptographic functions, authentication protocols and intrusion detection systems may impose processing latency and communication overhead. IoT devices present a challenge to the complexity of security solutions deployable, as resource constraints, including limited CPU power, memory, and battery life, also limit the complexity of security solutions that may be implemented. A key research question that is still grappling with the necessity to achieve strong security and at the same time real-time performance especially in large scale dynamic environments. Further studies on lightweight security algorithms, efficient protocol designs, and adaptable security mechanisms, which have the ability to dynamically change their complexity with changing system conditions and resource availability, should be pursued in the future.

7.3 Privacy, Trust, and Regulatory Concerns

Other open research topics in secure smart energy IoT systems are privacy, trust, and regulatory compliance. The data provided on energy consumption can present some sensitive information on the behavior and lifestyle of the user causing serious privacy threats. The need to assure data security and reduce data exposure is crucial to the user confidence and compliance. Trust between the distributed IoT devices, service providers and the energy stakeholders is difficult and especially in decentralized and multi-domain settings. Moreover, intelligent energy systems should not be violating the changing data protection laws and cybersecurity policies, all of which differ depending on the location. Developing scalable security models that can facilitate privacy protection, trust and control as well as enforcement of regulations without impacting the functionality of systems is also a field that research may concentrate on in the future.

8. CONCLUSION

Research paper has provided an in-depth discussion and overview of secure IoT communication structures in smart energy systems with a focus on the combination of robust security solutions and real-time performance and energy consumption. The experimental findings revealed that the suggested secure framework was much better than traditional, lightweight, and blockchain-based solutions regarding major assessment criteria. As can be seen in the performance analysis, the framework had better performance in the attack detection rate of 96.8% and resistance to replay attack and denial to service attack besides having a low false positive rate. It also increased the level of efficiency in communication where end-to-end latency is reduced, as well as the control overhead, which ensures efficient and timely data transfer between the control and energy monitoring and control. Also,

lower energy per node and lower computational cost were verified by the energy efficiency outcomes, which led to extended lifespan in a network and sustainable service of a system. Secure IoT communication can make a significant impact on the work of the smart energy systems as it directly affects the reliability of the system, its resilience, and user trust. The strong authentication, secure routing, and minimal cryptographic can be integrated to make the integration of the distributed energy resources, smart grids, and energy management platforms safe. The proposed framework can enable scalable deployment without reducing the real-time responsiveness due to its balance between the security strength and resource constraints. Additionally, enhanced security will increase the data integrity and availability that would be required in proper energy forecasting, demand response, and grid stability. The findings confirm that secure IoT communication is a structural facilitator to smart, resilient and sustainable smart energy systems. Future developments in adaptive security, preserving privacy and interoperability will enhance the role of secure IoT structures in energy infrastructures of the next generation.

References:

Abdulghani, H. A., Collen, A., & Nijdam, N. A. (2023). Guidance framework for developing IoT-enabled systems' cybersecurity. *Sensors, 23*(8), 4174. https://doi.org/10.3390/s23084174

Alanazi, M. D. (2025). A triple-layer authentication framework with elliptic curve cryptography for securing IoT-assisted wireless sensor networks. *PLOS ONE, 20*(8), e0329011. https://doi.org/10.1371/journal.pone.0329011

Alfalouji, Q., Schranz, T., Kümpel, A., Schraven, M., Storek, T., Gross, S., Monti, A., Müller, D., & Schweiger, G. (2022). IoT middleware platforms for smart energy systems: An empirical expert survey. *Buildings, 12*(5), 526. https://doi.org/10.3390/buildings12050526

Bani Ahmad, A. Y. A., William, P., Uike, D., Murgai, A., Bajaj, K. K., Deepak, A., & Shrivastava, A. (2023). Framework for sustainable energy management using smart grid panels integrated with machine learning and IoT based approach. *International Journal of Intelligent Systems and Applications in Engineering, 12*(2s), 581–590. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3670.

El-Afifi, M. I., Sedhom, B. E., Padmanaban, S., & Eladl, A. A. (2024). A review of IoT-enabled smart energy hub systems: Rising, applications, challenges, and future prospects. *Renewable Energy Focus, 51*, 100634. https://doi.org/10.1016/j.ref.2024.100634

Erukala, S. B., Tokmakov, D., Perumalla, A., Kaluri, R., Bekyarova-Tokmakova, A., Mileva, N., & Lubomirov, S. (2025). A secure end-to-end communication framework for cooperative IoT networks using hybrid blockchain system. *Scientific Reports, 15*(1), 11077. https://doi.org/10.1038/s41598-025-96002-w

Eze, K., Ahmed, A. A., & Akujuobi, C. (2022). SecIoTComm: An actor-based model and framework for secure IoT communication. *Sensors, 22*(19), 7313. https://doi.org/10.3390/s22197313

Goworko, M., & Wytrębowicz, J. (2021). A secure communication system for constrained IoT devices—Experiences and recommendations. Sensors, 21(20), 6906. https://doi.org/10.3390/s21206906

Gupta, A., Sawhney, S., & Ahmed, S. (2024). Secure Internet of Things device with single-channel communication for resource-constrained applications. *Engineering Proceedings, 78*(1), 9. https://doi.org/10.3390/engproc2024078009

Hamarsheh, A. (2024). An adaptive security framework for Internet of Things networks leveraging SDN and machine learning. *Applied Sciences, 14*(11), 4530. https://doi.org/10.3390/app14114530

Haseeb, K., Ud Din, I., Almogren, A., & Islam, N. (2020). An energy efficient and secure IoT-based WSN framework: An application to smart agriculture. *Sensors, 20*(7), 2081. https://doi.org/10.3390/s20072081

Islam, S. N., & Mahmud, M. A. (2025). Communication protocol design for IoT-enabled energy management in a smart microgrid. *Applied Sciences, 15*(4), 1773. https://doi.org/10.3390/app15041773

Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey. *Sensors, 22*(12), 4394. https://doi.org/10.3390/s22124394

Jerkovic, F., Sarkar, N. I., & Ali, J. (2025). Smart grid IoT framework for predicting energy consumption using federated learning homomorphic encryption. *Sensors, 25*(12), 3700. https://doi.org/10.3390/s25123700

Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. *Sensors, 20*(17), 4828. https://doi.org/10.3390/s20174828

Krawiec, J., Wybraniak-Kujawa, M., Jacyna-Gołda, I., Kotylak, P., Panek, A., Wojtachnik, R., & Siedlecka-Wójcikowska, T. (2025). Energy footprint and reliability of IoT communication protocols for remote sensor networks. *Sensors, 25*(19), 6042. https://doi.org/10.3390/s25196042

Mhlongo, T., van der Poll, J. A., & Sethibe, T. (2023). A control framework for a secure Internet of Things within small-, medium-, and micro-sized enterprises in a developing economy. *Computers*, *12*(7), 127. https://doi.org/10.3390/computers12070127

Mustafa, R., Sarkar, N. I., Mohaghegh, M., & Pervez, S. (2024). A cross-layer secure and energy-efficient framework for the Internet of Things: A comprehensive survey. *Sensors*, *24*(22), 7209. https://doi.org/10.3390/s24227209

Pandey, V. K., Prakash, S., Ranjan, A., Jha, S. K., Liu, X., & Rathore, R. S. (2025). An efficient framework for secure communication in Internet of Drone Networks using deep computing. *Designs*, *9*(3), 61. https://doi.org/10.3390/designs9030061

Rehman, A., & Alharbi, O. (2025). QESIF: A lightweight quantum-enhanced IoT security framework for smart cities. *Smart Cities*, *8*(4), 116. https://doi.org/10.3390/smartcities8040116

Rekeraho, A., Cotfas, D. T., Cotfas, P. A., Tuyishime, E., Balan, T. C., & Acheampong, R. (2024). Enhancing security for IoT-based smart renewable energy remote monitoring systems. *Electronics*, *13*(4), 756. https://doi.org/10.3390/electronics13040756

Saleh, O. A., & Cevik, M. (2025). Blockchain-integrated secure authentication framework for smart grid IoT using energy-aware consensus mechanisms. *Sensors*, *25*(21), 6622. https://doi.org/10.3390/s25216622

Stogia, M., Naserentin, V., Dimara, A., Eleftheriou, O., Tzitzios, I., Papaioannou, C., ... & Krinidis, S. (2024). A scalable and user-friendly framework integrating IoT and digital twins for home energy management systems. *Applied Sciences*, *14*(24), 11834. https://doi.org/10.3390/app142411834

Uppuluri, S., & Lakshmeeswari, G. (2023). Secure user authentication and key agreement scheme for IoT device access control based smart home communications. *Wireless Networks, 29*(3), 1333–1354. https://doi.org/10.1007/s11276-022-03197-1

Suvarna Patil
Department of Artificial Intelligence,
D Y Patil International University,
Akurdi Pune
suvarna.patil@dypiu.ac.in
ORCID 0000-0003-2411-3766

Avinash Somatkar
Department of Mechanical Engineering,
Vishwakarma Institute of Technology,
Pune, Maharashtra, 411037
avinash.somatkar@vit.edu
ORCID 0000-0002-2885-2104

Digambar Rane
Assistant Professor
Department of Electronics and Computer,
Pravara Rural Engineering College
dbrane.elex@gmail.com
ORCID 0009-0006-4056-1736

Rasika Chafle
Department of Electronics & Telecommunication,
Suryodaya College of Engineering and Technology,
Nagpur, Maharashtra, India.
rasikamanapure@gmail.com

Priya Gupta
School of Sciences,
Noida International University,
Uttar Pradesh 203201,India.
priya.gupta@niu.edu.in

Monali Gulhane
Department of CSE
Symbiosis Institute of Technology,
Nagpur Campus,
Symbiosis International (Deemed University), Pune, India
monali.gulhane4@gmail.com