

Blockchain-enabled Data Integrity in Wireless Sensor Networks

Yahye Adam Omar

University of Hargeisa, Maroodijeeh, 2522, Somaliland

Email: yahye.adam@uoh.edu.so

Received: 31 March, 2024; Revised: 20 May, 2024; Accepted: 15 July, 2024; Published: 08 December, 2024

Abstract: Wireless sensor networks (WSNs) are widely used across various fields, facilitating the gathering of critical data for monitoring physical and environmental conditions. However, traditional WSNs encounter cybersecurity challenges, including weak node authentication, limited fault tolerance, insufficient detection of malicious nodes, and insecure data integrity management. Given these vulnerabilities, it is essential to develop effective solutions to address WSN cybersecurity issues. A key concern that requires special focus is ensuring robust data integrity management to resolve trust-related problems in WSNs. Most current existing solutions rely on centralized systems, which are vulnerable to tampering and offer no proper data integrity management or traceability for the data gathered from sensors. In this paper, we present an architecture based on blockchain technology to ensure secure data transmission and effective data integrity management for data collected from WSN devices. By employing the decentralized and immutable nature of blockchain, the integration of WSN and blockchain technology provides a robust infrastructure that features tamper-resistant for better decision-making process. The results show that the proposed architecture offers secure data storage and provides strong performance, capable of scaling to accommodate large WSNs through the use of blockchain. This study also identifies the most common challenges in integrating blockchain with WSNs and provides appropriate solutions to fully harness the benefits of blockchain applications in these networks.

Index Terms: Blockchain, Wireless Sensor Networks, Cyber Attacks, Integrity Management, Decentralization.

1. Introduction

Wireless communication provides the freedom to connect and communicate without being tethered to a physical cable [1]. This allows wireless communication networks to operate easily and fully automated, facilitating seamless data exchange. The proliferation of wireless sensor networks (WSNs) has revolutionized various domains, enabling real-time data collection and monitoring for applications ranging from environmental sensing to healthcare systems [2]. However, the inherently distributed and resource-constrained nature of WSNs introduces significant challenges in terms of data security, integrity, and reliability [3]. The decentralized nature of these networks, combined with the vulnerabilities inherent in wireless communication, exposes them to various threats, such as data tampering and unauthorized access.

Blockchain technology initially introduced as the underlying technology behind cryptocurrencies like Bitcoin, blockchain has evolved into a powerful tool with vast potential in various industries [4]. Its core features, including decentralization, consensus mechanisms, and cryptographic techniques, make it well-suited for enhancing the data security and trustworthiness of WSNs [5]. Blockchain offers several unique features that make it an attractive solution for wireless sensor networks security. First and foremost, it provides a decentralized architecture, eliminating the need for a central authority and reducing the risk of a single point of failure [6]. This decentralized nature of blockchain makes it inherently resilient to attacks and tampering attempts.

Moreover, blockchain ensures data integrity through cryptographic mechanisms. Each transaction or data exchange on the blockchain is secured using cryptographic hashes, making it virtually impossible for malicious actors to manipulate or tamper with the data without detection [7]. This feature can play a pivotal role in ensuring the integrity of wireless network communications. Additionally, the transparency and immutability of blockchain can enhance the accountability and traceability of network activities.

The main contribution of this paper is the development of a blockchain-based architecture to enhance cybersecurity in Wireless Sensor Networks (WSNs), specifically addressing data integrity and secure transmission. The proposed solution leverages blockchain's decentralized and immutable nature to provide tamper-resistant data management, overcoming the vulnerabilities of traditional, centralized systems. The architecture is shown to offer secure data storage, scalability for large WSNs, and improved decision-making capabilities. Additionally, the paper identifies key

challenges in integrating blockchain with WSNs and suggests solutions to fully utilize blockchain's potential in these networks.

2. Related Works

Most of today's software application models are centralized, controlled by a single central entity. All the nodes employed in the network are directly dependent on the central point. This structure can raise several challenges to network security; since all data is stored and managed by a central server, an attacker only needs to target that server to potentially compromise the integrity of the entire network.

According to [8], blockchain technology offers promising solutions to address security and efficiency issues in wireless sensor networks (WSNs). The study also mentioned that blockchain-inherited security features, including decentralization and tamper-resistance storage, can enhance data integrity from wireless network sensors. Concerning the WSNs, [9] mentioned that blockchain technology can be used to secure the integrity of data transmission and processing in wireless sensor networks. The study also proposed the advantage of designing a robust mechanism based on smart contracts and blockchain technology that allows the reliable processing of data.

The nature of decentralization architecture and the use of advanced cryptographic techniques make blockchain technology inevitably possess the necessary features required to make data from wireless sensor networks extremely difficult for unauthorized users to access or alter the information. As stated by [10], the integration of blockchain and WSNs enables secure data collection from the sensor nodes, leveraging the data integrity and reliability as well as visualization.

Recent research proposes blockchain-based solutions to enhance security in wireless sensor networks (WSNs). These approaches aim to strengthen data security, improve authentication, and detect malicious attacks. Blockchain technology is used to store node identities and validate network participants through public and private blockchains [11]. Some studies integrate blockchain with data transfer to establish secure WSN structures, making data tampering nearly impossible [12]. Others propose schemes combining heuristic, signature, and voting detection methods with blockchain to identify malicious nodes and threats [13].

Blockchain-integrated intelligent monitoring systems have also been developed to monitor network activities and measure performance metrics such as packet delivery ratio and detection accuracy [14]. These blockchain-based solutions aim to address critical security needs in WSNs, including privacy, dependability, and autonomy, while reducing vulnerabilities to hostile users and harmful usage.

[15] introduced a model that incorporates a security system to enhance the support for Wireless Sensor Networks (WSNs). Their study utilizes blockchain technology to store sensor node data across multiple devices within the network, which includes tracking transaction times. Additionally, their simulation results demonstrated that this approach significantly increases the difficulty of altering or tampering with the data.

The reviewed literature agrees that blockchain technology can effectively address various security and data integrity challenges in Wireless Sensor Networks (WSNs). By distributing data across multiple devices within the network, blockchain helps to detect malicious nodes that operating on the network and transmitting false data. Likewise, any software application model that incorporates blockchain technology can also take advantage of these built-in security features.

3. Typical Architecture and Applications of WSN

A Wireless Sensor Network (WSN) consists of several spatially distributed sensor nodes that are connected using wireless communication. A sensor node, also known as a mote, is a type of electronic device composed of a processor, storage, a transceiver, one or more sensors, an analogue-to-digital converter, and a battery for power [16]. Additional components, like a positioning unit and/or a mobilization unit, may also be present. This is illustrated in Fig 1.

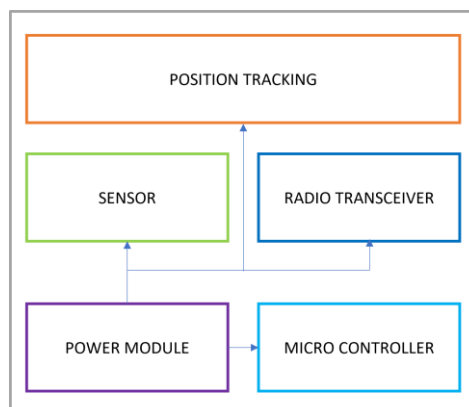


Fig. 1. Wireless sensor module.

Wireless sensor networks provide seamless connectivity among multiple sensor nodes, allowing for ubiquitous data gathering from diverse locations. This connectivity enables the integration of sensor data into larger systems. Fig. 2 illustrates the radio transmission from wireless sensors to the gateway, from where the data can be sent to the cloud via a wired Ethernet, cellular, or Wi-Fi network [17]. Thus, the data in WSN takes a multi-hop path to reach the sink node or base station.

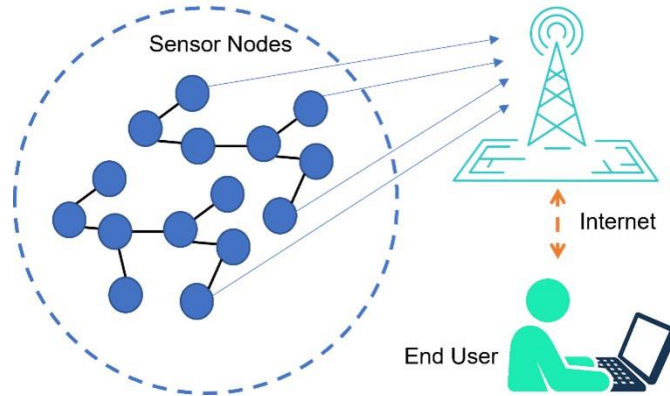


Fig. 2. The typical architecture of a WSNs.

WSNs are composed of many small sensors placed within a variety of layouts, such as star, ring, and mesh. The radio transmission capability of these sensors is usually limited to a radius of a few tens of meters, thus necessitating the use of nodes to transfer data from the sensors to the gateway.

3.1. Main WSN Applications

Connecting various functions, WSN allows nodes to communicate with one another and control one another. It can be used for various urban functions, such as monitoring infrastructure, including bridges and tunnels, power lines, and network cables [9]. Moreover, these sensors can be used to monitor even places that require long-term observations for detecting structural deterioration by simply attaching a sensor.

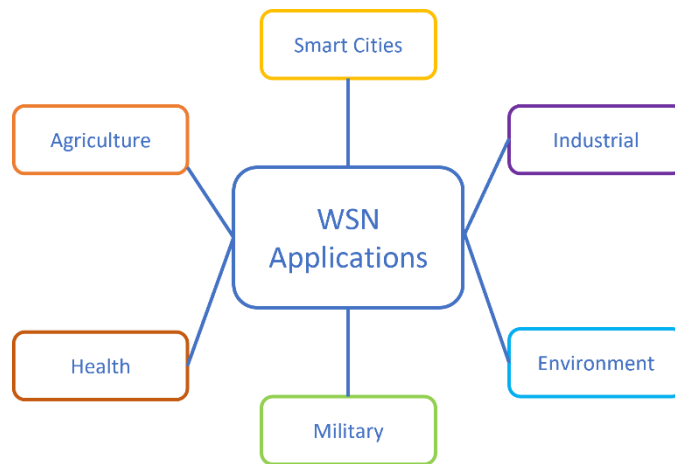


Fig. 3. Most popular categories of applications of WSNs.

Environmental monitoring is one of the main applications of WSNs like temperature, humidity, air quality, and water quality in forests and rivers. These networks enable early detection of natural disasters, pollution monitoring, and ecosystem preservation. In healthcare, WSNs facilitate remote patient monitoring, tracking vital signs, and detecting anomalies, thereby improving patient care and reducing hospital visits [18]. In agriculture, WSNs assist in precision farming by monitoring soil moisture, temperature, and crop conditions. Industrial automation also benefits from WSNs by enabling the condition monitoring of machinery, improving operational efficiency, and reducing maintenance costs. Furthermore, WSNs can also be integrated with emerging technologies such as the Internet of Things (IoT), edge computing, and artificial intelligence (AI) to extend their applications.

4. WSNs Security Constraints

A WSN is a special form of wireless network that has traits in common with other wireless systems, but also possess its own features that distinguishing from other WNs. While WSNs offer numerous benefits, such as flexibility,

scalability, and cost-effectiveness, they also present unique security challenges [19]. Addressing these security constraints is crucial to ensure the integrity, confidentiality, and availability of the data transmitted within the network. The following sub-sections outlining the main security constraints on WSNs:

4.1 Limited Resources

WSN nodes typically have limited processing power, memory, energy, and communication capabilities [20]. These constraints make it challenging to implement resource-intensive security mechanisms. To acquire complex security mechanisms, there is a high demand for extensive resource consumption. In addition, to increase the lifetime of the sensor, we tend to increase the processing power and memory size. Often, failure of the sensor nodes arises from exhausted batteries or the processing module [21]. Therefore, it should be considered an effective security design that does not complicate the setting of barriers to the sensor's functionality.

4.2 Unreliable Communication

As the WSNs use sensors that are incapable of handling reliable cryptographic algorithms or secure authentication mechanisms, their networks are susceptible to various attacks, including eavesdropping, jamming, and message alteration [22]. Furthermore, the open nature of wireless channels makes it easier for attackers to intercept or tamper with transmitted data. To ensure secure communication from the sensors to where data is processed, there is a need to employ secure communication protocols among the communicating devices through the wireless medium.

4.3 Node Deployment and Physical Vulnerability

WSN nodes are often deployed in hostile environments, such as remote locations or hazardous areas, making them susceptible to physical attacks. Attackers may physically tamper with or disable nodes, compromise sensors, or inject malicious code [23]. Moreover, the conditions in which the sensors are placed often vary, and the topology of the system is continually changing. Because of this, more dependable security protocols are necessary to handle the alterations in the environment.

4.4 Network Scalability

WSNs can comprise thousands or even millions of sensor nodes, creating scalability challenges for security mechanisms. As the network grows in size, key management, authentication, and secure routing become more complex. Efficient key distribution protocols, hierarchical architectures, and distributed security mechanisms are required to be employed to address scalability constraints [24].

4.5 Data Integrity

As WSNs are reluctant to employ robust and secure communication protocols such as public key cryptography, attackers can easily gain access to or sniff the collected data from the sensor while it's passing through multiple hops to reach the sink or base station. Therefore, to preserve data integrity in WSNs, reliable communication protocols should be considered.

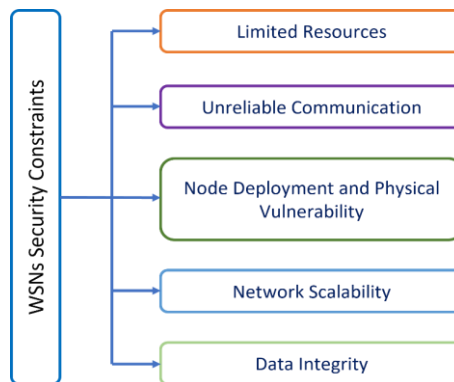


Fig. 4. WSNs Security constraints

Table 1. Proposed solutions for security constraint in WSNs from existing literature

Id, Reference	Author(s) Name	First	Security Constraints	Proposed Solutions
1. [25], [26]	Parenreng J, Sambo D		Limited Resources	- Combining data communications and data processing - Reducing the amount of data communication by moving the data processing algorithm to the sensor node

2. [27], [28]	Liu Paruvathavardhini J,	Unreliable Communication	• Light weight cryptographic algorithms (ECC) • Authenticate connected devices (sensors)
3. [29]	Madhu,	Node Deployment & Physical Vulnerability	• Tamper-resistant packaging • Secure bootstrapping • Machine learning IDS
4. [30], [31]	Verma V, Sambo	Network Scalability	• Efficient key distribution protocols • Hierarchical architectures • Distributed security mechanisms
5. [32],[33]	Elmahdi,	Data Integrity	• A SafeQ protocol • Message authentication code (MAC) protocol

5. Data Integrity Attacks and Threat Models in WSNs

As wireless communication occurs in the absence of a physical medium (cables), it possesses a nature of vulnerability that is greater than that of a wired network. Moreover, WSNs are often operated in environments where physical controls are not readily available, making the network susceptible to physical tampering [34]. Sensor nodes in the WSN have limited capabilities in terms of processing power and energy resources to handle robust security protocols. These limitations made WSNs vulnerable to a number of security attacks. The following are the main threats to the integrity of the WSN data:

5.1 Denial of Services Attack

In a WSN, each sensor node has limited resources, including battery power. Attackers can target specific nodes by initiating resource-intensive tasks or exploiting vulnerabilities, ultimately draining the node's energy resources [35]. This can result in the node becoming non-responsive or even permanently disabling it. This type of attack can occur in several forms e.g., disrupting the radio link, misrouting sensor data, or exhausting node resources.

Jamming: Attackers can intentionally transmit strong radio signals within the frequency range used by the WSN, effectively jamming or interfering with legitimate communications [36]. This disrupts the communication between sensor nodes and the base station, rendering the network ineffective.

Routing Attacks: Attackers can target the routing protocols used in WSNs, manipulating routing tables or forging routing messages. By disrupting the routing process, they can isolate certain nodes or prevent the delivery of data, leading to a denial of service [37].

Node Exhaustion: In a WSN, each sensor node has limited resources, including battery power. Attackers can target specific nodes by initiating resource-intensive tasks or exploiting vulnerabilities, ultimately draining the node's energy resources. This can result in the node becoming non-responsive or even permanently disabling it.

5.2 Data Modification Attack

A data modification attack in a WSNs refers to the unauthorized alteration of data transmitted within the network. These attacks aim to manipulate the integrity and accuracy of the data by altering the value of one or more of the data readings by either taking over the sender's sensor or inserting themselves between the sender and the receivers [38].

5.3 False Data Insertion

This type of attack involves taking control of one or more network nodes and making them accept false messages with incorrect information. Another way the attacker can carry out this attack is by adding new nodes to the network that provide false information.

5.4 Data Deletion

This type of attack occurs when an adversary tries to drop individual data readings or prevent data packets in transit from reaching their intended destination throughout the network. Attackers can compromise individual sensor nodes within the network and delete data stored on those nodes [39]. By gaining unauthorized access to a node, they can manipulate or erase the data stored in its memory or storage components. This can result in the loss of valuable information collected by the compromised node.

6. Blockchain Background

Blockchain technology is a decentralized digital ledger that enables secure and transparent record-keeping of transactions across multiple computers or nodes. At its core, a blockchain consists of a chain of blocks, where each block contains a list of transactions [40]. These transactions can represent the exchange of digital assets, contracts, or any other form of data.

Transactions are grouped into blocks and added to the blockchain in a sequential manner. Before a block is added, it goes through a validation process, ensuring the accuracy and legitimacy of the transactions. In addition, each block contains a unique identifier called a cryptographic hash, which is generated using a mathematical algorithm [41]. This Hash not only identifies the block but also links it to the previous block, forming a chain. Fig 5 shows a visual

representation of a blockchain transaction; the request for the transaction is sent out to all the peers of the blockchain network for validation and after successful approval the data stored in the ledger permanently.

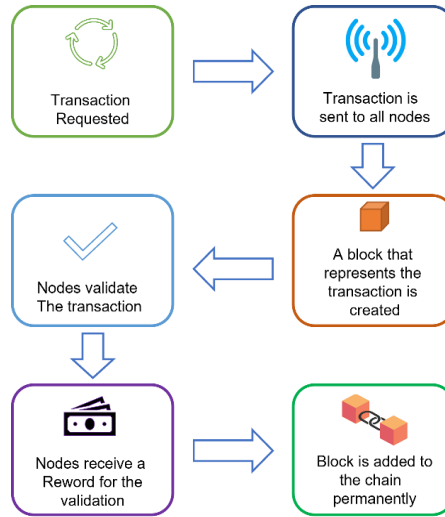


Fig. 5. Blockchain transaction workflow.

As the blockchain is distributed across multiple nodes, each participating node has a copy of the entire blockchain. This decentralization ensures that no single entity controls the entire system, making it more resistant to censorship and fraud. Additionally, the transparency of the blockchain allows anyone to view and audit the transaction history, enhancing trust and accountability.

Blockchain technology employs advanced cryptographic techniques to secure transactions and data [42]. Public-key cryptography is often used to provide secure digital identities, authenticate participants, and ensure confidentiality and integrity of data within the blockchain.

6.1 Key Characteristics

Blockchain technology is characterized by its decentralization; no single organization or entity has control over the data that is added to the blockchain. Instead, the information that is stored on the blockchain is verified and accepted by participants in a peer-to-peer network using a range of consensus protocols. Blockchain's internal structure ensures the immutability and transparency of the ledger [43]. Once a transaction is recorded on the blockchain, it becomes virtually impossible to alter or tamper with. This characteristic is achieved through cryptographic hashing and linking each transaction to the previous one, creating a chain of blocks.

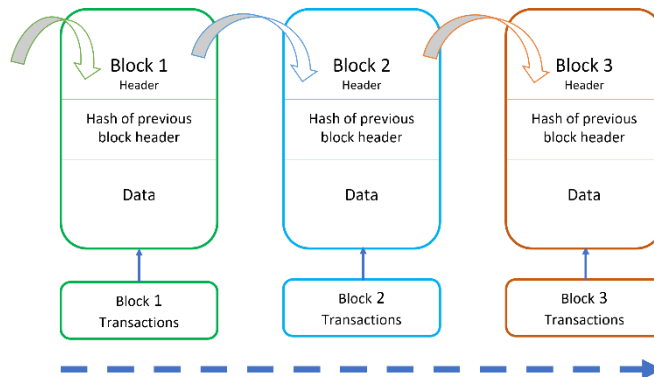


Fig. 6. Blockchain Structure.

7. Integration of Blockchain and WSNs for Data Integrity

Blockchain technology enables decentralized data storage by distributing information across multiple nodes within the blockchain network, rather than relying on a single centralized server. The convergence of blockchain technology with WSNs presents a promising opportunity to enhance the security, reliability, and data integrity of WSN applications [44]. In this section, we discuss how blockchain can be integrated with WSNs to address challenges related to data security, trustworthiness, and tamper resistance.

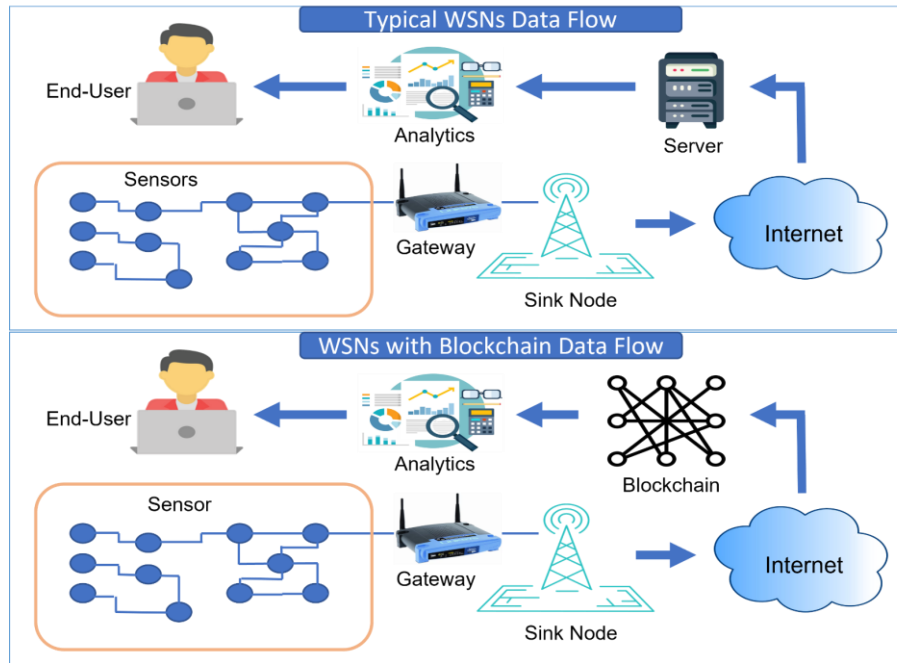


Fig. 7. Comparison between typical WSN data flow and WSN with blockchain.

In the preceding figure (Fig. 7), comparing the typical WSN data flow approach and blockchain integration, data in a typical WSN is stored on a single server, which is vulnerable to a single point of failure and susceptible to data modification attacks. In addition, the centralized approach has limitations in terms of reliability and trust. Blockchain can contribute to eliminating central data storage and offering a decentralized approach where data is replicated across many nodes [45]. Moreover, blockchain integration relies on a robust cryptographic mechanism that leverages data integrity.

By integrating blockchain, data gathered from sensor's operating environment can be decentralized, allowing individual sensor nodes to retain control over their own data [46]. Smart contracts on the blockchain can define access control and data sharing rules, ensuring privacy and enabling selective data sharing while maintaining confidentiality.

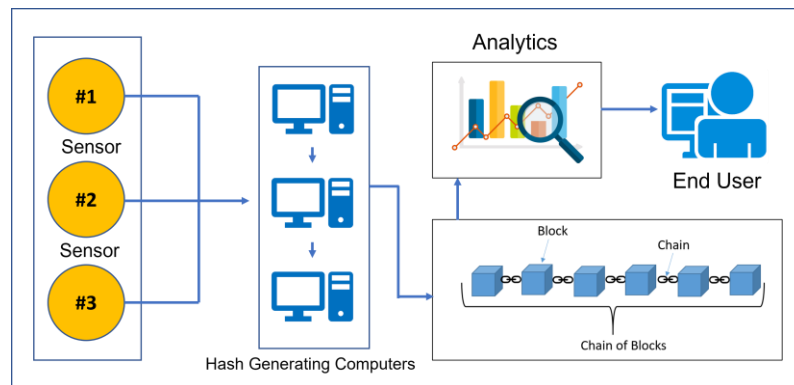


Fig. 8. Proposed blockchain WSN architecture for data storage.

Embedded microcontrollers are used to build the intended system in this study to connect the sensor that collecting the data. All small sensors send the data to an edge computer, which is a local processing unit that using SHA256 algorithm to generate transaction hash codes and sends the data to the blockchain. Relatively, the data can be shared to the cloud for further analysis and insights. Users can access WSN data from the blockchain. This access ensures data authenticity and security. The integration involves the development of smart contracts using Solidity code and Proof of Stake (PoS) consensus mechanism that does not require a high level of resources but offers the same security as Poof of work (PoW) or Delegated Proof of Stake (DPoS). The smart contract defines functions for storing and retrieving sensor data in the blockchain.

In this experiment, a Raspberry Pi is set up with eight temperature sensors. An edge computer is configured to generate a transaction hash codes for each data unit from the sensors. The validated data is stored on a private Ethereum blockchain network using Geth. A smart contract, written in Solidity, was developed to define functions for storing and retrieving the sensor data.

Table 2. Data stored in the Blockchain

Sensor	IoT 0 sense temperature: at time
Temperature	41
Timestamp	2024/08/21 – 14:24:12
SHA256	db469a4bc6ce135cf4eb65e21876c55d1206a882f6006dd8eb27215aabb6ccdc

In addition, we developed a localhost web application that presents three options for the user: Star WSN, Sensor Data, and Transaction Processed Graph. The web application is integrated with the Solidity smart contract to display sensor data from the Ethereum blockchain. When the "Transaction Processed Graph" button is clicked, the `getTotalDataEntries` function is invoked to determine the total number of data entries. A loop is then executed through each data entry using the `retrieveSensorData` function to fetch the timestamp, data, and sender associated with each entry. The retrieved data is stored in an array to be processed by the (D3.js) charting library.

8. Results Analysis

When the user clicks the "Transaction Processed Graph" button, a temperature analysis graph is generated from the blockchain database. As depicted in Figure 9, the transaction time increases with the number of connected sensors, indicating that scalability issue arises from this integration system. However, the results also reveal a notable decrease in transaction time when only the hash of the transaction data is stored, rather than the plain text and its hash. Consequently, a manual verification will be required later to check if the data is being tempered with.

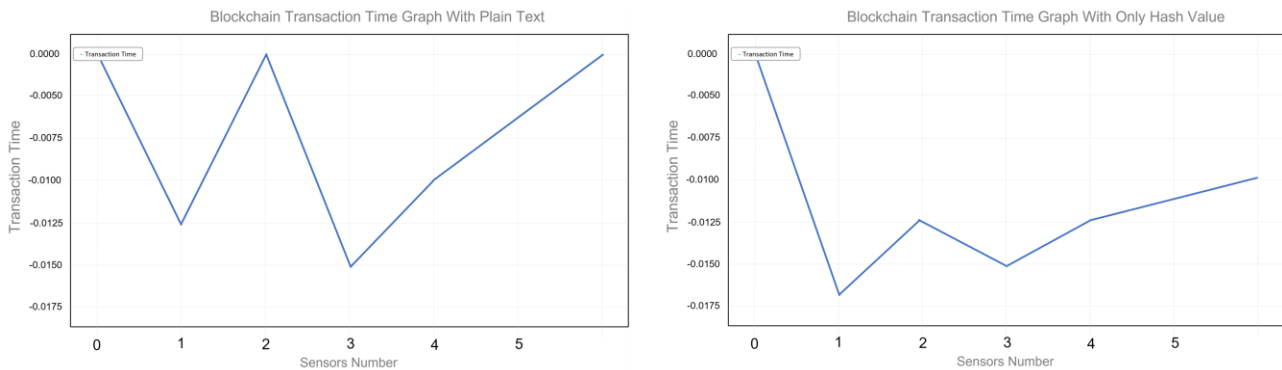


Fig. 9. Blockchain Transaction Time for Storing Sensor data.

During the experiment, we adjusted various parameters, such as the number of sensors transmitting data and the amount of data being recorded on the blockchain ledger. Both the sensor count and the transaction data volume had a significant effect on the speed at which the blockchain processes and records the data. Generally, higher data volumes and a greater number of sensors resulted in longer processing times. In addition, blockchain operations, including data verification and consensus algorithms, require significant computational power, which can drain the limited battery life of WSN nodes. These are the current issues that await resolution.

9. Challenges of Integration and Proposed Solutions

While blockchain has the potential to enhance the security, transparency, and data integrity of WSNs, its unique characteristics and constraints introduce complexities in their integration. The following are some common blockchain and WSNs integration challenges and proposed solutions:

- **Computational Limitations:** WSN nodes typically have limited computational resources (low processing power, memory, and storage). Running blockchain protocols, particularly Proof of Work (PoW), can be resource-intensive and beyond the capacity of typical WSN nodes [47]. A potential solution to this problem involves adopting lightweight consensus mechanisms such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), which demand less computational power. Additionally, employing a lightweight cryptographic method like elliptic curve cryptography (ECC) could address the limited computational capacity, as ECC is known for being both less resource-intensive and highly secure for encryption.
- **Latency and Transaction Time:** Blockchain-based transactions typically experience delays due to consensus mechanisms, leading to increased latency. In a time-sensitive WSN environment, where quick data processing is required (e.g., in real-time monitoring applications), this delay can be problematic [48]. Implement sidechains or permissioned blockchains tailored for specific WSN applications that can reduce latency.

Additionally, reducing data volume, such as only storing the hash of the data, can significantly improve response times.

- *Power Consumption:* WSNs often operate in energy-constrained environments where nodes are battery-powered. Blockchain protocols, especially PoW, are known for their high energy consumption, which could significantly reduce the battery life of WSN nodes. Use energy-efficient consensus mechanisms such as Proof of Authority (PoA) or Proof of Burn (PoB) that consume less power. Another solution arises from using LEACH (Low-Energy Adaptive Clustering Hierarchy), which is a popular hierarchical routing protocol designed for wireless sensor networks (WSNs) to improve energy efficiency [49]. LEACH organizes sensor nodes into clusters. Each cluster has a cluster head (CH), which is selected periodically.
- *Scalability:* As WSNs grow with more sensor nodes, the blockchain network might struggle to keep up with the increasing number of transactions (see Section 6). High transaction volumes can slow down the network, making it harder to scale. Researchers have introduced various techniques to address the scalability challenges of blockchain in wireless sensor networks (WSNs) [50]. One proposed approach involves using a blockchain based on directed acyclic graphs (DAGs) combined with load-balanced routing and lightweight authentication encryption. Additionally, some studies suggest that delegating blockchain functionality to specific nodes within the network can also improve WSN scalability.

10. Conclusions

In this paper, we introduce a blockchain-based architecture designed to manage and store data from WSN devices. The proposed system preprocesses sensor data using dedicated computers that generate a hash while retaining the plain text. Only the generated hash is sent to the blockchain database, allowing the network to efficiently handle large data volumes by storing the hash instead of the full plain text. Furthermore, the use of dedicated preprocessing units helps significantly reduce the computational and energy limitations of WSN nodes, which are often constrained by limited resources. By offloading intensive tasks to more capable machines, the architecture maintains the energy efficiency and longevity of WSNs without compromising the integrity and security of the data. We also implement a smart contract mechanism to ensure that the results of any data transfer are predetermined, thereby removing the possibility of malicious interactions. Despite the other reviewed methods in this study for ensuring data integrity in WSNs, we assume that blockchain's security features are particularly effective for data integrity and reducing the likelihood of malicious attacks by employing authorization and authenticating every device that is operating in the network.

References

- [1] J. M. Jornet, E. W. Knightly, and D. M. Mittleman, "Wireless communications sensing and security above 100 GHz," *Nature Communications* 2023 14:1, vol. 14, no. 1, pp. 1–10, Feb. 2023, doi: 10.1038/s41467-023-36621-x.
- [2] H. Kumar, "A Review of Wireless Sensor Network from Future Perspective," *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, vol. 12, no. 1, pp. 84–88, Feb. 2023, Accessed: Jul. 09, 2023. [Online]. Available: <https://eduzonejournal.com/index.php/eiprmj/article/view/259>
- [3] M. Sirajuddin and B. Sateesh Kumar, "Collaborative Security Schemes for Wireless Sensor Networks," *Lecture Notes in Electrical Engineering*, vol. 828, pp. 343–354, 2022, doi: 10.1007/978-981-16-7985-8_36/COVER.
- [4] F. A. Sunny et al., "A Systematic Review of Blockchain Applications," *IEEE Access*, vol. 10, pp. 59155–59177, 2022, doi: 10.1109/ACCESS.2022.3179690.
- [5] N. Badri, L. Nasraoui, and L. A. Saidane, "Blockchain for WSN and IoT Applications," 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, SETIT 2022, pp. 543–548, 2022, doi: 10.1109/SETIT54465.2022.9875746.
- [6] T. Yang et al., "Applying blockchain technology to decentralized operation in future energy internet," *ieeexplore.ieee.org*, doi: 10.1109/EI2.2017.8244418.
- [7] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," Jun. 2019, doi: 10.6028/NIST.IR.8202.
- [8] Rehman, A., Abdullah, S., Fatima, M., Iqbal, M. W., Almarhabi, K. A., Ashraf, M. U., & Ali, S. (2022). Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain. *Applied Sciences*, 12(21), 10794. <https://doi.org/10.3390/app122110794>.
- [9] Haro-Olmo, F. J., Alvarez-Bermejo, J. A., Varela-Vaca, A. J., & López-Ramos, J. A. (2021b). Blockchain-based federation of wireless sensor nodes. *The Journal of Supercomputing*, 77(7), 7879–7891. <https://doi.org/10.1007/s11227-020-03605-3>.
- [10] L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbabor, S. Kadry and S. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," in *IEEE Access*, vol. 9, pp. 128765–128785, 2021, doi: 10.1109/ACCESS.2021.3111923.
- [11] Nguyen, M. D., Nguyen, M. T., Vu, T. C., Ta, T. M., Tran, Q. A., & Nguyen, D. T. (2024). A Comprehensive Study on Applications of Blockchain in Wireless Sensor Networks for Security Purposes. *Journal of Computing Theories and Applications* ISSN, 3024, 9104.
- [12] Hsiao, S. J., & Sung, W. T. (2021). Utilizing blockchain technology to improve WSN security for sensor data transmission. *Comput. Mater. Contin.*, 68, 1899–1918.
- [13] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 217–234). Cham: Springer International Publishing.

- [14] Singh, T., & Vaid, R. (2023). Blockchain Integrated Intelligent Monitoring System for Wireless Sensor Network. 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), 612-620.
- [15] Nguyen, M., Nguyen, C., & Tran, H. T. (2022). A framework of deploying blockchain in wireless sensor networks. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 9(32).
- [16] P. E. A. S. T. Ehizuenlen, "Design of a Smart Custom Sensor Node Architecture for Wireless Sensor Network (WSN)," *Journal of Science and Technology Research*, vol. 5, no. 2, pp. 2023–133, Jun. 2023, doi: 10.5281/ZENODO.8014261.
- [17] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of Wireless Sensor Networks: An Up-to-Date Survey," *Applied System Innovation* 2020, Vol. 3, Page 14, vol. 3, no. 1, p. 14, Feb. 2020, doi: 10.3390/ASI3010014.
- [18] M. Majid et al., "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review," *Sensors* 2022, Vol. 22, Page 2087, vol. 22, no. 6, p. 2087, Mar. 2022, doi: 10.3390/S22062087.
- [19] J. Grover and S. Sharma, "Security issues in Wireless Sensor Network-A review," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions, pp. 397–404, Dec. 2016, doi: 10.1109/ICRITO.2016.7784988.
- [20] Z. Zhao, L. Du, F. Sun, Z. Fang, Z. Xu, and D. Chen, "A Review of Attacks and Security Protocols for Wireless Sensor Networks," *Article in Journal of Networks*, 2014, doi: 10.4304/jnw.9.5.1103-1113.
- [21] P. Bekal, P. Kumar, P. R. Mane, and G. Prabhu, "A comprehensive review of energy efficient routing protocols for query driven wireless sensor networks," *F1000Research* 2023 12:644, vol. 12, p. 644, Jun. 2023, doi: 10.12688/f1000research.133874.1.
- [22] S. Singh, R. Saurabh, T. Maitra, and D. Giri, "Security in Communication for Intelligent Wireless Sensor Networks : Issues and Challenges," *Computational Intelligence for Wireless Sensor Networks*, pp. 175–192, Jul. 2022, doi: 10.1201/9781003102397-10.
- [23] "Recent Trends for Security Applications in Wireless Sensor Networks – A Technical Review | IEEE Conference Publication | IEEE Xplore." <https://ieeexplore.ieee.org/abstract/document/8991249> (accessed Jul. 10, 2023).
- [24] M. Abujubbeh, F. Al-Turjman, and M. Fahrioglu, "Software-defined wireless sensor networks in smart grids: An overview," *Sustain Cities Soc*, vol. 51, p. 101754, Nov. 2019, doi: 10.1016/J.SCS.2019.101754.
- [25] J. M. Parenreng, A. Kitagawa, and D. D. Andayani, "A Study of Limited Resources and Security Adaptation for Extreme Area in Wireless Sensor Networks," *J Phys Conf Ser*, vol. 1244, no. 1, Jun. 2019, doi: 10.1088/1742-6596/1244/1/012013.
- [26] D. W. Sambo, B. Yenke, A. Förster, P. D.- Sensors, and undefined 2019, "Optimized clustering algorithms for large wireless sensor networks: A review," *mdpi.com*, doi: 10.3390/s19020322.
- [27] J. Liu and F. Xu, "Research on trust-based secure routing in wireless sensor networks," <https://doi.org/10.1117/12.2672753>, vol. 12610, pp. 942–948, Apr. 2023, doi: 10.1117/12.2672753.
- [28] J. Paruvathavardhini, B. Sargunam, and R. Sudarmani, "A Review on Energy Efficient Routing Protocols and Security Techniques for Wireless Sensor Networks," *Applied Mechanics and Materials*, vol. 912, pp. 55–75, Feb. 2023, doi: 10.4028/P-5S9P7J.
- [29] T. Madhu Midhan, K. Devika, R. Rajakumar, R. Manikandan, K. Dinesh, and M. Sreedevi, "A review on Machine Learning based IDS approaches in Wireless sensor networks," 2023 9th International Conference on Advanced Computing and Communication Systems, ICACCS 2023, pp. 1238–1243, 2023, doi: 10.1109/ICACCS57279.2023.10112982.
- [30] V. K. Verma, S. Singh, and N. P. Pathak, "Analysis of scalability for AODV routing protocol in wireless sensor networks," *Optik (Stuttg)*, vol. 125, no. 2, pp. 748–750, Jan. 2014, doi: 10.1016/J.IJLEO.2013.07.041.
- [31] D. W. Sambo, B. O. Yenke, A. Förster, and P. Dayang, "Optimized Clustering Algorithms for Large Wireless Sensor Networks: A Review," *Sensors* 2019, Vol. 19, Page 322, vol. 19, no. 2, p. 322, Jan. 2019, doi: 10.3390/S19020322.
- [32] X. Liu, J. Yu, F. Li, W. Lv, Y. Wang, and X. Cheng, "Data Aggregation in Wireless Sensor Networks: From the Perspective of Security," *IEEE Internet Things J*, vol. 7, no. 7, pp. 6495–6513, Jul. 2020, doi: 10.1109/JIOT.2019.2957396.
- [33] B. B. PGScholar and S. N. Asst Professor, "Preserving Privacy and Integrity in Wireless Sensor Network using Range Queries," *International Journal of Engineering Research & Technology*, vol. 2, no. 13, Jul. 2018, doi: 10.17577/IJERTCONV2IS13075.
- [34] E. Elmahdi, S. Yoo, ... K. S.-... on I. of T., and undefined 2019, "Protecting Data Integrity for Multi-Application Environment in Wireless Sensor Networks," *ieeexplore.ieee.org*, Accessed: Jul. 02, 2023. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/8875502/>
- [35] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," *Journal of Network and Computer Applications*, vol. 190, p. 103118, Sep. 2021, doi: 10.1016/J.JNCA.2021.103118.
- [36] S. Subramani and M. Selvi, "Comprehensive review on distributed denial of service attacks in wireless sensor networks," *International Journal of Information and Computer Security*, vol. 20, no. 3–4, pp. 414–438, 2023, doi: 10.1504/IJICS.2023.128828.
- [37] K. Dhivyasri, A. Suphalakshmi, M. R.-Int. J. Res. Appl. Sci. Eng, and undefined 2020, "Wireless sensor network jammer attack: A detailed review," *academia.edu*, Accessed: Jul. 10, 2023. [Online]. Available: <https://www.academia.edu/download/64124956/844.pdf>
- [38] Z. Alansari, N. B. Anuar, A. Kamsin, and M. R. Belgaum, "A systematic review of routing attacks detection in wireless sensor networks," *PeerJ Comput Sci*, vol. 8, p. e1135, Oct. 2022, doi: 10.7717/PEERJ-CS.1135/SUPP-1.
- [39] T. Rathod et al., "Blockchain for Future Wireless Networks: A Decade Survey," *Sensors* 2022, Vol. 22, Page 4182, vol. 22, no. 11, p. 4182, May 2022, doi: 10.3390/S22114182.
- [40] Z. Xia, Z. Wei, and H. Zhang, "Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/3449428.
- [41] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564, Sep. 2017, doi: 10.1109/BIGDATAACONGRESS.2017.85.

- [42] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, pp. 839–858, Aug. 2016, doi: 10.1109/SP.2016.55.
- [43] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102039, Aug. 2022, doi: 10.1016/J.SETA.2022.102039.
- [44] Y. A. Omar, S. B. Goyal, and V. Varadarajan, "Apply Blockchain Technology for Security of IoT Devices," *2021 IEEE International Conference on Emerging Trends in Industry 4.0, ETI 4.0 2021*, 2021, doi: 10.1109/ETI4.051663.2021.9619295.
- [45] M. Ali, I. A. Abd El-Moghith, M. N. El-Derini, and S. M. Darwish, "Wireless Sensor Networks Routing Attacks Prevention with Blockchain and Deep Neural Network.," *cdn.techscience.cn*, doi: 10.32604/cmc.2022.021305.
- [46] A. K. Dangi, G. A. Pandurang, G. V. Bachhav, M. K. Chakravarthi, A. Gehlot, and S. K. Shukla, "Blockchain Applications for Security Issues and Challenges in IOT," *2023 International Conference on Artificial Intelligence and Smart Communication, AISC 2023*, pp. 582–585, 2023, doi: 10.1109/AISC56616.2023.10085201.
- [47] S. J. Hsiao and W. T. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks," *IEEE Access*, vol. 9, pp. 72326–72341, 2021, doi: 10.1109/ACCESS.2021.3079708.
- [48] C. V. Nguyen, M. T. Nguyen, T. T. Le, T. A. Tran, and D. T. Nguyen, "Blockchain technology in wireless sensor network: benefits and challenges," *theblockchaintest.com*, vol. X, No. Y, 2021, Accessed: Jul. 10, 2023. [Online]. Available: <https://theblockchaintest.com/uploads/resources/Nguyen%20Le%20Tran%20-%20Blockchain%20Technology%20in%20Wireless%20Sensor%20Network%20-%202021%20Dec.pdf>
- [49] B. K. Chauhan and D. B. Patel, "A Systematic Review of Blockchain Technology to Find Current Scalability Issues and Solutions," pp. 15–29, 2022, doi: 10.1007/978-981-16-3346-1_2.
- [50] T. Singh, R. Vaid, and A. Sharma, "Security Issues in Blockchain Integrated WSN: Challenges and Concerns," *Proceedings of the 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2022*, 2022, doi: 10.1109/ICSES55317.2022.9914006.

Authors' Profiles



Yahye Adam Omar is a dedicated PhD candidate specializing in the field of computer science with a focus on Cyber Security. Currently pursuing doctoral studies, Yahye delves deeply into the intricate realms of interconnected devices, blockchain technology, and wireless network security. Their academic pursuits are driven by a passion for advancing the understanding and fortification of digital landscapes against emerging cyber threats.

How to cite this paper: Yahye Adam Omar, "Blockchain-enabled Data Integrity in Wireless Sensor Networks", *International Journal of Wireless and Microwave Technologies(IJWMT)*, Vol.14, No.6, pp. 15-25, 2024. DOI:10.5815/ijwmt.2024.06.02