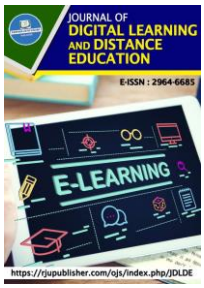

JOURNAL OF DIGITAL LEARNING AND DISTANCE EDUCATION (JDLDE)

ISSN: 2964-6685

https://www.rjupublisher.com/ojs/index.php/JDLDE

Internet of Things (IoT) Data Communication Challenges, and Solutions

Solomon Makasda DICKSON[a*] and Ijeoma Peace OKECHUKWU[a]

[a]*Department of Computer Science, National Institute for Nigerian Languages, Aba, Abia State, Nigeria*

*Corresponding author: dicksonsolomon1988@gmail.com

Abstract

IoT has become an integral part of our lives and data communication is one of the most important aspects of IoT. IoT devices can exchange data with each other via secure communication channels. This study aimed to review the IoT data communication challenges and solutions This paper attempts to address the key challenges and solutions for effective IoT data communication, starting by exploring the current challenges of IoT data communication related to scalability, reliability, and security, potential solutions to these challenges such as using a mesh network, centralized servers, and edge computing. In addition, the paper discusses the importance of proper authentication and authorization techniques to ensure secure communication between IoT devices. The potential of IoT data communication is vast and has the power to fundamentally transform our society. It is an exciting time to be involved in this field, and the future looks promising for the advancement of IoT data communication.

Keywords**:** Data, Potential, Communication, and Internet of Things

Acknowledgments: Thanks to all parties who have supported the implementation of this research. I hope this research can be useful.

For citation:
Dickson, S. M., & Okechukwu, I. P. (2024). Internet of Things (IoT) Data Communication Challenges, and Solutions. *Journal of Digital Learning and Distance Education, 2*(11), 803-808. https://doi.org/10.56778/jdlde.v2i11.226.

Introduction

In recent years, the Internet of Things (IoT) has emerged as a game-changing technology, with the potential to transform the way we live, work, and communicate (Radouan Ait Mouha, 2021); (Rejeb et al., 2024). IoT devices are constantly generating massive amounts of data, creating new opportunities for communication and data sharing (C. Li et al., 2024). This has led to a growing

interest in the development of efficient and effective methods for IoT data communication. As the use of IoT devices continues to grow, it has become essential for researchers and academics to explore the potential of IoT data communication and its impact on various industries. By analyzing and interpreting this data, researchers can gain valuable insights into consumer behavior, improve decision-making processes, and develop innovative solutions to real-world problems. Researchers are actively working towards addressing these challenges and ensuring that the potential of IoT data communication can be fully realized without compromising user data. From smart homes to self-driving cars, the potential applications of IoT data communication are endless. As technology continues to advance, academics must stay up-to-date with the latest developments and contribute to the growing body of knowledge in this field. This data has the potential to transform various industries and provide valuable insights. However, effective communication of this data is crucial to fully harness its potential. (Alaba et al., 2017).

The problem of IoT data communication has been a major challenge in the field of computer science in recent years. The increasing use of IoT devices has led to a vast amount of data being generated, making it difficult for traditional communication methods to effectively handle. This has resulted in issues such as slow data transfer, high latency, and data loss. This has led to challenges in data transmission, storage, and security. To address these challenges, various solutions have been proposed, including mesh networks, centralized servers, and edge computing.

This study aimed to review the IoT data communication challenges and solutions. The study sought to:

i. challenges and practicality of IoT data communication
ii. potential solutions as related to challenges of IoT data communication
iii. techniques of IoT data communication

Methodology

The V Model is a software development and testing methodology that emphasizes a structured approach to the development process. When applied to Internet of Things (IoT) Data Communication the V Model can be effectively utilized to address the unique complexities associated with securing interconnected devices.

Results and Discussion

Challenges of IoT data communication

The Internet of Things (IoT) has seen massive growth in recent years, revolutionizing the way we interact with technology. However, with this growth comes new challenges in the realm of data communication. As more and more devices become connected, the practicality of managing and analyzing the vast amounts of data generated by these devices becomes a major concern. This can lead to issues such as scalability, reliability, and security. These solutions include mesh networks, centralized servers, and edge computing. By continuously improving and implementing these solutions, we can ensure the practicality of IoT data communication and fully harness the potential of the IoT for various industries and applications.

Lack of Scalability: An increasing number of Internet of Things (IoT) devices have resulted in a significant amount of data being generated, making the scalability of data communication a major concern (Subrahmanyam et al., 2023); (Alsboui et al., 2021); (Tawalbeh et al., 2020). The current methods of data communication are unable to handle the sheer volume of data, leading to slow and inefficient processes. This has become a major hindrance in the development and utilization of IoT technology. However, the current data communication methods used in IoT systems lack scalability, which results in a bottleneck in data transmission. This hinders the performance of the system and limits its ability to handle a large number of devices ((Taye, 2023). Lack of Reliability: The lack of

reliability in IoT data communication has been a major challenge faced by researchers and practitioners alike. This issue has been a barrier to the widespread adoption of IoT technology in various industries. Lack of Security: This data communication presents a major security concern as sensitive information can easily be accessed by unauthorized parties. The various IoT environments, make it a practical and efficient solution to the lack of security in IoT data communication (Leloglu, 2017). The lack of security in IoT data communication is a complex issue with various factors contributing to it. These include the vulnerability of devices, the lack of standardization in security protocols, and the increasing sophistication of cyber-attacks. As such, it requires a multi-faceted approach to address this problem (Mishra et al., 2022).

Potential Solutions to These Challenges of IoT Data Communication

The solutions to the challenges of IoT data communication. It first analyzes the challenges in detail, such as bandwidth limitations, security concerns, and data reliability issues. Then, it proposes novel solutions to address these challenges, including significant improvement in the overall performance and scalability of IoT data communication, enhancing the efficiency and reliability of data communication in IoT systems, and implementing edge computing. A mesh network: A mesh network is a type of networking topology where each node is connected to multiple other nodes, creating a decentralized and redundant network. In the context of IoT data communication, a mesh network offers several advantages. Since each node can act as a router, it allows for wider coverage and avoids single points of failure. Additionally, a mesh network can dynamically route data through different paths, increasing the efficiency and reliability of data transmission (Zuo et al., 2013); (Ploumidis et al., 2015); (Cao et al., 2022). A mesh network, also known as a sensor network, is a type of network that is widely used in the field of IoT data communication (Escola et al., 2022); . It consists of a large number of interconnected devices, such as sensors and nodes, that work together to collect and transmit data.

Mesh networks are becoming increasingly popular due to their ability to provide reliable and efficient communication in IoT applications. One of the key advantages of mesh networks is their self-organizing capability. This means that the devices within the network can communicate with each other without the need for a central hub or router. Each device acts as a node, relaying data to other devices, ensuring that the entire network is connected. This makes mesh networks highly resilient and able to adapt to changes in the environment. Another advantage of mesh networks is their ability to cover large areas. Traditional wireless networks, such as Wi-Fi, have limitations in terms of range, making them unsuitable for large-scale IoT applications. However, with mesh networks, devices can communicate with each other over long distances, making them ideal for smart city projects and other applications that require extensive coverage (Kanellopoulos et al., 2023). Centralized servers: Centralized servers have become a popular solution for managing the vast amount of data generated by IoT devices. These servers act as a central hub for communication, storing, and processing data from multiple sources. By utilizing a centralized server, IoT data can be accessed, analyzed, and shared in a more organized and efficient manner. The implementation of centralized servers in IoT data communication has proven to be highly beneficial. It allows for faster and more reliable data transmission, as well as improved data security.

As IoT technology continues to advance, the use of centralized servers in data communication is only expected to increase. By utilizing this method, the vast amount of data generated by IoT devices can be effectively managed, allowing for more efficiency and accuracy in various fields (Soori et al., 2023). Edge computing: Edge computing is a method of processing data near the source, instead of sending it to a centralized location for processing. This method has gained popularity in the context of Internet of Things (IoT) data communication. In this scenario, IoT devices collect vast amounts of data that need to be processed and analyzed promptly. By utilizing edge computing, data can be processed and analyzed locally, significantly reducing the delay in communication and improving the efficiency of data processing. This has numerous benefits, such as

reducing network congestion, improving security, and enabling real-time decision-making. Overall, edge computing plays a crucial role in enhancing the capabilities of IoT data communication and has the potential to revolutionize the way we handle data in various academic fields.

The importance of proper authentication and authorization techniques to ensure secure communication between IoT devices

The use of proper authentication and authorization techniques is essential in ensuring secure communication. These techniques help to verify the identity of users and restrict access to sensitive information. By implementing these techniques, organizations can prevent unauthorized access to their systems and protect their data from potential threats. Additionally, proper authentication and authorization techniques also help to maintain the confidentiality, integrity, and availability of information. With the ever-increasing risks of cyber-attacks, organizations must prioritize the implementation of these techniques to secure their communication and protect their assets. Techniques to ensure the security of their communication (Rao & Nayak, 2014).

Authentication is the process of verifying the identity of an individual or entity using credentials, such as usernames and passwords. By requiring individuals to provide this information, institutions can ensure that only authorized individuals have access to sensitive information. This not only protects the data from unauthorized access but also helps to maintain the integrity and credibility of the communication (Y. Li & Liu, 2021); (Shojaei et al., 2024). Authorization, on the other hand, refers to the process of determining what actions an individual or entity is allowed to perform within a system. This can include reading, writing, modifying, or deleting data. By implementing proper authorization techniques, institutions can ensure that only authorized individuals have the necessary permissions to perform specific actions. This is important in maintaining the confidentiality, availability, and integrity of the information being communicated. The importance of proper authentication and authorization techniques in ensuring secure communication between Internet of Things (IoT) devices. The growing popularity and use of IoT devices have made them a prime target for cyber-attacks, making it crucial for proper security measures to be in place, various authentication and authorization techniques, and their effectiveness in securing IoT devices (Aziz Al Kabir et al., 2023); (Williams et al., 2022)

Conclusion

In conclusion, this paper provides a comprehensive overview of the current challenges and solutions related to IoT data communication. By understanding these challenges and solutions, developers can create robust and secure communication systems for various IoT applications. The potential of IoT data communication is vast and has the power to fundamentally transform our society. It is an exciting time to be involved in this field, and the future looks promising for the advancement of IoT data communication.

Conflicts of Interest

The authors declare no conflict of interest.

References:

Alsboui, T., Qin, Y., Hill, R., & Al-Aqrabi, H. (2021). Distributed Intelligence in the Internet of Things: Challenges and Opportunities. *SN Computer Science*, *2*(4), 277. https://doi.org/10.1007/s42979-021-00677-7

Aziz Al Kabir, M., Elmedany, W., & Sharif, M. S. (2023). Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques. *Journal of Cyber Security Technology*, *7*(4), 199–223. https://doi.org/10.1080/23742917.2023.2228053

Cao, X., Li, Y., Xiong, X., & Wang, J. (2022). Dynamic Routings in Satellite Networks: An Overview. *Sensors*, *22*(12), 4552. https://doi.org/10.3390/s22124552

Escola, J. P. L., Souza, U. B. D., Guido, R. C., Silva, I. N. D., Freitas, J. D. S., & Oliveira, L. D. A. (2022). A mesh network case study for digital audio signal processing in Smart Farm. *Internet of Things*, *17*, 100488. https://doi.org/10.1016/j.iot.2021.100488

Kanellopoulos, D., Sharma, V. K., Panagiotakopoulos, T., & Kameas, A. (2023). Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives. *Electronics*, *12*(11), 2490. https://doi.org/10.3390/electronics12112490

Leloglu, E. (2017). A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications*, *05*(01), 121–136. https://doi.org/10.4236/jcc.2017.51010

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

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Ploumidis, M., Pappas, N., Siris, V. A., & Traganitis, A. (2015). On the performance of network coding and forwarding schemes with different degrees of redundancy for wireless mesh networks. *Computer Communications*, *72*, 49–62. https://doi.org/10.1016/j.comcom.2015.05.001

Radouan Ait Mouha, R. A. (2021). Internet of Things (IoT). *Journal of Data Analysis and Information Processing*, *09*(02), 77–101. https://doi.org/10.4236/jdaip.2021.92006

Rao, U. H., & Nayak, U. (2014). Access Controls. In U. H. Rao & U. Nayak, *The InfoSec Handbook* (pp. 63–76). Apress. https://doi.org/10.1007/978-1-4302-6383-8_4

Rejeb, A., Rejeb, K., Appolloni, A., Jagtap, S., Iranmanesh, M., Alghamdi, S., Alhasawi, Y., & Kayikci, Y. (2024). Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. *Internet of Things and Cyber-Physical Systems*, *4*, 1–18. https://doi.org/10.1016/j.iotcps.2023.06.003

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y.-W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers*, *13*(2), 41. https://doi.org/10.3390/computers13020041

Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in industry 4.0, a review. *Internet of Things and Cyber-Physical Systems*, *3*, 192–204. https://doi.org/10.1016/j.iotcps.2023.04.006

Subrahmanyam, V., Kumar, S., Srivastava, S., Bist, A. S., Sah, B., Pani, N. K., & Bhambu, P. (2023). Optimizing horizontal scalability in cloud computing using simulated annealing for the Internet of Things. *Measurement: Sensors*, *28*, 100829. https://doi.org/10.1016/j.measen.2023.100829

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

Taye, M. M. (2023). Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions. *Computers*, *12*(5), 91. https://doi.org/10.3390/computers12050091

Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in the Internet of Things with a focus on the impact of emerging technologies. *Internet of Things*, *19*, 100564. https://doi.org/10.1016/j.iot.2022.100564

Zuo, Y., Ling, Z., & Yuan, Y. (2013). A hybrid multi-path routing algorithm for industrial wireless mesh networks. *EURASIP Journal on Wireless Communications and Networking*, *2013*(1), 82. https://doi.org/10.1186/1687-1499-2013-82.

.