International Journal of Computational and Electronic Aspects in Engineering
Volume 6, Issue 1, March 2025, pp 1-9
https://doi.org/10.26706/ijceae.6.1.20250203

Improving Communication Protocols Based on Crucial Data Transmission Security for IoT Techniques

Azhar W. Talab·

Computer Engineering Department, Northern Technical University, Mosul, Iraq

Corresponding Author: azhar.w@ntu.edu.iq

Abstract: Communication protocols need to be more reliable and efficient since the Internet of Things (IoT) is growing exponentially, changing how devices interact. IoT ecosystems often comprise many devices with varying degrees of processing power, low energy storage, and high network requirements. These elements provide serious obstacles to current communication methods, including latency issues, wasteful bandwidth use, and security flaws. The main goal of this research is to improve communication protocols specifically designed for IoT situations. The suggested improvements seek to solve the shortcomings of conventional protocols by putting adaptive processes, lightweight structures, and cutting-edge security measures into place. The project looks for methods to optimize bandwidth usage, lower latency, and encourage smooth device interoperability. It also emphasizes how crucial data transmission security is to defending against intrusions on IoT.

The research evaluates how well the enhanced protocols work in various IoT contexts using simulations, theoretical analysis, and hands-on testing. The results show how these streamlined protocols could allow for faster information sharing, less consumption of energy, as well as scalable IoT implementations.

Keywords: Communication Protocols; Internet of Things (IoT); Data Security.

RAME PUBLISHERS
INTERNATIONAL JOURNAL OF COMPUTATIONAL AND ELECTRONICS ASPECTS IN ENGINEERING
ISSN: 2395-4116 (PRINT)
ISSN: 2395-4124 (ONLINE)
A Quarterly Publishing Journal

Article – Peer Reviewed
Received: 8 January 2025
Accepted: 20 February 2025
Published: 10 March 2025

Cite this article: Azhar W. Talab, "Improving Communication Protocols Based on Crucial Data Transmission Security for IoT Techniques", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 6, issue 1, pp. 1-9, 2025.
https://doi.org/10.26706/ijceae.6.1.20250203

1. Introduction

The Internet of Things changes technology, enables information sharing more easily, and increases corporate efficiency by connecting networks, devices, and services. As the Internet of Things grows, developing dependable communication protocols is becoming increasingly crucial. Device-to-device data flow must be managed for these protocols to remain reliable, efficient, and secure [1][2].

In this document, the author proposes solutions to enhance communication protocols of IoT systems targeting central issues such as IoT scalability, latency, security, and overall interoperability within the ecosystem. An analysis of a few selected research papers shows the significant developments as well as some challenges being faced. For example, One paper puts forward the issue of the exponential increase of IoT devices and that there is an urgent need for scalable cloud services and emphasizes that it is imperative to adopt fog computing and the fog-to-cloud model as a primary means of devolution of the cloud services to the end users [1][3]. Another study assesses the protocols used in securing IoT applications and notes how Internet security technologies are insufficient for IoT devices with limited capabilities. This illustrates the need for tailored security measures [2].A survey focuses on vulnerabilities in Industrial IoT systems, classifying attacks by IoT architecture layers and exploring robust security solutions tailored to industrial environments [4]. Research comparing various wired and wireless protocols examines their characteristics, benefits, and drawbacks, aiming to identify optimal bidirectional sensor network configurations using devices like Arduino, ESP-12, and Raspberry Pi [5]. An editorial presents a special issue on eight papers related to IoT improvements and several examples of IoT technologies that can transform different fields of study [6].

A second paper investigates a reinforcement learning-based routing protocol to improve data transmission in wireless sensor networks (WSNs). The protocol works on various challenges, like device endurance lives, and reduces energy utilization to enhance networks' lifespan and cover sensors [7]. According to a recent survey on IoT, providing interoperability and security are two vital areas in the development of IoT systems that need further investigation, and establishing international standards for secure communication between heterogeneous IoT entities would help to break through barriers to its implementation [8]. Presented the study on the Internet Engineering Task Force (IETF) protocol suite for high poster in interface between wireless sensor networks and the Internet [9]. Another paper discusses application layer protocols including CoAP, MQTT, XMPP, RESTful services, AMQP, and WebSockets. It evaluates their reliability, security, and application of the IoT applications [10]. This review addresses networking communication technologies with encapsulation and routing protocols. It identifies the issues of interoperability, security, and energy management, and offers a comprehensive taxonomy of IoT network protocols together, these studies emphasize the need for innovation in communication protocols to support IoT's continued growth and success, ensuring secure, efficient, and scalable data exchange in increasingly complex networks [11][12].

2. The Role of Communication Protocols in IoT

The foundation of Internet of Things systems is communication protocols. They make it easier for devices, gateways, and cloud systems to coordinate and exchange data [13] [14]. Popular protocols like MQTT, CoAP, and Zigbee meet a number of needs, such as scalability, low latency, and low power consumption. However, as IoT networks become more sophisticated, improved protocols that can manage more devices and a wider range of applications are required [15] [16].

3. The Role of Communication Protocols in IoT

The IoT is revolutionizing the way devices communicate and, therefore, is introducing major improvements in communication protocols. Such advances are necessary to further improve productivity, enhance connectivity, and develop a wider range of applications in diverse industries. In this scenario, M2M communication, protocols for low power and low bandwidth are two major research areas under consideration [17] [18].

A. Machines-to-Machine Communication

M2M communication is a process where data is transferred directly between devices without human intervention. It acts as the backbone for the internet of things applications, which enables systems to perform tasks automatically and smoothen their operation. M2M communication greatly enhances operational efficiency, reliability, and speed, especially in industries such as manufacturing, healthcare, and transportation [19].

A major advancement in M2M communication is the creation of protocols such as MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol): This lightweight messaging protocol is designed for low-bandwidth, high-latency environments, ma ing it ideal for IoT scenarios. Its publish-subscribe model allows devices to communicate asynchronously, eliminating the need for constant connectivity and optimizing data transmission efficiency [20].

Specifically developed for constrained devices and networks, CoAP adopts a RESTful architecture similar to HTTP but is optimized for IoT environments. It supports small message sizes and low overhead, enabling efficient communication between devices with limited processing power and energy resources [21].

These protocols enable real-time data exchange, essential for remote monitoring, predictive maintenance, and innovative grid management applications. For instance, sensors can interact with machines in a smart factory to optimize production workflows, minimize downtime, and enhance overall efficiency [22].

B. Low Power and Low Bandwidth Protocols

As IoT devices grow, energy-efficient communication protocols become increasingly critical, particularly for battery-powered devices in remote or hard-to-reach areas. Low-power, low-bandwidth protocols are designed to meet these demands, enabling devices to function efficiently while maintaining performance [23]. LoRaWAN (Long Range Wide Area Network) and Sigfox are two prominent protocols used in low-power, wide-area networking.

LoRaWAN: This protocol is designed for long-range communication while consuming very little power, making it perfect for uses such as smart agriculture, environmental monitoring, and asset tracking. Its capability to transmit small data packets over extensive distances allows devices to function for years on a single battery, which greatly lowers maintenance costs and minimizes environmental impact [24] [25].

Sigfox: Following the same principle, Sigfox provides low-power, low-bandwidth communication for Internet of Things devices. It is a low-cost alternative for low data transmission frequency applications, e.g., smart meters or tracking devices. In a narrowband radio frequency, Sigfox uses minimal power compared to satisfactory connectivity [26].

Beyond these protocols, energy-optimizing approaches, including adaptive communications, further enhance power reduction. Regenerate in a single case, the communication rates can be dynamically attenuated on end devices according to the degree of data (i.e., what is to be transmitted). They may resort to low-power-sleep modes to conserve power when not actively running [25].

Testing in an actual environment is a requirement to validate the workout of such low-energy and low-throughput protocols. Heavy trials in different environments help to discover possible sensitivities and then improve performance in different conditions. This guarantees that information can be used predictably to support decision-making in the field [27].

4. Challenges in Existing Protocols

A. Scalability

Nevertheless, most communication protocols in that category are not scalable because of the worldwide deployment of Internet of Things (IoT) networks and the millions of end devices talking among themselves [28]. A significant problem is network overload, packet collisions, and increased latency, which can degrade performance if the number of connected devices increases [29].

B. Interoperability

Since IoT ecosystems are built on interoperable heterogeneous devices from different vendors, seamless communication between heterogeneous networks is required [30]. However, interoperability issues always accompany abnormal structures, a decline in network performance, and the disconnection of continuous device connections [31].

C. Adequately Security

IoT networks are highly susceptible to cyberattacks, such as data breaches and DDoS (Distributed Denial of Service) attacks. The accelerating proliferation of IoT (Internet of Things) networks has posed significant security challenges [32]. If IoT devices are attacked, it can cause a lot of trouble to the device's owner, such as data breaches, malware attacks, and DDoS attacks. These threats turn sensitive user data vulnerable, critical services become disrupted, and even so, lead to massive network breakage. Even with these threats, our current security infrastructures are not robust enough to protect IoT systems from being compromised [33].

D. Energy Efficiency

Battery-powered IoT (Internet of Things) uses low-energy protocols to guarantee a lasting baseline data acquisition [34]. In inefficient protocols, device batteries are drained to the extent of continual failure mode, maintenance costs are raised, and service outages occur [35].

5. Proposed Methodology to Enhance Communication Protocols

A. Adaptive Protocols

Real-time communication protocols that dynamically trade off modulation speed with bandwidth allocation and opportunistic error correction can provide considerable advantages in raising scalability and efficiency [36]. Such adaptive protocols can guarantee robust performance in highly dynamic IoT systems [37].

B. Standardization Efforts

Achieving a high level of interoperability in the field requires universal standards across industries. Standardized protocols minimize fragmentation and allow the combined use of devices from different manufacturers, which promote cross-talk and, in turn, leads to better network efficiency [38].

C. Enhanced Security Measurements

Communication protocols must include state-of-the-art mechanisms, such as end-to-end encryption, high-security authentication, and anomaly detection systems, to mitigate security problems. These properties can reduce the risk of accidental access, data theft, and other cyber attacks [39].

C. Energy Optimization Techniques

Energy-conforming protocols should aim to reduce power usage while maintaining performance [40]. Strategies including adaptive duty cycling sleep modes, and optimized data transfer can more than proportionally extend the lifetime of battery-powered IoT devices, thereby decreasing costs associated with maintenance and system reliability [41].

6. Case Studies and Applications

A. Smart Cities

Smart cities use complex communication protocols to optimize the efficient use of the urban environment, precisely traffic control, waste management, and electric distribution. For example, a flexible MQTT protocol with strengthened security capabilities allows real-time bidirectional data exchange communications between sensors and base stations [42]. It is a heavy and scaleable data exchange, applicable to fast solutions to traffic jam problems, smart waste management, intelligent energy management, etc. Integration of IoT devices and secure protocols may improve operation efficiency and integrate ecological sustainability into operations. They have essential practical usefulness for the evolution of intelligent, adaptive urban ecosystems, which in turn will lead to an increase in the quality of life in future cities since cities will be becoming more prominent and more significant [43] [44].

B. Industrial IoT (IIoT)

This industrializing of IoT as a trend of modern manufacturing is an effective driver of information passive flow between robots, sensors and controllers. Comprehensively, communication protocols play an essential role in delivering a seamless stream of input data, and therefore in operational efficiency [45]. Enhanced versions of the Constrained Application Protocol (CoAP) are best suited to guarantee performance for resources limited industrial applications, e.g. Due to the extreme minimalism of CoAP messaging concerning both weight and efficiency, devices can communicate with each other through very low bandwidth and energy. Such optimization is practical to permit real-time online embedded decision-making, which can lead to efficiency gains and improve innovation and competitive advantages (e.g., manufacturing) [46] [47].

C. Healthcare

Communication between Internet-of-things (IoT) sensors and remote end users, i.e., secure and low round-trip latency communication between IoT sensors and end users for health-care IoT (i.e., They must be reliable to make practical use of useful health information. Recent advances in data encryption schemes are able to offer protection against the disclosure of the patients' latent, private data to unauthorized access, and adaptive communication protocols are also able to dynamically tailor the communication flow according to the availability of network conditions and can deliver high performance in any network condition [48]. These improvements enable better patient experiences and more efficient care delivery. As the use of the Internet of Things (IoT) in healthcare increases, reliable communication security and adaptive communication will still be of great significance to safeguard health and privacy of patients [49][50].

D. Agriculture

IoT devices in agriculture capture critical indicators such as soil conditions, weather, and crop health, allowing farmers to take data-driven approaches to maximize yield and use resources best. Efficient energy communication schemes play an essential role for these systems since they increase the lifetime of deployed sensors in remote or complex conditions [51]. Reduced energy use has the consequence of cost savings and provides a constant flow of data that farmers can better utilize to respond to environmental changes. These advances have resulted in the sustainability and good functioning of agricultural activities and, therefore, sustainable and resilient farming systems [52][53].

7. Emerging Trends in IoT Communication Protocols

A. Edge Computing Integration

The use of edge computing is growing at a feverish pace, and it is central to delivering the ultimate efficiency of the Internet of Things (IoT) application services by offloading the local processing of data sources. Latency, on the other hand, could be very compact, i.e., latency contains as much information as conventional incidences, and thus latency can accelerate decision-making and produce faster responses. In addition, the communication network overhead is reduced by directly optimizing the amount of information that needs to be sent to a central cloud system (i.e., the central system in the center) through the data transmission network [54]. Reliable communication protocols (difference edge-to-cloud) are required to ensure unimpeded communication and information transfer between on-site devices and cloud providers. According to these protocols, valuable information can flow naturally in real-time applications, such as manufacturing, medicine, and smart cities, enhancing this aspect and operational efficiency [55].

B. AI-Driven Protocols

Artificial intelligence (AI)-based communication control is changing how network operations are run by predicting performance and adjusting dynamically. AI refines protocols from traffic analysis to data flow analysis to environmental analysis to enhance efficiency and minimize latency. This dynamic adjustment guarantees a more efficient utilization of the available resources as well as high bandwidth consumption in high-traffic situations such as IoT applications and streaming services [56]. In particular, AI can identify and proactively prevent failure points, making the networks more robust and resilient. Significantly, by further intensifying communication flow, AI-driven protocols substantially increase user experience and performance [57].

C. Blockchain Integration

The combination of blockchain and communication protocols can further secure the IoT, as it offers a decentralized, tamper-resistant architecture for device identity management and transactions. Due to the blockchain's inherent property (i.e., immutability, verity), the data exchange between devices will be verified. It allows safe authentication and authorization of operations and mitigates the risk of data leaks and illegitimate access [58]. By adding data to a network of nodes, blockchain leaves no single points of failure, allowing the system to be resilient. As IoT grows in popularity, blockchain provides a firm solution for the security of private data and trust establishment within interconnected systems [59].

D. The Role of 5G in IoT

The implementation of 5G networks faces a new generation of mobile communications, which, therefore, has low latency and high bandwidth characteristics necessary for intelligent IoT applications [60][61]. The throughput scalability to 100-times the throughput using 4G/5G bandwidth provides low latency, real-time end-to-end transfer of data rates, and the capacity to support high numbers of networked applications, thus generating a tsunami of new applications from applications like smart city, autonomous driving, and telesmdc [62].

Communicative protocols must cope with the higher data throughput and lower latency offered by 5G. Enhanced protocols will ensure efficient data transmission, enabling the delivery of critical information without delays—essential for industrial automation and emergency response systems [63] [64].

In addition, 5G provides, innovative network structures such as network slicing, enabling the development of virtual networks for particular purposes [65]. This is feasible thanks to protocols that allow the dynamic assignment of resources according to real time demand, while at the same time achieving optimal performance for a wide spectrum of application [66][67].

In summary, the widespread adoption of 5G necessitates the evolution of communication protocols to unlock the full potential of IoT applications. This paradigm shift will lead to innovation, more enhanced user experiences, and novel applications in many industries [68][69].

8. Conclusions

The explosive growth of the (IoT) lays its demand for high-performance communication protocols, which are promised to be reliable even for many connected devices. In this work, we highlight the problems in IoT environments, e.g., lack of device resources, high traffic, latency, and security vulnerability, and describe the relevant solutions for these requirements.

The main conclusions point to the need to incorporate adaptive, low-power mechanisms to decrease latency and bandwidth and ensure that data transfer is in real-time and energy minimal. With the installation of holistic secure infrastructures such as deep encryption and intrusion detection mechanisms, IoT networks are protected from cyberattacks. In addition, by employing such protocols, interfacing various types of devices can be achieved, one of the most important aspects driving the growth of IoT ecosystems.

According to the research, there is a strong incentive to strike optimal tradeoffs between efficiency, security, and scalability, which serves as a motivation for subsequent IoT deployments. By selecting the critical factors, the paper helps form smarter and more robust IoT networks that can be utilized in smart cities, industrial automation, healthcare, agriculture, and other areas.

With the broader deployment of IoT by many IoT users, the data and trends in this work shall play an important role in communication protocol design for future IoT systems. These advances will drive, enable, and innovate and are not just intrinsic to device connectivity by nature. In turn, they will provide new opportunities for IoT and disruptive applications in all industries.

References

[1] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration," ACM Computing Surveys, vol. 1, no. 1, pp. 1-30, Feb. 2019. doi: 10.1155/2018/5349894.

[2] Mohammed Fareed Mahdi,” Revolutionizing the Future Investigating the Role of Smart Devices In IOT” International Journal of Computational and Electronic Aspects in Engineering, VOL.5 Issue.1January 2024, pp 1-15

[3] M. K. Hasan, Z. Weichen, N. Safie, F. R. A. Ahmed, and T. M. Ghazal, "A Survey on Key Agreement and Authentication Protocol for Internet of Things Application," IEEE Access, vol. 12, pp. 61642-61661, Apr. 2024. doi: 10.1109/ACCESS.2024.3393567.

[4] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications," Sensors, vol. 21, no. 11, p. 3654, May 2021. doi: 10.3390/s21113654.

[5] Glória, F. Cercas, and N. Souto, "Comparison of Communication Protocols for Low Cost Internet of Things Devices," in Proceedings of the SEEDA-CECNSM Conference, Lisbon, Portugal, Sept. 2017. doi: 10.23919/SEEDA-CECNSM.2017.8088226.

[6] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities," International Journal of Communication Systems, vol. 25, no. 10, pp. 1101-1102, Dec. 2012. doi: 10.1002/dac.2417.

[7] S. Bhimshetty and V. I. Agughasi, "Energy-efficient deep Q-network: reinforcement learning for efficient routing protocol in wireless internet of things," Indonesian Journal of Electrical Engineering and Computer Science, vol. 33, no. 2, pp. 971-980, Feb. 2024. doi: 10.11591/ijeecs.v33.i2.pp971-980.

[8] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1020-1045, Feb

[9] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities," IEEE Wireless Communications, vol. 20, no. 6, pp. 91-98, Dec. 2013. doi: 10.1109/MWC.2013.6700124.

[10] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A Survey on Application Layer Protocols for the Internet of Things," International Journal of Communication Systems, vol. 25, no. 10, pp. 1101-1102, Dec. 2012. doi: 10.1002/dac.2417.

[11] Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends," Wireless Communications and Mobile Computing, vol. 2018, Article ID 5349894, 2018. doi: 10.1155/2018/5349894.

[12] Varga, P., Blomstedt, F., Ferreira, L. L., & Eliasson, J. (2017). Making system of systems interoperable—The core components of the Arrowhead Framework. *Journal of Network and Computer Applications*, 81, 85-95.

[13] Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing*, 16(2), 62-67.

[14] Sye Loong Keoh, Sandeep S. Kumar, et al. (2014). Lightweight security solutions for the Internet of Things: A standardization perspective. *IEEE Internet of Things Journal*, 1(2), 99-112.

[15] Banks, A., & Gupta, R. (2014). MQTT Version 3.1.1. *OASIS Standard*. Retrieved from https://mqtt.org.

[16] Ibarra-Esquer, J. E., et al. (2017). IoT for global development to achieve the United Nations Sustainable Development Goals: The IoT taxonomies. *IEEE Access*, 4, 3668-3679.

[17] Chen, J., & Kunz, T. (2016). Performance evaluation of IoT protocols under a constrained wireless access network. *2016 International Conference on Selected Topics in Mobile and Wireless Networking*.

[18] Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N., & Kantzavelou, I. (2022). IoT: Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*, *3*, 1-13. https://doi.org/10.1016/j.iotcps.2022.12.003

[19] Li, C., Wang, J., Wang, S., & Zhang, Y. (2024). A review of IoT applications in healthcare. Neurocomputing, 565, 127017. https://doi.org/10.1016/j.neucom.2023.127017

[20] Seoane, V., Garcia-Rubio, C., Almenares, F., & Campo, C. (2021). Performance evaluation of CoAP and MQTT with security support for IoT environments. *Computer Networks*, *197*, 108338. https://doi.org/10.1016/j.comnet.2021.108338

[21] Tariq, M. A., Khan, M., Raza Khan, M. T., & Kim, D. (2019). Enhancements and Challenges in CoAP—A Survey. *Sensors*, *20*(21), 6391. https://doi.org/10.3390/s20216391

[22] Bayılmış, C., Ebleme, M. A., Çavuşoğlu, Ü., Küçük, K., & Sevin, A. (2022). A survey on communication protocols and performance evaluations for Internet of Things. *Digital Communications and Networks*, *8*(6), 1094-1104. https://doi.org/10.1016/j.dcan.2022.03.013

[23] Aldin, H. N. S., Ghods, M. R., Nayebipour, F., & Torshiz, M. N. (2023). A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology. *Sensors International*, *5*, 100258. https://doi.org/10.1016/j.sintl.2023.100258

[24] Stanco, G., Navarro, A., Frattini, F., Ventre, G., & Botta, A. (2024). A comprehensive survey on the security of low power wide area networks for the Internet of Things. *ICT Express*, *10*(3), 519-552. https://doi.org/10.1016/j.icte.2024.03.003

[25] Safi, H., Jehangiri, A. I., Ahmad, Z., Alramli, O. I., & Algarni, A. (2024). Design and Evaluation of a Low-Power Wide-Area Network (LPWAN)-Based Emergency Response System for Individuals with Special Needs in Smart Buildings. *Sensors (Basel, Switzerland)*, *24*(11), 3433. https://doi.org/10.3390/s24113433

[26] Alqurashi, H., Bouabdallah, F., & Khairullah, E. (2022). SCAP SigFox: A Scalable Communication Protocol for Low-Power Wide-Area IoT Networks. *Sensors*, *23*(7), 3732. https://doi.org/10.3390/s23073732

[27] Bakare, M. S., Abdulkarim, A., Shuaibu, A. N., & Muhamad, M. M. (2024). Energy management controllers: Strategies, coordination, and applications. *Energy Informatics*, *7*(1), 1-37. https://doi.org/10.1186/s42162-024-00357-9

[28] Lamport, L., Shostak, R., & Pease, M. (1982). "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems*, 4(3), 382-401.

[29] Al-Fares, M., Loukissas, A., & Vahdat, A. (2008). "A Scalable, Commodity Data Center Network Architecture." *ACM SIGCOMM Computer Communication Review*, 38(4), 63-74.

[30] Dimitri Belli, Paolo Barsocchi, Filippo Palumbo "A meta modeling-based interoperability and integration testing platform for IoT systems," Journal Name, vol. x, no. y, pp. xx-xx, Year

[31] Amir Torab-Miandoab, Taha Samad-Soltani, Ahmadreza Jodati, Peyman Rezaei "Interoperability of heterogeneous health information systems: a systematic literature review," BMC Medical Informatics and Decision Making, vol. 23, no. 18, 2023

[32] Miorandi, D., Sicari, S., Pellegrini, P., & Chlamtac, I. (2012). "Internet of Things: Vision, Applications and Research Challenges." Ad Hoc Networks, 10(7), 1497-1516.

[33] Sadeghi, A., Wachsmann, C., & Waidner, M. (2015). "Security and Privacy Challenges in Industrial Internet of Things." 2015 8th International Conference on the Network of the Future (NoF), 1-6.

[34] H. N. S. Aldin, M. R. Ghods, F. Nayebipour, and M. N. Torshiz, "A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology," Sensors International, vol. 5, p. 100258, Jan. 2024, doi: 10.1016/j.sintl.2023.100258.

[35] M. H. Alsharif, A. H. Kelechi, A. Jahid, R. Kannadasan, M. K. Singla, J. Gupta, and Z. W. Geem, "A comprehensive survey of energy-efficient computing to enable sustainable massive IoT networks," Alexandria Engineering Journal, vol. 91, pp. 12-29, Mar. 2024, doi: 10.1016/j.aej.2024.01.067.

[36] M. H. Alsharif, A. H. Kelechi, A. Jahid, R. Kannadasan, M. K. Singla, J. Gupta, and Z. W. Geem, "A comprehensive survey of energy-efficient computing to enable sustainable massive IoT networks," *Alexandria Engineering Journal*, vol. 91, pp. 12-29, Mar. 2024, doi: 10.1016/j.aej.2024.01.067.

[37] Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, "A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook," *Computer Networks*, vol. 202, p. 109-123, 2022, doi: 10.1016/j.comnet.2022.109123.

[38] Sabina Szymoniak, Sabina Szymoniak, Sabina Szymoniak "Defense and Security Mechanisms in the Internet of Things: A Review," Open Access, 7 January 2025

[39] Shahid Allah Bakhsh , Muhammad Almas Khan , Fawad Ahmed a, Mohammed S. Alshehri , Hisham Ali , Jawad Ahmad "Enhancing IoT Network Security Through Deep Learning-Powered Intrusion Detection System," *Open Access*, vol. 24, December 2023

[40] Stallings, W. Data and Computer Communications. Pearson Education. (2021).

[41] Iyengar, M Thomson, RFC 9000: "QUIC: A UDP-Based Multiplexed and Secure Transport Protocol" 2070-172, March 2021, IETF.

[42] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." SIAM Journal on Computing.

[43] Alotaibi, N. S., Sayed Ahmed, H. I., M Kamel, S. O., & ElKabbany, G. F. (2024). Secure Enhancement for MQTT Protocol Using Distributed Machine Learning Framework. *Sensors (Basel, Switzerland)*, *24*(5), 1638. https://doi.org/10.3390/s24051638

[44] M. Houichi, A. Ben Saad, and A. Al-Mamary, "Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach," *Computers, Materials & Continua*, vol. 81, no. 1, pp. 393-441, Oct. 2024. doi: 10.32604/cmc.2024.054007.

[45] Farooq, M. S., Abdullah, M., Riaz, S., Alvi, A., Rustam, F., Flores, M. A., Galán, J. C., Samad, M. A., & Ashraf, I. (2022). A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry. *Sensors*, *23*(21), 8958. https://doi.org/10.3390/s23218958

[46] Latif, S., Driss, M., Boulila, W., Jamal, S. S., Idrees, Z., & Ahmad, J. (2021). Deep Learning for the Industrial Internet of Things (IIoT): A Comprehensive Survey of Techniques, Implementation Frameworks, Potential Applications, and Future Directions. Sensors (Basel, Switzerland), 21(22), 7518. https://doi.org/10.3390/s21227518

[47] Zahoor, S., & Mir, R. N. (2021). Resource management in pervasive Internet of Things: A survey. *Journal of King Saud University - Computer and Information Sciences*, *33*(8), 921-935. https://doi.org/10.1016/j.jksuci.2018.08.014

[48] Li, C., Wang, J., Wang, S., & Zhang, Y. (2024). A review of IoT applications in healthcare. *Neurocomputing*, *565*, 127017. https://doi.org/10.1016/j.neucom.2023.127017

[49] Abdulmalek, S., Nasir, A., Jabbar, W. A., M Almuhaya, M. A., Bairagi, A. K., Al-Masrur Khan, M., & Kee, H. (2022). IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. Healthcare, 10(10), 1993. https://doi.org/10.3390/healthcare10101993

[50] Pradip Balbudhe, Disha Sune, Manjiri Kapkar, Shivani Meshram, Vidya Kaikade, Swati panse." Internet of Things (IoT) Based Smart Health Monitoring System – A Case Study" International Journal of Computational and Electronic Aspects in Engineering. Volume 2: Issue 3, August 2021, pp 91-96

[51] Rajak, P., Ganguly, A., Adhikary, S., & Bhattacharya, S. (2023). Internet of Things and smart sensors in agriculture: Scopes and challenges. *Journal of Agriculture and Food Research*, *14*, 100776. https://doi.org/10.1016/j.jafr.2023.100776

[52] Akhter, R., & Sofi, S. A. (2022). Precision agriculture using IoT data analytics and machine learning. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5602-5618. https://doi.org/10.1016/j.jksuci.2021.05.013

[53] Rohini Pochhi, Sandeep Thakre, Balwant Bansod" Using wireless sensor network for monitoring and controlling of farm" International Journal of Computational and Electronic Aspects in Engineering. Volume 2: Issue 1, March 2021, pp 22-25

[54] Al-Dulaimy, Y. Sharma, M. G. Khan, and J. Taheri, "Introduction to Edge Computing," in *Edge Computing: Models, Technologies and Applications*, June 2020. [Online]. Available: http://www.es.mdu.se/publications/6093-

[55] Ergen, M., Saoud, B., Shayea, I., El-Saleh, A. A., Ergen, O., Inan, F., & Tuysuz, M. F. (2024). Edge computing in future wireless networks: A comprehensive evaluation and vision for 6G and beyond. *ICT Express*, *10*(5), 1151-1173. https://doi.org/10.1016/j.icte.2024.08.007

[56] Mohammed ELHajj. Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions. *Network*, *5*(1), 1. https://doi.org/10.3390/network5010001

[57] Mata, J., De Miguel, I., Durán, R. J., Merayo, N., Singh, S. K., Jukan, A., & Chamania, M. (2018). Artificial intelligence (AI) methods in optical networks: A comprehensive survey. *Optical Switching and Networking*, *28*, 43-57. https://doi.org/10.1016/j.osn.2017.12.006

[58] Almarri, S., & Aljughaiman, A. (2023). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, *16*(23), 10177. https://doi.org/10.3390/su162310177

[59] Rai, H. M., Shukla, K. K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. *Heliyon*, *10*(19), e38917. https://doi.org/10.1016/j.heliyon.2024.e38917

[60] Pons, M., Valenzuela, E., Rodríguez, B., & Arturo, J. (2022). Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review. *Sensors*, *23*(8), 3876. https://doi.org/10.3390/s23083876

[61] Salar Jamal Rashid, Ahmed Maamoon Alkababji & AbdulSattar Mohammed Khidhir(2021). ‘Communication and Network Technologies of IoT in Smart Building: A Survey ‘,NTU JOURNAL OF ENGINEERING AND TECHNOLOGY. E-ISSN:2788-998X.

[62] Mazurczyk, W., Bisson, P., Jover, R. P., Nakao, K., & Cabaj, K. (2020). Special issue on Advancements in 5G Networks Security. *Future Generation Computer Systems*, *110*, 314-316. https://doi.org/10.1016/j.future.2020.04.043

[63] Attaran, M. (2021). The impact of 5G on the evolution of intelligent automation and industry digitization. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 5977. https://doi.org/10.1007/s12652-020-02521-x

[64] Dangi, R., Lalwani, P., Choudhary, G., You, I., & Pau, G. (2021). Study and Investigation on 5G Technology: A Systematic Review. *Sensors (Basel, Switzerland)*, *22*(1), 26. https://doi.org/10.3390/s22010026

[65] Jain, H., Chamola, V., & Jain, Y. (2020). 5G network slice for digital real-time healthcare system powered by network data analytics. *Internet of Things and Cyber-Physical Systems*, *1*, 14-21. https://doi.org/10.1016/j.iotcps.2021.12.001

[66] Zahoor, S., Ahmad, I., Ben Othman, M. T., Mamoon, A., Rehman, A. U., Shafiq, M., & Hamam, H. (2022). Comprehensive Analysis of Network Slicing for the Developing Commercial Needs and Networking Challenges. *Sensors (Basel, Switzerland)*, *22*(17), 6623. https://doi.org/10.3390/s22176623

[67] Alhakam Ayad Salih” Improved Security and Handover Technique in (4G) LTE” International Journal of Computational and Electronic Aspects in Engineering. Volume 3: Issue 4, December 2022, pp 76-83

[68] Dangi, R., Jadhav, A., Choudhary, G., Dragoni, N., Mishra, M. K., & Lalwani, P. (2022). ML-Based 5G Network Slicing Security: A Comprehensive Survey. *Future Internet*, *14*(4), 116. https://doi.org/10.3390/fi14040116

[69] Abhita Gokhale, Labdhi Gada, Kolambi Narula, Amol Jogalekar" Software Defined Networking Towards 5G Network "International Journal of Computational and Electronic Aspects in Engineering. Volume 4: Issue 3, July-September 2023, pp 68-77