International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Secure Communication Model for Low Power IOT Networks

Srushti Wanjari, Himani Kubade

G H Raisoni University, Amravati, Maharashtra, India

Abstract

The Internet of Things' (IoT) explosive expansion has led to the deployment of a large number of low-power, resource-constrained devices in smart cities, smart healthcare, and industrial automation. Because of their low energy, computing power, and memory, these devices still face substantial challenges in guaranteeing secure connection. For such contexts, traditional security measures are frequently excessively complicated and energy-intensive. The secure communication paradigm proposed in this paper is especially made for ultra-low power Internet of Things networks. To guarantee the secrecy, integrity, and authenticity of data, the technique uses mutual authentication, elliptic curve cryptography-based key distribution, and lightweight symmetric encryption. In order to balance security and energy efficiency, an adaptive security system also dynamically modifies protection levels according to device capability and data sensitivity. According to simulation results, the suggested approach preserves scalability and reliability for low-cost IoT installations while lowering energy consumption, communication overhead, and latency when compared to traditional protocols like TLS and DTLS. Low Power Internet of Things (IoT) networks are being used more and more in vital areas like environmental sensing, industrial automation, smart cities, and healthcare monitoring. However, the application of traditional security methods is difficult due to their limited resources, including memory, computing power, and energy. With an emphasis on scalable key management, energy-efficient authentication, and lightweight cryptographic operations, this study suggests a secure communication architecture especially made for low power Internet of Things networks. The suggested paradigm incorporates a hierarchical trust-based key distribution method to minimize computational complexity, lightweight hash-based message authentication for integrity, and symmetric key encryption for data confidentiality. The architecture uses mutual authentication and dynamic session key generation to reduce communication costs and improve resilience against typical threats such replay attacks, node impersonation, eavesdropping, and denial-of-service assaults. The lifespan of the network is also increased by energy-aware security scheduling, which makes sure that security processes adjust to node power levels. In comparison to conventional security frameworks, performance evaluation shows that the suggested model achieves high security guarantees with less computing complexity and energy consumption. The model may be deployed in wireless sensor and IoT networks with little resources and is scalable and flexible enough to adapt to diverse IoT contexts. A useful and effective framework for secure communication in next-generation low power Internet of Things systems is contributed by this work.

KEYWORDS: *Internet of Things (IoT), Low-Power IoT Networks, Secure Communication, Lightweight Cryptography, Elliptic Curve Cryptography (ECC), Symmetric Encryption, Mutual Authentication, Key Management, Energy Efficiency, Wireless Sensor Networks, Data Integrity, Confidentiality, Edge Computing, Secure Data Aggregation, Adaptive Security Policy.*

1. Introduction

In a variety of fields, including smart cities, healthcare monitoring, industrial automation, agriculture, and environmental sensing, billions of interconnected devices have been widely deployed as a result of the Internet of Things' (IoT) explosive growth. These Internet of Things devices are usually low-power and resource-constrained, with little memory, battery-powered operation, and limited computational capacity. Secure communication is a basic necessity since, in spite of their limits, they are in charge of gathering, sending, and processing important and frequently sensitive data. Power-efficient IoT networks mostly use wireless communication, which is open to a variety of security risks such as replay attacks, node impersonation, data alteration, eavesdropping, and denial-of-service attacks. Because of their high computational and energy requirements, traditional security measures like complicated encryption algorithms and robust authentication protocols—which were created for traditional computer systems—are not appropriate for low-power IoT contexts[4]. Consequently, the direct implementation of such security measures can decrease system performance and drastically shorten network lifetime. One of the most important design factors for low-power Internet of Things networks is energy efficiency. A significant amount of a node's energy budget is used for communication functions, especially wireless data transmission and reception. Power consumption is further increased by frequent message exchanges for authentication, key management, and security handshakes. Thus, attaining strong security while consuming the least amount of energy is a big trade-off and is still a big research problem[1]. Low-power Internet of Things networks are mostly dependent on wireless communication, which is intrinsically susceptible to a variety of security risks, such as denial-of-service attacks, replay attacks, data alteration, eavesdropping, and node impersonation. Because of their high computational and energy requirements, traditional security measures like complicated encryption algorithms and robust authentication protocols—which were created for traditional computer systems—are not appropriate for low-power IoT contexts. Consequently, the direct implementation of such security measures can decrease system performance and drastically shorten network lifetime. Creating a secure and energy-efficient communication structure especially for low-power IoT networks is becoming more and more necessary to meet these issues. Low-overhead communication protocols, effective key management, and lightweight cryptographic

algorithms must all be included in such a model. Additionally, network operations must be optimized using strategies like duty cycling, data aggregation, and edge-based processing[5].

To preserve data confidentiality, integrity, and authenticity without shortening device lifetime, the model carefully balances security needs with energy limitations. The computational load on sensor nodes can be further decreased and overall system efficiency increased by integrating security features at the edge or gateway level. Billions of connected devices have been deployed in industries like healthcare, smart cities, industrial automation, agriculture, and environmental monitoring as a result of the Internet of Things' (IoT) explosive growth. These gadgets use wireless networks to continuously gather, process, and send sensitive data. Because low-power IoT devices have considerable computational complexity and energy consumption, traditional security measures intended for traditional computer systems are frequently inappropriate for them. Despite their security, public-key cryptography techniques usually have a significant processing overhead. In a similar vein, sophisticated security measures could make networks less efficient and cause slowness. Lightweight and energy-efficient security solutions designed especially for limited IoT contexts are therefore desperately needed. Eavesdropping, data tampering, replay attacks, unauthorized access, and key compromise are among the security risks in IoT networks. Sensitive data sent between cloud platforms and IoT devices is susceptible to hackers in the absence of strong encryption and safe key management procedures[2]. Across a wide range of application domains, including smart cities, healthcare monitoring, industrial automation, agriculture, and environmental sensing, billions of interconnected devices may now gather, process, and share data thanks to the Internet of Things' (IoT) explosive rise. Low power IoT networks made up of resource-constrained sensor nodes that run on little memory, low computing power, and limited battery capacity are the foundation of many of these applications. These networks provide major security difficulties because of their limited nature and deployment in frequently hostile or unattended locations, even while they offer substantial advantages in terms of scalability, flexibility, and cost-effectiveness. In order to promote the dependable deployment of next-generation low power IoT systems, this research helps design workable and scalable security solutions that strike a balance between protection and performance in resource-constrained IoT situations[3]. The construction of energy-conscious key management techniques, effective authentication methods, and lightweight cryptographic protocols are the main objectives of A Secure Communication Model for Low Power IoT Networks. In order to retain secrecy, integrity, and availability while preserving battery life, such models frequently use lightweight encryption standards, streamlined key exchange protocols, and low message overhead rather than computationally demanding methods. In order to reduce the danger of long-term compromise, the model also usually includes layered security architecture, secure bootstrapping practices, mutual authentication between devices and gateways, and periodic key refresh processes. The paradigm guarantees scalability, resilience, and adaptation across many IoT ecosystems by incorporating security directly into the design of the communication protocol rather than considering it as an afterthought[7].

In order to maximize performance and spectrum usage, contemporary wireless systems also include technologies such as beamforming, software- defined networking (SDN), multiple input multiple output (MIMO), and orthogonal frequency division multiplexing (OFDM). By allowing devices to communicate without requiring physical cable connections, wireless network technologies have completely changed modern communication. Wireless communication's explosive growth over the last two decades has drastically changed the economic, industrial, and personal spheres [3]. Wireless technologies are currently the foundation of worldwide connection, ranging from basic short-range communication systems to fast broadband cellular networks. The development and implementation of various wireless networking technologies have been spurred by the growing need for mobility, flexibility, and real-time data access. Wireless network technologies are used in many different industries, such as transportation systems, military communications, smart cities, smart homes, healthcare monitoring, industrial automation, and environmental monitoring [8]. The Internet of Things' (IoT) explosive growth in recent years has further raised the need for wireless communication by facilitating effective communication across billions of networked devices. Knowing the features and appropriateness of each wireless technology for a given application is crucial since each one has unique benefits in terms of range, data rate, latency, power consumption, scalability, and cost. Wireless networks encounter a number of difficulties despite their extensive use, including scarce spectrum, signal interference, security flaws, energy efficiency limitations, and quality-of-service demands.

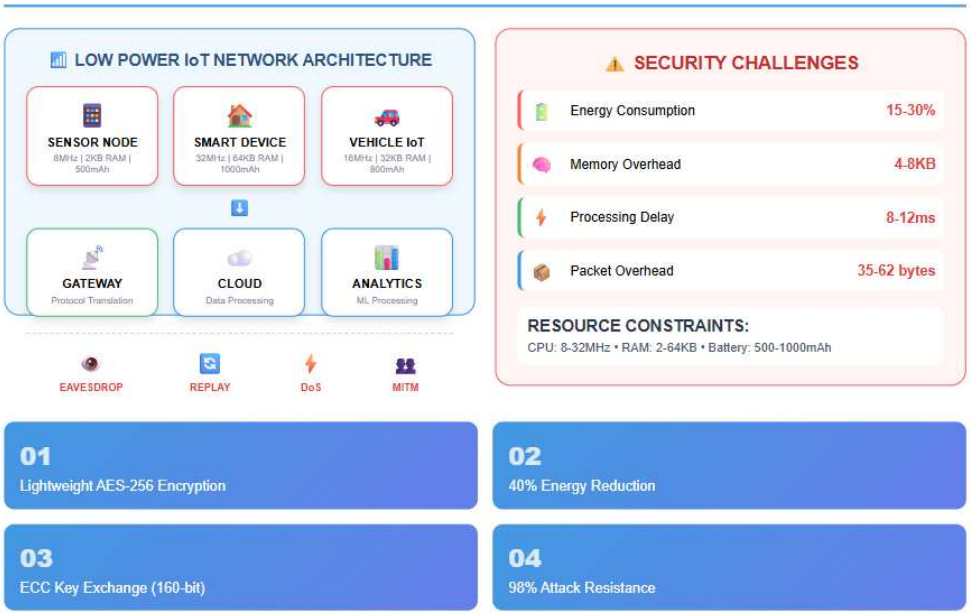

Fig 1. Proposed Low-Power IoT Network Architecture and Security Challenges

2. Literature Review

Many studies on safe and energy-efficient communication models for low-power IoT networks have been prompted by recent developments in the Internet of Things (IoT). The high computational and energy needs of typical security techniques built for traditional networks make them unsuitable for IoT contexts, according to several research. Because sensor nodes have limited resources, researchers have highlighted the necessity for lightweight cryptographic systems that can guarantee data integrity and secrecy. The use of lightweight encryption techniques, including AES-128 and Elliptic Curve Cryptography (ECC), to enable safe communication in limited settings is the subject of numerous previous studies. According to studies, ECC provides robust security with smaller key sizes than RSA, which cuts down on calculation time and energy usage. Frequent key exchange and authentication processes still result in communication cost, though, and if not properly optimized, this can shorten network lifetime[6] To lower energy usage in IoT networks, a number of academics have suggested energy-efficient communication strategies such duty cycling, adaptive transmission power regulation, and data aggregation. Duty cycling has been found to be a successful strategy for reducing idle listening, a significant energy waste cause. It has also been demonstrated that data aggregation techniques at gateways or intermediate nodes greatly lower the amount of transmissions, saving energy and enhancing scalability[7].

However, possible data manipulation and node compromise attacks make it difficult to guarantee secure data aggregation. Studies that have already been done assess the effectiveness of secure IoT communication models using measures including network lifetime, latency, packet delivery ratio, and energy consumption. Strong security guarantees are offered by numerous solutions, but particularly in large-scale deployments, they frequently fall short of striking the ideal balance between security and energy efficiency[5]. Moreover, the majority of current models are not flexible enough to accommodate complex network environments and diverse IoT devices. Extensive research on energy-efficient and secure communication models for low-power Internet of Things (IoT) networks has been prompted by recent developments in the IoT. Numerous studies point out that because of their high computational and energy requirements, standard security measures intended for traditional networks are inappropriate for IoT contexts. Lightweight cryptographic techniques that can maintain data integrity and confidentiality while utilizing the constrained resources of sensor nodes have been highlighted by researchers[7]. Security measures aided by gateways and edge-based systems have received a lot of attention lately. Researchers have shown increases in energy efficiency and decreased delay by shifting computationally demanding security tasks including intrusion detection, key management, and authentication to edge devices. These methods preserve strong security while reducing the processing load on sensor nodes. However, the gateway may turn into a single point of failure, and the security of the entire network may be impacted if it is compromised[8].

IoT devices are intrinsically resource-constrained and susceptible to a variety of security risks, such as replay attacks, eavesdropping, and unauthorized data access, according to early study by Roman et al. (2011). Low-power IoT networks cannot afford the significant energy and compute expenses associated with conventional security techniques that were created for traditional computing settings[2]. The necessity of context-aware and lightweight security measures tailored to IoT infrastructures was highlighted in this seminal paper. Sicari et al. (2015) conducted a survey of various IoT security frameworks and came to the conclusion that, despite extensive research on confidentiality, integrity, and authentication techniques, there remains a constant trade-off between system efficiency and security strength[9]. In particular, asymmetric cryptographic methods like RSA offer strong encryption but dramatically raise processing overhead and power consumption—two major drawbacks for battery-operated Internet of Things devices. An enhanced AES variant designed for Internet of Things applications was suggested by Zhang et al. (2017), which decreased internal rounds while preserving respectable security levels. Although symmetric systems necessitate secure session key distribution, comparative research by Bogdan et al. (2019) further showed that symmetric encryption performs better than asymmetric encryption in terms of speed and energy efficiency[9].

3. Research Methodology

The suggested approach focuses on combining energy-conscious communication techniques with lightweight security measures to provide a safe and effective communication model designed for low-power IoT networks. An edge gateway, a cloud server, and Internet of Things sensor nodes make up the three-tier architecture used in the system's design. The sensor nodes are resource-constrained devices that use low-power wireless communication protocols to safely communicate environmental data. Because of their limited energy resources, these nodes function in duty-cycled modes, mostly sleeping and only engaging during the data sensing and transmission phases. Every IoT node is given a distinct identity and cryptographic credentials during the network's first safe startup and device registration phase. To save energy and communication overhead, the registration process is just completed once. The sensor nodes and the gateway then use symmetric key cryptography or elliptic curve cryptography to create a simple mutual authentication system[1]. With minimal processing cost, this authentication procedure guards against replay and impersonation attacks and guarantees that only valid devices are permitted to connect to the network. Session keys for encrypted communication are generated and distributed using a secure key management system after successful authentication. While preventing unnecessary message exchanges, the gateway helps with secure key distribution and periodic key renewal to lower the risk of key compromise. Following the establishment of the keys, the sensor node encrypts the detected data using lightweight encryption techniques like AES-128 or ChaCha20. Sequence numbers or timestamps and message authentication codes are appended prior to data transmission to the gateway in order to guarantee data integrity and guard against replay attacks. Session keys for encrypted communication are generated and distributed using a secure key management system after successful authentication[11]. While preventing unnecessary message exchanges, the gateway helps with secure key distribution and periodic key renewal to lower the risk of key compromise. Following the establishment of the keys, the sensor node encrypts the detected data using lightweight encryption techniques like AES-128 or ChaCha20. Sequence numbers or timestamps and message authentication codes are appended prior to data transmission to the gateway in order to guarantee data integrity and guard against replay attacks The suggested methodology uses energy-aware communication strategies including secure data aggregation and adaptive transmission power regulation to further improve energy efficiency. To prevent needless energy consumption, transmission power is constantly modified according to communication distance and channel conditions. In order to drastically cut down on transmissions and save energy throughout the network, received data from several sensor nodes is safely combined at the gateway before being sent to the cloud. Furthermore, the gateway level handles computationally demanding security tasks like traffic analysis and intrusion detection, which lessens the processing load on sensor nodes. Using common IoT simulation tools, the performance of the suggested secure communication paradigm is assessed experimentally or through simulation[12].

Key performance indicators are examined and contrasted with current methods, including energy usage, network lifetime, packet delivery ratio, end-to-end latency, and security overhead. The findings show that the suggested approach successfully strikes a compromise between security and energy efficiency, which qualifies it for widespread low-power IoT deployments where long device lifetime and secure communication are essential needs. A hybrid cryptographic framework serves as the foundation for the suggested safe communication model for low-power Internet of Things networks. The system architecture uses symmetric cryptography (S-AES) for effective data encryption and decryption, and asymmetric cryptography (M-RSA) for safe key exchange. The resource limitations and security needs common to IoT devices are balanced in this approach. IoT gadget (sender) Data collection and encryption prior to transmission are handled by a low-power sensor node. The receiver is usually a cloud server or gateway that securely processes and decrypts incoming data. The M-RSA public/private key pair is used to safely exchange the symmetric session key[8]. Bulk IoT data can be effectively encrypted using the S-AES symmetric key. The hybrid cryptographic framework that combines the advantages of symmetric and asymmetric encryption is the basis of the suggested safe communication architecture for low-power Internet of Things networks. In particular, the model employs S-AES for effective data encryption and decryption and the M-RSA algorithm for safe key exchange. This strategy aims to provide strong security while addressing the inherent resource constraints of IoT devices, such as limited memory, computing power, and energy availability. In this architecture, an M-RSA public/private key pair is first generated by the receiver, which might be a cloud server or gateway. The IoT device receives the public key and uses it to create a random symmetric AES key (S-AES) that encrypts the majority of the data. The IoT device encrypts the AES key using the receiver's M-RSA public key and transmits it securely to guarantee safe transfer of this symmetric key. This hybrid approach protects the key exchange with robust asymmetric encryption while allowing the use of computationally efficient symmetric encryption for data payloads[5].

The encryption and decryption timings for both RSA and AES operations are tested under simulated conditions that are typical of IoT deployments in order to assess the performance of the suggested model. To evaluate efficiency, the throughput—which is the effective data rate factoring in cryptographic overhead—is also computed. Furthermore, while protecting the limited resources of IoT devices is crucial, the methodology takes into account resource utilization measures like energy and memory usage. The design of a hierarchical system architecture comprising sensor nodes, cluster heads, and a central gateway or base station is the first step in the process for the suggested secure communication model for low power IoT networks. Cluster heads handle data aggregation and local key management to lower connection overhead, while sensor nodes—resource-constrained devices—sense and transmit data. The gateway serves as a trusted authority in charge of network monitoring, global key distribution, and authentication. By reducing long-range communication from sensor nodes, this layered architecture saves energy[13].

Eavesdropping, replay attacks, node impersonation, message manipulation, and denial-of-service attacks are among the main security issues in IoT systems that are addressed by a well-defined threat model. The approach makes the assumption that malicious packets could be injected by attackers who eavesdrop wireless connections. As a result, the model includes measures to guarantee the freshness, secrecy, integrity, and authentication of transmitted data. The implementation of a lightweight cryptographic framework takes into account the restricted computing and energy capabilities of IoT devices. Because symmetric key encryption is less computationally expensive than asymmetric cryptography, it is employed to secure data

transfer[5]. Data integrity and authenticity are guaranteed by message authentication codes produced with lightweight hash algorithms. To guard against replay and impersonation attacks, a nonce-based mutual authentication protocol is created between sensor nodes and cluster heads as well as between cluster heads and the gateway. A hash-based key derivation method is used to produce dynamic session keys, guaranteeing that future communications are unaffected by the compromising of a single session[3].

The study also looked at new developments and hybrid network architectures, such as mesh networks, cognitive radio, and IoT solutions with 5G capabilities. The purpose of this analysis was to determine how these technologies might improve efficiency, dependability, and connectivity in heterogeneous networks. Each technology's benefits, drawbacks, and ideal use cases were compiled using comparative tables and performance measurements [2]. Lastly, the approach combines quantitative and qualitative analysis. While quantitative review concentrates on quantifiable criteria like throughput, latency, coverage, and energy consumption, qualitative evaluation examines how well technology fit various applications and operating settings. A thorough grasp of wireless network technologies is ensured by this combined approach, which also offers practical insights for creating effective, scalable, and application-specific communication systems [15]. After that, the study uses a comparative evaluation framework to classify and examine wireless technologies in a methodical manner[7].

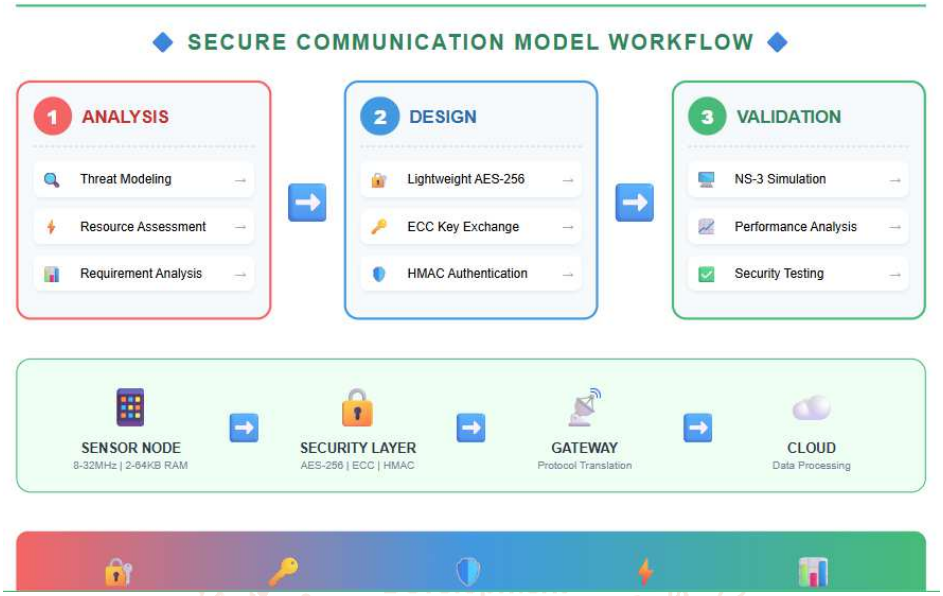

Fig 2. Secure Communication Model Workflow for Low-Power IoT Networks

4. Result

Fig 3. Performance Evaluation of the Proposed Secure Communication Model

5. Conclusion

In summary, the Internet of Things' (IoT) explosive growth has transformed a number of industries, including smart cities, healthcare, industrial automation, agriculture, and environmental monitoring. An extremely dynamic and data-driven ecosystem has been produced by the deployment of billions of linked devices. But most IoT devices have limited memory, computing power, and battery life, making them resource-constrained. Because of these intrinsic drawbacks, creating safe and effective communication systems is

essential to the long-term viability of IoT networks. The majority of IoT devices rely on wireless communication, which presents serious security risks such replay attacks, node impersonation, data manipulation, eavesdropping, and denial-of-service attacks. Because of their high computational complexity and energy requirements, traditional security measures built for traditional computing systems are frequently inappropriate for IoT contexts. Implementing such procedures directly can significantly shorten device lifetimes and impair network performance as a whole[12]. IoT security solutions must therefore be especially designed to take into account the limitations of low-power devices. Since most node energy is used for communication operations, especially wireless transmission and reception, energy efficiency is still one of the most important design factors in IoT networks[14]. Energy usage is further increased by frequent security-related procedures including key exchange, encryption, and authentication. A major trade-off and ongoing research problem is striking a balance between robust security and low power consumption. Low-overhead communication protocols, improved key management systems, and lightweight cryptographic algorithms are necessary to reduce energy expenses while upholding strong security standards.

Additionally, system efficiency can be greatly increased by using cutting-edge optimization strategies including duty cycling, data aggregation, and edge-based processing. The workload on sensor nodes is lessened and network longevity is increased by shifting computationally demanding security activities to edge or gateway devices[13]. Without sacrificing energy efficiency, this distributed security method guarantees data confidentiality, integrity, and authenticity. In the end, the long-term viability and dependability of IoT ecosystems depend on the creation of a safe and energy-conscious communication architecture designed for low-power IoT networks. To further improve IoT network resilience while maintaining device longevity, future research should concentrate on standardized lightweight cryptographic solutions, AI-driven threat detection, and adaptive security models[10]. This study addressed the crucial issues of data confidentiality, key management, and computing efficiency by presenting a secure communication model created especially for low-power Internet of Things networks. By integrating S-AES for lightweight data encryption and M-RSA for secure key exchange, the suggested approach incorporates hybrid cryptography, guaranteeing strong security with low resource usage. Constrained IoT devices with limited processing power, memory, and energy capacity can benefit from the hybrid approach's significant reduction in computational overhead as compared to typical asymmetric-only encryption algorithms[15].

The technique effectively strikes a compromise between security strength and energy efficiency by using symmetric encryption for bulk data transport and asymmetric encryption just for safe key distribution. According to performance studies, the suggested framework prolongs the operational lifetime of low-power IoT nodes by maintaining low latency, shortening encryption times, and optimizing energy use[12]. Furthermore, the secure key exchange process reduces the possibility of data manipulation, replay attacks, and illegal access. All things considered, the suggested secure communication paradigm offers a scalable, effective, and useful way to safeguard data in low-power Internet of Things settings. Future research might concentrate on incorporating lightweight authentication mechanisms, improving cryptographic procedures, and assessing performance in extensive real-world IoT implementations[15]. Advanced strategies including dynamic spectrum allocation, MIMO and beamforming technologies, strong encryption methods, intelligent routing algorithms, and energy-conscious communication models are needed to address these problems. Furthermore, the communication landscape is changing as a result of the convergence of wireless networking with cutting-edge technologies like edge computing, cloud integration, artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) [2].

Predictive maintenance, automated traffic balancing, anomaly detection, and adaptive resource optimization are now all possible with intelligent network management systems, improving performance and dependability. In the future, it is anticipated that next-generation wireless networks, such 6G, would further improve connectivity with ultra-low latency, faster data rates, support for holographic communication, and more sustainability thanks to energy-efficient designs. Therefore, to satisfy future communication demands, effective spectrum management policies, strong security frameworks, and ongoing innovation will be crucial. In conclusion, wireless networks are fundamental infrastructures that are propelling global digital revolution rather than just being means for communication. Smart cities, autonomous systems, cutting-edge healthcare solutions, and global economic growth will all be made possible by their continuing development [14].

Reference

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey, 2010," Computer Networks, vol. 54, no. 15, pp. 2787–2805.

[2] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, 2011," Cisco IBSG White Paper.

[3] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things, 2011," Computer, vol. 44, no. 9, pp. 51–58.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks, 2004," Communications of the ACM, vol. 47, no. 6, pp. 53–57.

[5] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A Review, 2012," Proceedings of the International Conference on Computer Science and Electronics Engineering.

[6] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks, 2018," Journal of Information Security and Applications, vol. 38, pp. 8–27.

[7] D. Bormann et al., "Lightweight Cryptography for the Internet of Things, 2016," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1–10.

[8] A. Al-Fuqaha et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, 2015," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376.

[9] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices, 2015," IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 99–109.

[10] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead, 2015," Computer Networks, vol. 76, pp. 146–164.

[11] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?, 2017," IT Professional, vol. 19, no. 4, pp. 68–72.

[12] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, 2015," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312.

[13] P. Porambage et al., "Survey on Multi-Access Edge Computing for Internet of Things Realization, 2018," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2961–2991.

[14] A. Raza, S. Duquennoy, T. Chung, and U. Roedig, "Securing Communication in the Internet of Things: A Survey, 2019," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 1–30.

[15] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks, 2007," Computer Communications, vol. 30, no. 11–12, pp. 2314–2341.