A REVIEW OF WIRELESS SENSOR NETWORK TECHNOLOGIES IN THE CONTEXT OF THE INTERNET OF THINGS (IoT)

*** OGALA Justin. O. and MUGHELE Ese S. ***
Department of Cyber Security, University of Delta
justin.ogala@unidel.edu.ng, s.mughele@unidel.edu.ng

Abstract— *This review paper provides an in-depth analysis of Wireless Sensor Network (WSN) technologies in the context of the Internet of Things (IoT). With the widespread use of IoT, the demand for WSNs has increased tremendously, making it necessary to explore the technologies that enable the integration of WSNs and IoT. This paper discusses the fundamental concepts of WSNs and IoT, explores the challenges faced by WSNs in the context of IoT, and provides insights into the various applications of WSNs in IoT. The review also examines the data collection and aggregation technique used in WSNs and highlights the limitations of current WSN technologies. Finally, the paper concludes with recommendations for future research to address the challenges facing WSNs in the context of IoT and to improve the efficiency and effectiveness of WSN technologies.*

Index Terms— Wireless Sensor Network (WSN), Internet of Things (IoT), Integration, Challenges, Applications, Aggregation technique

1.0 INTRODUCTION

The rapid development of wireless networking technology has greatly impacted various aspects of daily life. One of the most promising technologies in this regard is the Internet of Things (IoT), which connects numerous devices in the physical world, transforming our daily lives. As a result, there is a growing need for continuous communication in all areas, especially those with increased activity.

The IoT is characterized as the fusion and communication of responsive objects or "things." The widespread use of IoT devices has led to the development of new technologies and applications. These devices, which include household appliances, security cameras, and environmental monitoring sensors, are equipped with a range of transceivers, microcontroller devices, and protocols to transmit control and sensor data needed [5]. The data collected from sensors and other real-time modules are transmitted to centralized repositories, where it is cumulatively stored and accessible to authorized users. The IoT's wireless communication technology differs significantly from that of traditional wired or wireless networking systems due to the large number of communication devices available [11]. Despite this, IoT-based traffic is not typically crucial because each IoT device senses and transmits data to a specific IoT server, and data generated by numerous objects collectively has a limited impact on the network's performance. As a result, IoT networks can operate securely and sustainably without any human intervention.

Wireless Sensor Networks (WSNs) are the foundation of the IoT-based systems that surround us and are critical to introducing significant improvements shortly of energy savings techniques [2]. The rapid technological advancement of these devices has resulted in energy consumption issues in the information exchange, which has become more critical [10]. The rapid increase in communication and information exchange has led to unsustainable increases in energy consumption and carbon emissions-saving techniques [1]. In most applications, such as environmental control and protection, agriculture, border surveillance and protection, etc., sensor nodes must operate effectively for extended periods, ranging from several months to years, depending on the application's requirements for the communication unit [21]. The energy used by these sensors determines how long the application will

- *OGALA Justin. O.*
  Department of Cyber Security, University of Delta
  justin.ogala@unidel.edu.ng
- *MUGHELE Ese S.,*
  Department of Cyber Security, University of Delta
  s.mughele@unidel.edu.ng

last, and dead nodes can affect data reliability, device compatibility, and accuracy. A typical sensor node consists of four main components: the processing unit, the communication unit, the sensing/identification unit, and the power supply unit [7], [8], as shown in Figure 1.

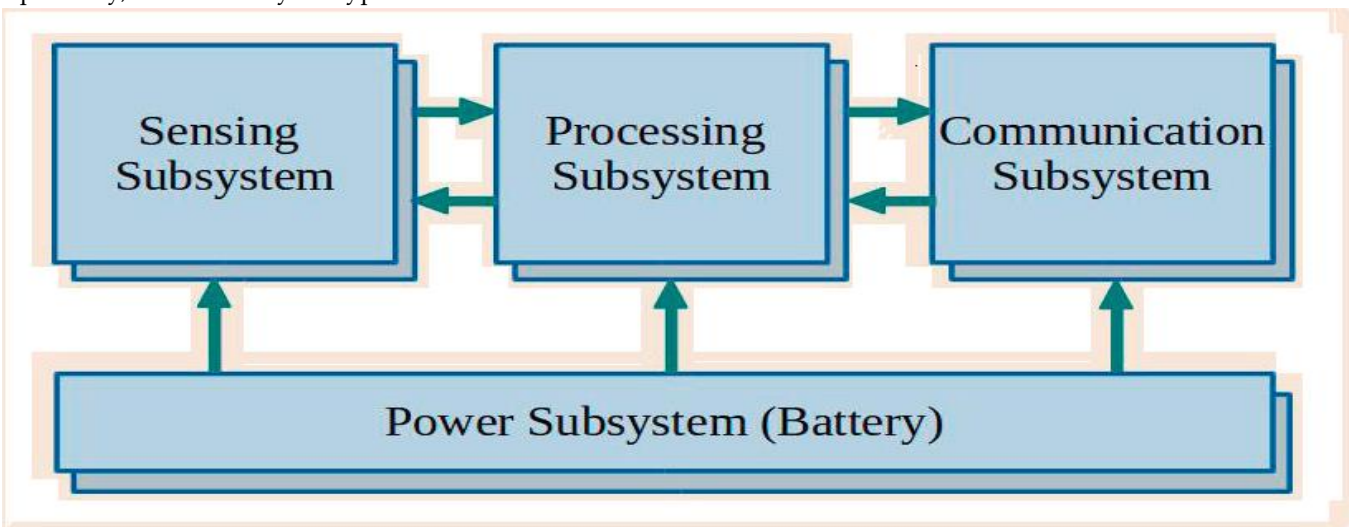

Figure 1: A typical IoT-based sensor node architecture
(Source: Healy et al., 2008; Fahmy, 2016)

2.0 RELATED LITERATURE

Here is the tabular form for some of the related literature for this study:

Reference	Year	Title	Methodology	Key Findings
Abdul-Qawy, A. S., Magesh, P. P. J. E., & Srinivasulu, T. [1]	2015	The Internet of Things (IoT): An Overview	Review	Overview of IoT
Antar, S. A. H., Abdul-Qaw, N. M., Almurisi, S., & Tadisetty, S. [2]	2020	Classification of Energy Saving Techniques for IoT-based Heterogeneous Wireless Nodes	Survey	Classification of energy-saving techniques
Arat, F., & Demirci, S. [3]	2020	Energy and QoS Aware Analysis and Classification of Routing Protocols for IoT and WSN	Analysis and classification	Energy and QoS aware analysis and classification of routing protocols
Begum, K., & Dixit, S. [4]	2016	Industrial WSN using IoT: A survey	Survey	Survey of industrial WSN using IoT
Cho, Y., Kim, M., & Woo, S. [5]	2018	Energy-Efficient IoT based on Wireless Sensor Networks for Healthcare	Design	Energy-efficient IoT for healthcare

Claessens, J. [6]	2008	Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer	Panel discussion	Discussion on trust, security, privacy, and identity perspective for the future internet service offer
Fahmy, H.M. [7]	2016	Wireless Sensor Networks: Concepts. Applications, Experimentation and Analysis, Signal and Communication Technology	Review	Overview of wireless sensor networks
Healy, M., Newe, T., & Lewis, E. [8]	2008	Wireless Sensor Node hardware: A review	Review	Overview of wireless sensor node hardware
Islam, M. S., & Dey, G. K. [9]	2019	Precision Agriculture: Renewable Energy Based Smart Crop Field Monitoring and Management System Using WSN via IoT	Design	Design of a renewable energy-based smart crop field monitoring and management system using WSN via IoT
Kaur, N., & Sood, S. K. [10]	2017	An Energy-Efficient Architecture for the Internet of Things (IoT)	Design	Design of an energy-efficient architecture for IoT
Kim, H. W., & Kyue, D. [11]	2012	Technology and Security of IoT	Review	Overview of technology and security of IoT
Kim, K. I. [12]	2016	Clustering Scheme for (m, k)-Firm Streams in Wireless Sensor Networks	Analysis	Clustering scheme for (m, k)-firm streams in WSN
Lenka, R. K., Rath, A. K., & Sharma, S. [13]	2019	Building Reliable Routing Infrastructure for Green IoT Network	Design	Design of a reliable routing infrastructure for a green IoT network
Mahakalkar, N., & Pethe, R. [14]	2018	Review of Routing Protocol in a Wireless Sensor Network for an IOT Application	Review	Review of routing protocol in a WSN for an IoT application
Muruganandam, K., Balamurugan, B., & Khara, S. [15]	2018	Design Of Wireless Sensor Networks For IoT Application: A Challenge and survey	Survey	Survey on the challenges and design of wireless sensor networks for IoT applications

Table 1: the related literature for this study

3.0 ROLE OF IoT IN WSN

Several research papers and studies have been conducted on the role of IoT in WSN, and this section presents some of the most significant literature, along with their respective in-text citations.

One study focused on the design and implementation of a solar-powered WSN and precision agricultural (PA) network using IoT architecture to enhance smart agriculture management systems. This study enabled real-time data transfers over IoT, offering farmers practical information about various environmental conditions such as saltwater intrusions, soil moisture, water levels, wet conditions, temperature, and the general status of the field [9],[13],[18].

Another study analysed IoT data collection and decision-making ideas, specifically in Industrial WSNs, to enhance energy utilization. The study's results showed that applying the Chaotic Whale Optimization Process to WSN-IoT environmental activities could make the integrated system use less energy [4].

In terms of WSN, a survey was conducted to evaluate the performance of routing protocols in terms of delays, energies, jitters, throughput, and packet-delivery ratios (PDR), using latencies, bandwidth, jitter, and delay as performance metrics. An algorithm was also proposed to improve Ad Hoc On-Demand Distance Vector (AODV) routing in IoT by combining the routing table and the internet access table into a single table [13], [14].

Another study proposed a novel sequence of algorithms for cluster adaptation and rotating, a novel energy consumption reduction mechanism for long-range communications, and an energy-conscious multi-user & multi-hop hierarchical routing protocol (EAMMH-RP) that distributes energy equally across cluster formation sensor nodes. The proposed protocol was tested in the Castalia simulator to ensure its effectiveness in various situations, such as packet transmission, average energy use, end-to-end latency, and network life [17].

A protocol with a reliable routing mechanism for IoT sensing networks was also proposed, which included a clustering and multipathing strategy to minimize energy use and increase reliability. The new protocol was tested using the Castalia simulator, and the results showed the differences between the proposed protocol and the IoT that is already in use [17], [20].

Other studies examined the routing algorithms and models in terms of their characteristics, such as minimizing delay, maximizing data delivery ratio, and conserving energy. For classification, the IoT and WSN-based IoT algorithms were split into two groups: energy consciousness and delay; throughput, data transfer, and packet loss awareness [3].

Lastly, WSN systems utilize sensor nodes with an onboard CPU to monitor a specific area's environment. The sensor nodes are linked to the base station, which serves as the WSN System's processing hub. The WSN system's base station is connected to the Internet to share data, which can be processed, analyzed, stored, and mined using WSN (fig. 2) [16].

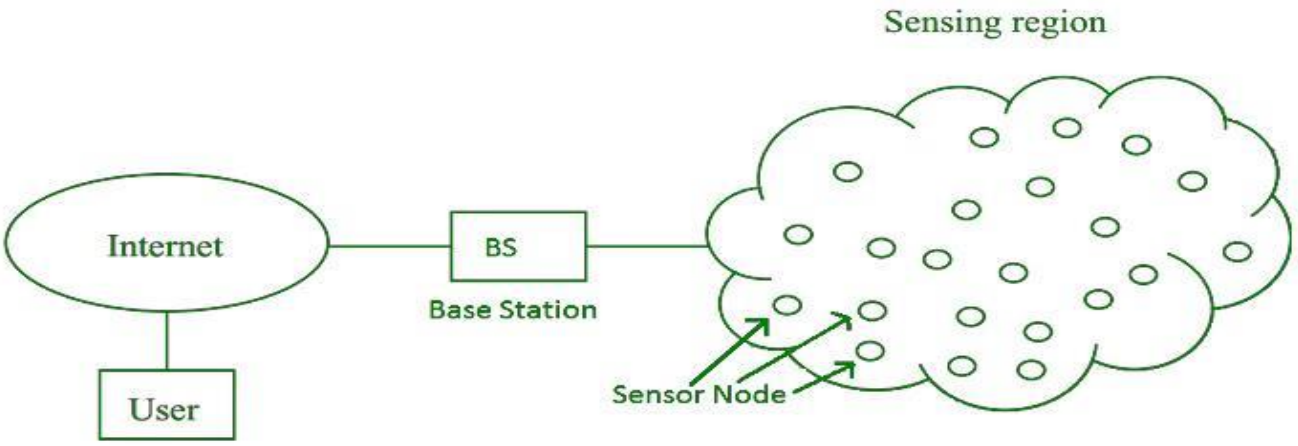

Figure 2: An IoT-based sensor network
(Source: Adapted from Prakash, 2019)

4.0 SOLUTIONS TO WSN CHALLENGES IN IoT

Given the numerous challenges associated with WSNs in IoT, various solutions have been proposed. These solutions aim to address the issues discussed in section II. Some of the proposed solutions include:

a. **Real-time management:** To address the issue of real-time management, a smart data-driven middleware architecture can be implemented. This architecture will allow for the transmission of real-time information only when a certain threshold is reached. Additionally, an effective service gateway design can be implemented to reduce the amount of data that needs to be sent [20].
b. **Privacy and security:** To ensure privacy and security in WSNs, various levels of safety measures can be implemented. These measures are suitable for M2M deployments where there is already a trust connection between the server and the device [15], [18]. Additionally, the use of a unique and effective gateway, as well as a key, can be employed to ensure effective security.
c. **Security:** To address the security challenges associated with WSNs, various measures can be implemented. These measures include the use of physical security to prevent attackers from adding malicious nodes to the network, and blocking or capturing them. Additionally, the use of effective security frameworks and malware prevention techniques can be employed [6].
d. **Service Quality:** To improve the quality of service in WSNs, techniques for load distribution can be implemented. This will ensure that the burden of intelligence provision is distributed among the nodes that have access to resources [15]. Additionally, the use of advanced QoS techniques can help maintain a stable network.
e. **Configuration:** To ensure effective configuration in WSNs, advanced network management tools can be implemented. These tools will enable the network to self-heal by locating and removing problematic nodes. Additionally, they can help in creating scalable networks that are easy to manage [15].
f. **Availability:** To maintain the availability of WSNs, encryption schemes can be employed. These schemes will help protect the network from hacking and other malicious attacks. Additionally, techniques for data access and modification can be implemented to ensure that the network remains available at all times.
g. **Data Integrity:** To maintain the integrity of data in WSNs, advanced data management tools can be employed. These tools will enable the network to detect and correct any errors or inconsistencies in the data. Additionally, they can help in ensuring that the data is always accurate and reliable.
h. **Confidentiality:** To ensure confidentiality in WSNs, advanced encryption tools can be implemented. These tools will help protect the privacy of the data and information transmitted over the network. Additionally, techniques for data sharing and access control can be employed to ensure that only authorized users can access sensitive data [15].

In conclusion, WSNs play a critical role in the functioning of the IoT. However, they also present significant challenges that must be addressed to ensure their effective operation. By implementing the proposed solutions discussed in this article, it is possible to address the various challenges associated with WSNs in IoT and ensure their continued operation.

5.0 APPLICATION OF WSN IN IoT

WSN has various applications in the Internet of Things (IoT).

a. **System Design**: One of the primary applications of WSNs in IoT is system design. IoT sensors need to continually perceive the environment to convey data to the end user. WSN allows for the development of sensor networks that can accomplish this task effectively. To increase the overall network lifetime, data communication must be performed in an energy-efficient manner. WSN's inherent capabilities, such as low power consumption, make it an ideal technology for IoT system design [16],[21].
b. **Home Automation:** Apart from IoT system design, WSN has numerous other applications in IoT. Home automation is one such application. WSN can be used to develop smart homes, where all electronic devices are interconnected and can be controlled remotely. This type of home automation can provide users with an unparalleled level of comfort and convenience.
c. **Weather Monitoring:** Weather monitoring is another application of WSN in IoT. WSN can be used to deploy weather monitoring systems that can monitor various environmental parameters, such as temperature, humidity, and air pressure. This information can be used to provide real-time weather forecasts and alerts.
d. **Used in Agriculture:** WSN can also be used in agriculture to monitor crop growth and soil moisture levels. By deploying WSN-based systems, farmers can remotely monitor crop conditions and take appropriate action, such as adjusting irrigation and fertilization schedules, to optimize crop yields.
e. **Biomedical Patient Monitoring:** Biomedical patient monitoring is another application of WSN in IoT. WSN-based patient monitoring systems can be used to remotely monitor patients' vital signs and other health parameters. This type of system can be particularly useful for patients with chronic illnesses who require regular monitoring.

f. **WSN-based Surveillance Systems:** WSNs can also be used in surveillance and monitoring for security purposes. WSN-based surveillance systems can be deployed in public spaces, such as airports and train stations, to monitor suspicious activities and identify potential threats.

g. **Landslide Detection:** Landslide detection is another application of WSN in IoT. WSN-based systems can be used to monitor soil moisture levels and detect potential landslide risks. This information can be used to take preventive action, such as evacuating residents, in the event of a potential landslide.

h. **Noise Level Monitoring:** Finally, WSN can be used to monitor noise levels in the environment. This type of monitoring can be particularly useful in urban areas, where excessive noise levels can have a detrimental impact on public health.

In conclusion, WSN has numerous applications in the Internet of Things, including IoT system design, home automation, weather monitoring, agriculture, biomedical patient monitoring, surveillance and monitoring for security purposes, landslide detection, and noise level monitoring. WSN's inherent capabilities, such as low power consumption and reliable data communication, make it an ideal technology for these applications.

6.0 DATA COLLECTION AND AGGREGATION TECHNIQUES IN WSNs

6.1. Data Collection Techniques

Data collection is a critical component of WSNs, as it involves the collection of data from multiple sensors deployed in various environments. There are two main data collection techniques used in WSNs: centralized and decentralized.

a. Centralized data collection involves transmitting all the data collected by the sensors to a central node or gateway for further processing and analysis. This technique is useful for applications where real-time data is not required and where the focus is on long-term data analysis.

b. Decentralized data collection, on the other hand, involves distributing the data collection and processing tasks among the different sensors in the network. This technique is useful for applications where real-time data is required and where the focus is on short-term data analysis.

6.2. Aggregation Techniques

Aggregation is the process of combining multiple data points collected by different sensors to create a single, aggregated value. There are several aggregation techniques used in WSNs, including:

a. **Spatial aggregation:** This technique involves combining data from multiple sensors that are geographically close to each other. This technique is useful for applications where the focus is on obtaining an overall picture of a particular environment or area.

b. **Temporal aggregation**: This technique involves combining data collected at different time intervals to obtain an overall picture of the environment over a longer period. This technique is useful for applications where the focus is on identifying trends and patterns over time.

c. **Hybrid aggregation:** This technique involves combining spatial and temporal aggregation techniques to obtain a more comprehensive view of the environment. This technique is useful for applications where the focus is on both short-term and long-term data analysis.

d. **Compressive sensing:** This technique involves compressing the data collected by the sensors before transmission to reduce the amount of data that needs to be transmitted. This technique is useful for applications where the focus is on energy efficiency and reducing the amount of data transmitted over the network.

Conclusion: Data collection and aggregation are critical components of WSNs, and their integration with IoT technologies is essential for the effective functioning of these networks. There are several data collection and aggregation techniques used in WSNs, each with its advantages and disadvantages. Understanding these techniques is crucial for the development of efficient and effective WSNs that can support the growing demand for IoT applications.

7.0 CONCLUSION

The advancement of computer technology has facilitated the development of WSNs, which are capable of constantly sensing the necessary parameters. In recent years, IoT-based WSN systems have garnered significant attention. However, due to limited bandwidth, power, and resources, these systems face challenges with the point-to-point transmission. An excellent solution to this problem is data collection.

The analysis of vital data using less energy is a crucial issue in sensor networks. Consequently, different data aggregation algorithms have been developed, as discussed in this work, to reduce power consumption. This study reviews existing literature on the function of IoT in WSN and presents various data aggregation strategies proposed in previous works. The primary objectives of

data-gathering approaches are to ensure network security, enhance the quality of service (QoS), and conserve energy.

8.0 LIMITATIONS AND RECOMMENDATIONS

While WSNs and their applications in IoT have shown great potential, there are still several limitations and challenges that need to be addressed. Some of these limitations include:

1. **Limited Network Capacity:** WSNs have limited capacity due to the small size of nodes, limited processing power, and memory. This limitation affects the amount of data that can be transmitted and the range of the network.
2. **Security Challenges:** WSNs are vulnerable to different types of security threats such as jamming attacks, eavesdropping, and denial of service attacks. Therefore, there is a need to develop effective security mechanisms that can protect these networks from various types of attacks.
3. **Energy Efficiency:** Energy efficiency is critical in WSNs as nodes are typically battery-powered. Data aggregation techniques can help reduce energy consumption, but there is still a need for more energy-efficient protocols and algorithms.
4. **Reliability:** WSNs are often deployed in harsh environments and remote locations where maintenance is difficult. Therefore, these networks need to be reliable and resilient to ensure continuous operation.

To address these limitations, several recommendations can be made:

1. Develop more energy-efficient algorithms and protocols that can help reduce the energy consumption of nodes in WSNs.
2. Enhance the security of WSNs by developing effective security mechanisms that can protect these networks from different types of attacks.
3. Increase the network capacity of WSNs by developing more powerful and efficient nodes and improving communication protocols.
4. Explore new applications and use cases for WSNs in different industries and sectors.
5. Conduct more research on WSNs and IoT to improve the understanding of these technologies and develop new solutions that can address the existing challenges.

In conclusion, while WSNs and IoT have great potential, there are still several limitations and challenges that need to be addressed. By addressing these limitations and implementing the recommendations mentioned above, WSNs and IoT can become more reliable, secure, and energy-efficient, and can enable new and innovative applications and use cases.

ACKNOWLEDGEMENT

The authors are grateful to the Marie Curie Library of the Abdus Salam. We also appreciate the European Centre for Research Training and Development, the United Kingdom for access to research materials and resources.

REFERENCES

[1] A. Abdul-Qawy, A. S., Magesh, P. P. J. E., & Srinivasulu, T. (2015). The Internet of Things (IoT): An Overview [IJERA]. *International Journal of Engineering Research and Applications, 5*(12), 71–82.

[2] Antar, S. A. H., Abdul-Qaw, N. M., Almurisi, S., & Tadisetty, S. (2020). Classification of Energy Saving Techniques for IoT-based Heterogeneous Wireless Nodes. *Procedia Computer Science, 171*, 2590–2599. https://doi.org/10.1016/j.procs.2020.04.281

[3] Arat, F., & Demirci, S. ‘‘Energy and QoS Aware Analysis and Classification of Routing Protocols for IoT and WSN,” 2020 7th International Conference on Electrical and Electronics Engineering (ICEEE), Antalya, Turkey, 2020, pp. 221-225, https://doi.org/10.1109/ICEEE49618.2020.9102614Amazon services. (n.d.). What is ‘Local shops on Amazon? Retrieved from https://services.amazon.in/services/sell-on-amazon/local-shops.html

[4] Begum, K., & Dixit, S. ‘‘Industrial WSN using IoT: A survey,” 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 499-504, https://doi.org/10.1109/ICEEOT.2016.7755660

[5] Cho, Y., Kim, M., & Woo, S. Energy Efficient IoT based on Wireless Sensor Networks for Healthcare, Int. Conf. Adv. Commun. Technol. (ICACT) (2018).

[6] Claessens, J. (2008). *Trust, Security, Privacy, and Identity perspective.* Panel on Future Internet Service Offer.

[7] Fahmy, H. M. (2016). *Wireless Sensor Networks: Concepts. Applications, Experimentation and Analysis, Signal and Communication Technology*. Springer. https://doi.org/10.1007/978-981-10-0412-4

[8] Healy, M., Newe, T., & Lewis, E. (2008). Wireless Sensor Node hardware: A review, in 2008 IEEE Sensors, 621-624.

[9] Islam, M. S., & Dey, G. K. ‘‘Precision Agriculture: Renewable Energy Based Smart Crop Field Monitoring and Management System Using WSN via IoT,” 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 2019, pp. 1-6, https://doi.org/10.1109/STI47673.2019.9068017

[10] Kaur, N., & Sood, S. K. (2017). An Energy-Efficient Architecture for the Internet of Things (IoT). *IEEE Systems Journal, 11(2),* 796–805. https://doi.org/10.1109/JSYST.2015.2469676

[11] Kim, H. W., & Kyue, D. (2012). Technology and Security of IoT. *J. Korea Instit. Informat. Secur. Cryptol., 22(1),* 7–13.

[12] Kim, K. I.(2016) ‘‘Clustering Scheme for (m, k)-Firm Streams in Wireless Sensor Networks,” the Journal of information and communication convergence engineering, vol.14, no. 2, pp. 84-88, 2016 https://doi.org/10.6109/jicce.2016.14.2.084

[13] Lenka, R. K., Rath, A. K., & Sharma, S. (2019). Building

Reliable Routing Infrastructure for Green IoT Network. IEEE Access: *Practical Innovations, Open Solutions, 7,* 129892–129909. https://doi.org/10.1109/ACCESS.2019.2939883

[14] Mahakalkar, N., & Pethe, R. "Review of Routing Protocol in a Wireless Sensor Network for an IOT Application," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 21-25, https://doi.org/10.1109/CESYS.2018.8723935

[15] K. Muruganandam, B. Balamurugan, Dr Sibaram Khara, Design Of Wireless Sensor Networks For IoT Application: A Challenges and survey, ijecs, 26 March 2018, Page No.: 23790-23795

[16] Prakash, R., Kansal, P., & Kakar, V. K. "Optimized Hybrid Clustered Protocol for IoT Heterogeneous Wireless Sensor Networks," 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 2019, pp. 1-6, https://doi.org/10.1109/CICT48419.2019.9066258

[17] Priyanga, M., Leones Sherwin Vimalraj, S., & Lydia, J. "Energy Aware Multiuser & Multi-hop Hierarchical – Based Routing Protocol for Energy Management in WSN-Assisted IoT," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2018, pp. 701-705, https://doi.org/10.1109/CESYS.2018.8724073

[18] S. Sarkar, K. U. Rao, J. Bhargav, S. Sheshaprasad and A. Sharma C.A., "IoT Based Wireless Sensor Network (WSN) for Condition Monitoring of Low Power Rooftop PV Panels," 2019 IEEE 4th International Conference on Condition Assessment Techniques in Electrical Systems (CATCON), Chennai, India, 2019, pp. 1-5, doi:10.1109/CATCON47128.2019.CN0045

[19] Thangarasu, G., & Dominic, P. D. D. M. bin Othman, R. Sokkalingam and K. Subramanian, "An Efficient Energy Consumption Technique in Integrated WSN-IoT Environment Operations," 2019 IEEE Student Conference on Research and Development (SCOReD), Bandar Seri Iskandar, Malaysia, 2019, pp. 45-48, https://doi.org/10.1109/SCORED.2019.8896238

[20] Young-bok, C., Sang-ho, L., & Woo, S.-H. (2017). "An Adaptive Clustering Algorithm of Wireless Sensor Networks for Energy Efficiency", Journal of The Institute of Internet [IIBC]. *Broadcast. Commun., 17(1),* 99–106.

[21] Zhou, X. Green Communication Protocols for Mobile Wireless Networks PhD thesis, University of Ottawa, 2017.

Justin O. OGALA

Ogala, Justin Onyarin is an experienced computer science lecturer with a diverse educational background. He holds a B. Tech in Computer Science & Mathematics from the Federal University of Technology, Minna, Niger State (1998), an MBA in Information Technology from Lagos State University, Lagos (2007), and an M.Sc in Information Technology from the National Open University of Nigeria (2018). Currently, he is pursuing a PhD in Computer Science at Ambrose Ali University, Ekpoma, Edo State, Nigeria.

He has a strong research background and extensive expertise in various areas of computer science, including DevOps, Cybersecurity, Software Analysis and Development, Intelligent Computing, Big Data Analysis, Software Engineering, Distributed Computing, Computer and Society, Artificial Intelligence, Machine Learning, Software Development, Web Development, Web Programming, Web Technologies, Application Development, Agile Development, and Unified Language.

In addition to his academic pursuits, he is a member of the Teachers Registration Council of Nigeria (TRCN), the International Association of Engineers (IAENG) in the UK, and the Computer Professionals Registration Council of Nigeria (CPN). His passion for computer science and commitment to his profession make him a valuable asset to any organization or research team.

Dr Ese S. MUGHELE

Dr Mrs Mughele, Ese Sophia, is the Pioneer Ag. Head of Department Cyber Security, Faculty of Computing University of Delta, Agbor Delta State. Nigeria. She is an Alumnus of the great University of Benin, where she obtained her PhD degree in Computer Science majoring in Machine Learning, Soft Computing, and Information Systems, and M.Phil. Computer Science majoring in Soft Computing and Information Systems in the Department of the Computer Science University of Benin. She obtained M.Sc in Computing and Information Science (ARCIS) at the University of Ibadan majoring in Information Systems, Congestion Control Mechanisms, and Queuing Models, and a B.Sc (Hons) in Computer Science from Ambrose Alli University Ekpoma and a major in Information Systems and the University of Calabar where she bagged a Diploma in Computer Science.

Dr Mrs Mughele has over 60 peer-reviewed referenced publications in International, National, and local journals and conference papers. She is a member of several professional organizations.