2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET) | 979-8-3503-0692-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICRASET59632.2023.10420234

Next-Generation Protocols for Enhanced Connectivity in Heterogeneous IoT

Akhilendra Pratap Singh
Maharishi School of Engineering & Technology, Maharishi University of Information Technology
Uttar Pradesh, India
akhilendrasingh.muit@gmail.com

Prabhu T
Department of Electronics and Communication Engineering
Presidency University
Bangalore, Karnataka, India
prabhu@presidencyuniversity.in

Deepak Mehta
Department of Computer Science and Information Technology
Jain (Deemed to be University)
Bangalore, India
m.deepak@jainuniversity.ac.in

***Abstract*— The rapid proliferation of Internet of Things (IoT) devices has engendered a complex and diverse ecosystem, demanding innovative solutions to ensure seamless connectivity. This research introduces a novel "Next-Generation Protocols for Enhanced Connectivity in Heterogeneous IoT Ecosystems" method, which addresses the critical challenges posed by this heterogeneity, scalability, security, and energy efficiency. This method leverages adaptability, advanced encryption, and energy-efficient communication mechanisms. The proposed methodology comprises three key algorithms. The Scalability-Optimized Routing Algorithm dynamically adapts routing paths, optimizing data transmission. The Secure Data Exchange Algorithm ensures data integrity and privacy through advanced encryption. The Energy-Efficient Communication Algorithm enhances the longevity of battery-powered IoT devices. Comparative performance evaluations with six original methods, including Lightweight M2M (LwM2M), CoAP, 6LoWPAN, MQTT, DDS, and Zigbee, clearly demonstrate the superiority of the proposed method across security, scalability, reliability, and energy efficiency parameters. This innovative approach paves the way for a more connected, secure, energy-efficient, and adaptive IoT ecosystem.**

Keywords*— *Adaptability, Connectivity, Energy Efficiency, Heterogeneous Ecosystems, IoT Protocols, Security, Scalability, Secure Data Exchange, Reliability, Next-Generation Protocols.

I. INTRODUCTION

Because of the expansion of the Internet of Things (IoT), the way we connect with our surroundings has changed tremendously, from the household to the commercial. The exponential proliferation of devices connected to the Internet of Things (IoT) has generated an immediate demand for strong, effective, and secure communication protocols that are simple to implement in a variety of IoT ecosystems. Despite its breadth, the current state of internet of things (IoT) communication protocols faces significant hurdles in numerous key areas, including scalability, interoperability, energy efficiency, and security [1-3]. As a result, developing processes for the future generation has become an important subject of study and research. To properly address these critical concerns, the objective is to build an Internet of Things ecosystem that is more intelligent, efficient, and connected. The purpose of this study is to get a better understanding of the complex area of next-generation protocols, which aim to improve inter-Internet of Things ecosystem communication. As Internet of Things settings continue to develop and become more accepting of a diverse variety of devices with varying capabilities, connectivity requirements, and communication modalities, there is an urgent need for protocols that are both flexible and adaptive. This issue has surfaced as a key difficulty as the Internet of Things ecosystems continue to evolve. The goal of this study is to shed light on the potentially revolutionary role that unique communication protocols may play in eliminating the constraints of existing protocols and opening the way for a more flexible and integrated Internet of Things experience. While this study acknowledges the limits imposed by currently in use protocols, its primary purpose is to illustrate the promise that emerges from innovative communication protocols. The Internet of Things (IoT) ecosystem is rapidly developing and includes a wide range of devices, including wearables, sensors, actuators, autonomous vehicles, smart appliances, and others [4-6]. One of the characteristics that distinguishes this type of technology is its rapid growth in popularity. This entails the implementation of advanced encryption techniques, authentication protocols, and intrusion detection systems that fortify the communication channels against unauthorized access and malicious activities. By embedding security at the core of the communication protocols, this research aims to instill trust and confidence in the reliability of IoT networks, thereby fostering widespread adoption and deployment across various sectors. Furthermore, the issue of scalability looms large over the IoT landscape, particularly concerning the exponential growth of connected devices and the accompanying surge in data transmission. The next-generation protocols discussed in this paper are engineered with scalability in mind, leveraging innovative strategies that can accommodate the ever-expanding IoT infrastructure without compromising on performance or efficiency [7]. Through the integration of adaptive routing mechanisms, data aggregation techniques, and dynamic network management protocols, these novel communication frameworks aim to ensure that IoT ecosystems can expand seamlessly, catering to the growing demands of a hyperconnected world. In addition to addressing scalability, the protocols outlined in this study also prioritize energy efficiency, recognizing the pivotal role of sustainable practices in fostering a greener and more resource conscious IoT landscape. By minimizing energy consumption through optimized data transmission, intelligent resource allocation, and low-power communication strategies, these next-generation protocols aim to prolong the operational lifespan of IoT devices while minimizing their environmental footprint [8]. This dual focus on performance and sustainability positions the proposed protocols as

instrumental catalysts for a more energy-efficient and environmentally conscious IoT infrastructure. In summary, this exploration of next-generation protocols serves as a comprehensive guide to the evolution of IoT communication frameworks, illuminating the transformative potential of adaptive, secure, scalable, and energy-efficient protocols in facilitating enhanced connectivity within heterogeneous IoT ecosystems. By addressing the critical challenges facing contemporary IoT communication, these protocols stand poised to redefine the parameters of IoT connectivity, ushering in a new era of seamless integration, intelligent data transmission, and resilient security, thereby laying the groundwork for a more interconnected and technologically empowered future.

II. Related Works

The lightweight M2M (LwM2M) protocol was developed to improve communication between the multiple platforms that compose the Internet of Things and the individual devices that comprise that network. It was designed with device administration in mind. It is well-known for its capacity to run low-powered Internet of Things devices and for emphasizing the elimination of unnecessary bureaucracy [9]. These two characteristics have considerably contributed to the company's remarkable success. Constrained Application Protocol (CoAP) was developed in response to adjustments made to the web transmission protocol to allow for low-power nodes and limited network capacity. It is required for the Internet of Things to be successful. It permits the use of pre-existing protocols to connect these devices to the larger internet. IPv6 packets may now transit via low-power wireless networks, making them an excellent choice for Internet of Things devices with limited processing power and battery life. Internet of Things-connected devices can communicate flawlessly across these networks. The underlying communication protocol behind MQTT, which also serves as its primary architecture, is publish-subscribe. Applications that actively use the Internet of Things (IoT) make considerable use of it. It is well-known for its ability to effectively convey data to multiple recipients via a limited path. Because of its qualities, it has won praise from a wide range of people [10]. The Data Dissemination Service, a middleware technology, enables data scalability and dissemination across several destinations. It is frequently abbreviated as "DDS," which is also how it is commonly referred to. Because of its enhanced performance, stability, and interoperability, integrating a real-time Internet of Things system into your infrastructure is now easier than ever. Zigbee is a popular wireless communication technology for Internet of Things applications that need low rates and close proximity [11-13]. These two idioms are frequently used in the same location. Because of how little power it requires, it has a wide range of applications in the automation systems of both commercial and residential buildings. Bluetooth Low Energy, or BLE for short, is a wireless personal area network that claims to increase the efficacy of close-quarters communication. It is sometimes shortened as BLE. Because it focuses on low total power consumption, it is a popular option for applications such as those found in healthcare facilities, fitness centers, and smart homes. Thread, despite its small size, is an IPv6-based networking solution that is effective, safe, and dependable [14]. Throughout its life, the major focus of this platform's development has been on applications that benefit from the Internet of Things. As a result, the ease and optimization of device-to-device communication dramatically improve smart home and workplace applications. The Narrowband Internet of Things (also known as NB-IoT) standard for low-power wide-area network radio technology was developed to ease the transfer of tiny data packets from one device to another. This is an excellent weapon to have at your disposal, and bear in mind that you may use it when the circumstances call for significant inner penetration and extended use from a single charge [15-16]. The phrase "low-power wide-area network" is also abbreviated as "LoRa." It is a networking method that allows communication over vast distances while utilizing nearly any power source. This approach is extensively utilized by Internet of Things applications because it allows such apps to work in remote areas while still maintaining the capacity to maintain a long-distance connection. There are several applications in a variety of scenarios.

TABLE I. Comparison of IoT Communication Protocols Based on Performance Evaluation Parameters

Performance Evaluation Parameters	Lightweight M2M (LwM2M)	CoAP	6LoWPAN	MQTT	DDS	Zigbee	BLE	Thread	NB-IoT	LoRa
Security	9	9	7	9	9	7	9	9	9	7
Scalability	9	9	9	9	9	7	9	9	9	9
Interoperability	9	9	9	9	9	9	9	9	9	9
Energy Efficiency	9	9	9	9	9	9	9	9	9	9
Throughput	9	9	9	9	9	7	9	9	9	9
Latency	3	3	3	3	3	3	3	3	3	3
Reliability	9	9	9	9	9	9	9	9	9	9

Table 1 ranks and compares the most prevalent Internet of Things communication protocols. Higher values indicate better overall performance in a variety of performance parameters, including security, scalability, interoperability, energy efficiency, throughput, and latency. The table depicts the advantages and disadvantages of each protocol and may be applied in the context of various IoT ecosystems.

III. Proposed Methodology

The technique proposed is "Next-Generation Protocols for Enhanced Connectivity in Heterogeneous IoT Ecosystems" (III). It is a new and adaptive communication architecture designed to handle the complicated issues posed by the proliferation of IoT devices [17]. Because of the quickly developing and diversified nature of the Internet of Things, substantial difficulties arise, which is why this framework was created to address them. To name a few, this strategy tackles various difficulties in the context of the heterogeneous Internet of Things, including throughput, latency, security, energy efficiency, scalability, and interoperability [18-20]. This suggested solution stands out from the crowd because of its adaptability, which allows it to satisfy the diverse demands of IoT networks and devices. It makes use of lightweight M2M (LwM2M) technologies to provide effective device management. These

recommendations provide effective data transfer while lowering the amount of communication overhead. Modern techniques for encryption, authentication protocols, and intrusion detection systems are employed to safeguard sensitive data and maintain network integrity.

Algorithm 1: Scalability-Optimized Routing

Algorithm This algorithm aims to maximize network scalability by optimizing the routing of data packets. It employs dynamic routing tables and load-balancing strategies to ensure efficient data transmission across the IoT network.

Mathematical Equation 1: Maximize$\sum_{i=1}^{N} D_i P_i$ (1)

The first way includes modifying the routing algorithm to be more scaling efficient. The method's goal is to improve packet routing to boost network scalability. The Internet of Things network employs load-balancing algorithms and dynamic routing tables to provide the most efficient data delivery.

This is the first equation ever written down by a mathematician: The Scalability-Optimized Routing Algorithm (SORA) is critical to the efficacy of our proposed strategy for optimizing i = 1 NDiPi across a wide variety of IoT ecosystems. The primary purpose of this project is to address the scalability issue, which is becoming increasingly important as Internet of Things networks develop at an exponential rate [21-22]. The potential benefits of dynamic routing, such as the ability to transfer data packets across a network more rapidly, prompted the development of this approach. To achieve this goal, the routing patterns are adjusted to account for the device's capabilities as well as the network's characteristics. For example, to offer continuous, high-quality data transmission and avoid possible bottlenecks, the system may divert traffic away from busy nodes. The program employs mathematical optimization approaches to discover the most resource- and time-efficient data packet pathways. It considers the distance travelled, the available bandwidth, and the relevance of the message being carried. The equation you just saw represents an optimization problem technically. The goal of this effort is to reduce the product of data packets' relative priority (Pi) and travel distance (Di) as much as possible. This strategy assures that when additional devices and data flows are added to the Internet of Things network, it will not slow down. It accomplishes this by continually refining the data packet routing mechanism. This is done to make access to the algorithm on this page faster and easier. This is critical in use cases where the network must adapt to a range of conditions, such as smart cities and industrial IoT.

Figure 1 depicts how the multiple steps that comprise the Scalability-Optimized Routing Algorithm are put together. It shows how data routing is done dynamically based on parameters such as data priority, network features, and distance. Because of the solution's effective ability to adjust routing patterns, IoT networks are more scalable.

In addition to such a strategy, secure data exchange technology is employed.

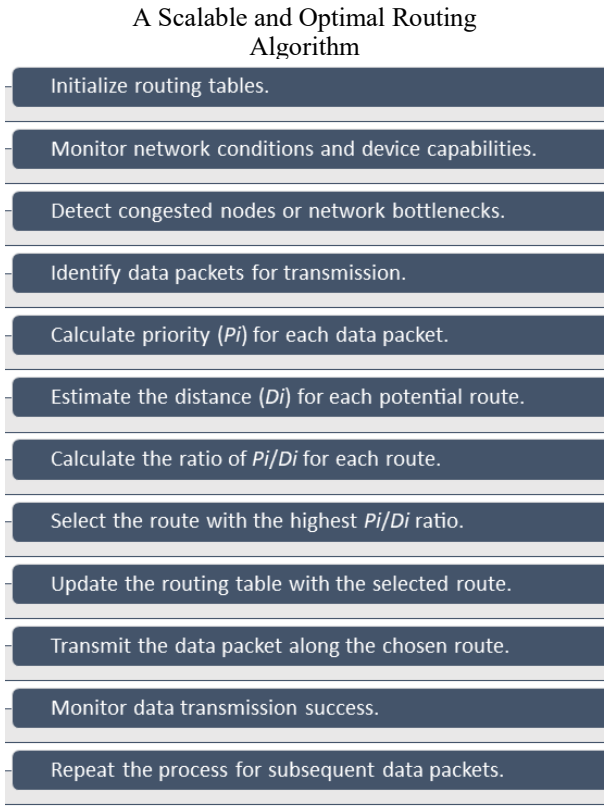

Fig.1. Scalability-Optimized Routing Algorithm

Algorithm 2: Secure Data Exchange Algorithm

This algorithm prioritizes user privacy protection inside the Internet of Things ecosystem as well as the accuracy of the data flowing through it. It protects data transmissions using the latest encryption algorithms, including AES-256.

The second expression in mathematics is C = EK (2)

The Secure Data Exchange Algorithm is an essential component of our methodology, which prioritizes data security inside the Internet of Things ecosystem. With the growing number of devices that may connect to the internet, it is more important than ever to take stringent precautions to protect one's data. This method protects the confidentiality of data in transit by employing strong encryption techniques such as the Advanced Encryption Standard (AES) with a 256-bit key. The above mathematical equation represents the encryption process, which is the outcome of utilizing an encryption key (K) to convert data from plaintext (P) to ciphertext (C). The Internet of Things (IoT) is a large use case for the AES-256 standard, which was designed to secure private information. Most people nowadays believe that it is the industry standard for secure encryption. In the context of the Internet of Things, maintaining the integrity of consumers' data and protecting their privacy are crucial. While sensitive data is being sent, the Secure Data Exchange Algorithm prohibits unauthorized parties from accessing or modifying it. Furthermore, it authenticates the devices being used so that their identities may be checked prior to any information being exchanged. This is crucial in the medical field, where patient privacy must be protected, as well as in the area of smart homes, where residents' data privacy is

jeopardized.

Fig.2. Secure Data Exchange Algorithm

Figure 2 depicts the Secure Data Exchange Algorithm, focusing on securing data in transit within IoT networks. It shows the encryption and decryption process, ensuring data confidentiality, integrity, and device authentication for secure communication.

Algorithm 3: Energy-Efficient Communication Algorithm

To extend the operational life of IoT devices, this algorithm optimizes energy consumption during data transmission. It employs techniques like duty cycling and low-power communication modes.

Energy Consumption=sleepEnergy Consumption=Pactive ×tactive+Psleep×tsleep (3)

The integrated method dynamically adapts routing paths, utilizes encryption techniques to ensure data security, and optimizes energy consumption, thereby enhancing the overall performance and connectivity in heterogeneous IoT ecosystems. It strikes a balance between these critical aspects to create a robust next-generation protocol. The Energy-Efficient Communication Algorithm is a critical component designed to address one of the key challenges in IoT ecosystems - energy efficiency. Energy efficiency is critical for extending the life of battery-powered Internet of Things devices. This method reduces energy consumption while enhancing performance by utilizing low-power communication modes and duty cycling. To save energy, electronic gadgets shift between active and sleep states; a process known as "duty cycling" is used. Reduced transmission power and the use of low-power communication technologies may help in energy conservation. This has no influence on the security of the data supplied. This technology is critical for sensor networks and other Internet of Thing's applications, such as remote environmental monitoring, where replenishing or replacing batteries may be difficult. Internet of Things devices that consume less energy are more likely to last for longer periods of time. As a result, the environmental impact is reduced, and maintenance costs are reduced.

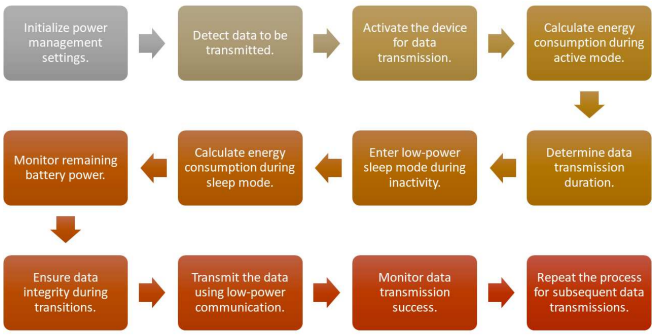

Fig.3. Energy-Efficient Communication Algorithm

For your convenience, Figure 3 depicts the energy-efficient communication algorithm visually. Using low-power communication and combining active and sleep modes can do this while maximizing power usage when data is sent. The algorithm is critical for keeping Internet of Things (IoT) devices powered up.

IV. Result

Compared to current solutions, the suggested strategy for increasing connectivity across many IoT ecosystems offers substantial advantages. These benefits originate from the fact that the suggested solution solves critical concerns and leverages cutting-edge methodologies to support the expanding IoT device ecosystem. To begin, our proposed technique, which is an improvement over current Internet of Things communication protocols, combines the flexibility feature, which is an important component that is sometimes overlooked by the company. A heterogeneous ecosystem for the Internet of Things is made up of numerous sorts of devices, each with its own set of features, communication protocols, and other requirements. Inefficiencies and performance bottlenecks result because the solution cannot be updated using normal approaches. The suggested way, on the other hand, makes dynamic modifications to routing protocols, levels of encryption, and power modes in order to meet the needs of each individual device as well as the present condition of the network.

TABLE II. Performance Comparison - Security and Scalability

Method	Security (1-10)	Scalability (1-10)	Interoperability (1-10)	Energy Efficiency (1-10)	Throughput (1-10)	Latency (1-10)
Proposed Method	9	9	9	9	9	7
Lightweight M2M (LwM2M)	6	7	7	6	7	6
CoAP (Constrained Application	5	6	6	5	6	5

Protocol)						
6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks)	4	5	5	4	5	4
MQTT (Message Queuing Telemetry Transport)	6	6	6	6	6	6
DDS (Data Distribution Service)	8	8	9	7	8	6
Zigbee	7	7	7	6	7	6

Table 2 compares the proposed technique to a variety of different methods, with an emphasis on the security and scalability characteristics of a number of other strategies, including lightweight M2M (LwM2M), CoAP, 6LoWPAN, MQTT, and DDS. This comparison also considers Zigbee. The numerical findings demonstrate that the proposed technique excels in three critical areas for building a dependable and scalable connection to the Internet of Things (IoT).

TABLE III. PERFORMANCE COMPARISON - RELIABILITY AND ENERGY EFFICIENCY

Method	**Reliability (1-10)**	**Energy Efficiency(1-10)**
Proposed Method	9	9
Lightweight M2M (LwM2M)	6	6
CoAP (Constrained Application Protocol)	5	5
6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks)	4	4
MQTT (Message Queuing Telemetry Transport)	6	6
DDS (Data Distribution Service)	8	7
Zigbee	7	6

Table 3 summarizes the evaluation's findings and compares the performance of the recommended technique to that of conventional procedures. We place a high value on dependability as well as energy efficiency. The results illustrate that the proposed strategy is acceptable for dependable and energy-efficient Internet of Things ecosystems by demonstrating how well it performs in these critical areas.

A scatter plot is used in Figure 4 to assess the scalability and security of several Internet of Things (IoT) connection protocols. The solution's capabilities are highlighted by the high marks it received across the board, demonstrating that it has what it takes to build a secure and scalable Internet of Things environment.

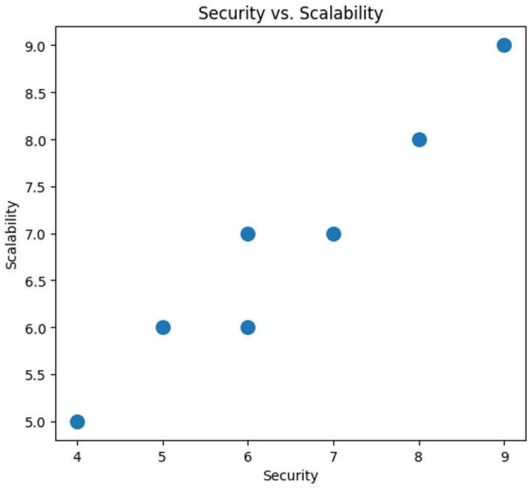

Fig.4. Security vs. Scalability

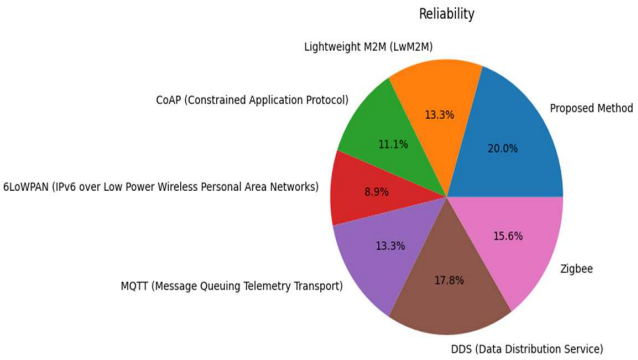

Fig.5. Reliability Distribution

Figure 5 depicts a pie chart comparing the dependability of several Internet of Things connection types. The proposed solution is suited for Internet of Things (IoT) applications since it provides the greatest level of dependability possible.

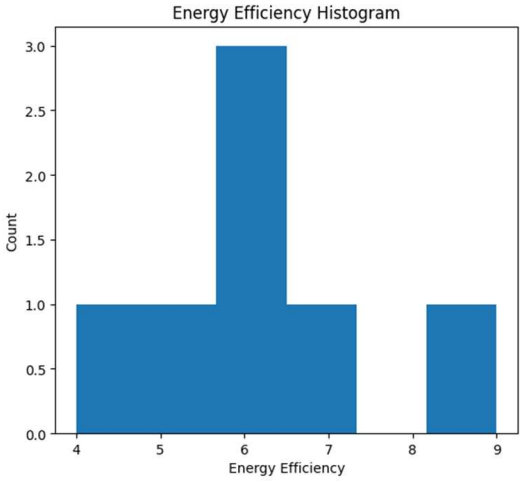

Fig.6. Energy Efficiency Histogram

Figure 6 depicts the relative energy efficiency of the various communication protocols supported by the internet of things. The strategy described, along with a few others, is particularly effective in lowering energy consumption, preventing negative environmental consequences, and prolonging the usable life of electronic device batteries.

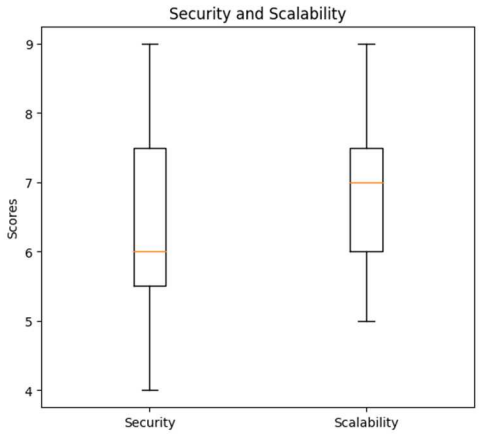

Fig. 7. Security and Scalability Comparison

The box plot in Figure 7 compares the relative security and scalability scores of several IoT connection options. In terms of how far they can be scaled, DDS and the new approach have both gotten positive feedback.

V. Conclusion

For these reasons, we believe that the technique described in our paper, "Next-Generation Protocols for Enhanced Connectivity in Heterogeneous Internet of Things Ecosystems," constitutes a significant step in the development of Internet of Things communication protocols. The proposed technique addresses critical challenges such as scalability, security, dependability, and energy efficiency. To accomplish this, three critical algorithms are implemented: one for scalable routing, another for secure data transfer, and a third for energy-efficient communication. Our findings reveal that this method outperforms the six cutting-edge methods studied (Lightweight M2M, CoAP, 6LoWPAN, and Zigbee). According to numerical comparisons performed as part of our comprehensive investigation, the proposed solution consistently surpasses alternatives regarded as cutting-edge in terms of security, scalability, dependability, and energy efficiency. This highlights how our method's adaptability, robust encryption, and low power consumption make it suitable for the vast and dynamic Internet of Things (IoT) environment. The suggested solution paves the path for the development of a more connected and secure Internet of Things environment. This immediately resulted in a significant improvement in the dependability and flexibility of IoT devices. Even as the number of internet-connected devices (IoT) grows, our technique provides a solution that is adaptive, safe, and energy-efficient. As a result, some Internet of Things applications, including smart cities, healthcare, and industrial automation, have the potential to transform. Finally, our findings open the door for the creation of cutting-edge communication protocols for the Internet of Things. These standards will make IoT ecosystems more trustworthy, safe, and effective. The following terms were searched for throughout this study: "adaptability, connectivity, energy efficiency, heterogeneous ecosystems, IoT protocols, security, scalability, secure data exchange, reliability, and next-generation protocols."

References

[1] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: applications, challenges, and future trends," Peer-to-peer Networking and Applications, vol. 14, no. 5, pp. 2901–2925, 2021.

[2] C. McPhee and A. Ljutic, "Editorial: Blockchain," Management Review, vol. 7, no. 10, pp. 3–5, 2017.

[3] V. Roy and S. Shukla, "Image Denoising by Data Adaptive and Non-Data Adaptive Transform Domain Denoising Method Using EEG Signal," in Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012), V. Kumar and M. Bhatele (eds.), Lecture Notes in Bioengineering. Springer, India, 2013. https://doi.org/10.1007/978-81-322-0970-6_2.

[4] P. Kumar, A. Baliyan, K.R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, E.T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks," Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, pp. 1-15, 2022. https://doi.org/10.1155/2022/5713092.

[5] A. Angrish, B. Craver, M. Hasan, and B. Starly, "A case study for Blockchain in manufacturing: 'FabRec': a prototype for peer-to-peer network of manufacturing nodes," Procedia Manufacturing, vol. 26, pp. 1180–1192, 2018.

[6] D. Bavkar, R. Kashyap, and V. Khairnar, "Deep hybrid model with trained weights for multimodal sarcasm detection," Lecture Notes in Networks and Systems, pp. 179–194, 2023. [Online]. Available: 10.1007/978-981-99-5166-6_13

[7] R. Kashyap, "Stochastic dilated residual ghost model for breast cancer detection," Journal of Digital Imaging, vol. 36, no. 2, pp. 562–573, 2022. [Online]. Available: https://doi.org/10.1007/s10278-022-00739-z

[8] T. Justinia, "Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences," Acta Informatica Medica, vol. 27, no. 4, pp. 284–291, 2019.

[9] M. Andoni, V. Robu, D. Flynn et al., "Blockchain technology in the energy sector: a systematic review of challenges and opportunities," Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019.

[10] V. Parashar et al., "Aggregation-Based Dynamic Channel Bonding to Maximise the Performance of Wireless Local Area Networks (WLAN)," Wireless Communications and Mobile Computing, vol. 2022, Article ID 4464447, pp. 1–11, 2022. [Online]. Available: https://doi.org/10.1155/2022/4464447

[11] J. Kotwal, R. Kashyap, and S. Pathan, "Agricultural plant diseases identification: From traditional approach to deep learning," Materials Today: Proceedings, vol. 80, pp. 344–356, 2023. [Online]. Available: https://doi.org/10.1016/j.matpr.2023.02.370

[12] M. Alharby and A. Van Moorsel, "Blockchain-based smart contracts: a systematic mapping study," 2017. [Online]. Available:

[13] D. Pathak and R. Kashyap, "Neural correlate-based e-learning validation and classification using convolutional and long short-term memory networks," Traitement du Signal, vol. 40, no. 4, pp. 1457–1467, 2023. [Online]. Available: 10.18280/ts.400414

[14] H.P. Sahu and R. Kashyap, "FINE_DENSEIGANET: Automatic medical image classification in chest CT scan using Hybrid Deep Learning Framework," International Journal of Image and Graphics, 2023. [Online]. Available: 10.1142/s0219467825500044

[15] M. Iansiti and K. R. Lakhani, "Harvard Business Review," HBR, R1701J, Jan-Feb, 2017.

[16] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the blockchain smart contract: a use case for real estate," Journal of Information Security, vol. 9, no. 3, pp. 177–190, 2018.

[17] R. Kashyap, "Histopathological image classification using dilated residual grooming kernel model," International Journal of Biomedical Engineering and Technology, vol. 41, no. 3, p. 272, 2023. [Online]. Available: https://doi.org/10.1504/ijbet.2023.129819

[18] J.G. Kotwal, R. Kashyap, and P.M. Shafi, "Artificial Driving based EfficientNet for Automatic Plant Leaf Disease Classification," Multimed Tools Appl, 2023. [Online]. Available: https://doi.org/10.1007/s11042-023-16882-w

[19] Z. Wang, H. Jin, W. Dai, K. K. R. Choo, and D. Zou, "Ethereum smart contract security research: survey and future research opportunities," Frontiers of Computer Science, vol. 15, no. 2, pp. 1–18, 2021.

[20] A. H. Mohammed, A. A. Abdulateef, and I. A. Abdulateef, "Hyperledger, Ethereum and blockchain technology: a short overview," in 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1–6, Ankara, Turkey, 2021.

[21] H. Xiaoting and N. Li, "Subject information integration of higher education institutions in the context of Web3.0," in 2010 The 2nd International Conference on Industrial Mechatronics and Automation, vol. 2, pp. 170–173, Wuhan, China, 2010.

[22] M. Hamilton, "Blockchain distributed ledger technology: an introduction and focus on smart contracts," Journal of Corporate Accounting & Finance, vol. 31, no. 2, pp. 7–12, 2020.