International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Prevention of Sybil Attack on Block Chain to Ensure Security of Wireless Sensor Network

[1]Satpal Singh, [2]Dr. Subhash Chander

Submitted: 11/10/2023 **Revised**: 29/11/2023 **Accepted**: 09/12/2023

Abstract: This study explores the enhancement of security and reliability in a Wireless Sensor Network (WSN) using blockchain technology. We focus on the integration of blockchain within WSN to provide robust authentication without the involvement of a third party. The methodology begins with the collection of routing data using Q-tables in MATLAB, followed by uploading this data to the blockchain, ensuring the data's security with SHA256 cryptography encryption. The blockchain network's resilience is assessed against a Sybil attack by employing two consensus algorithms, Proof of Work (PoW) and Proof of Authority (PoA). We execute a Sybil attack on the blockchain network, aiming to investigate the efficiency of PoW and PoA in detecting and preventing the attack. The assessment reveals that PoW provides superior security guarantees, maintaining the blockchain's integrity, validity, and resilience against the attack, albeit with higher computational efforts. In contrast, PoA demonstrates faster operations but fails to ensure the network's integrity post-attack, proving to be less reliable in a hostile environment. This comprehensive examination offers valuable insights into the security dynamics of a blockchain-integrated WSN, contributing substantially to the field by outlining the strengths and weaknesses of employing different consensus algorithms in thwarting potential attacks on the network.

***Keywords**: Wireless Sensor Network, Block chain, Proof of Work, Proof of Authority.*

1. Introduction

Wireless Sensor Networks (WSNs) have brought about a significant enhancement in the quality of life. They have made it convenient for individuals to communicate with distant devices without the necessity for a physical connection. This advancement in technology allows devices to interact over a distance, making various tasks more efficient and less cumbersome. However, this ease of interaction is not without its challenges. WSNs are vulnerable to a range of security threats, including hacking and virus attacks. These vulnerabilities can be exploited bymalicious entities to compromise the network's functionality and integrity.

One such malicious activity is the Sybil attack. In a Sybil attack, a single node within the network falsely presents itself as several different nodes. By creating these false identities, the attacker aims to infiltrate the network, establishing connections with legitimate nodes. This infiltration allows the attacker to manipulate the network's routing data, altering it to serve their malicious purposes. The attacker can create an overwhelming number of false nodes, seeking to gain control over the entire network. This control enables them to manipulate the network's operations, leading to data loss and potential harm to the system as a whole. The entire network

1Research Scholar,Departmentof ComputerScience,
Punjabi University
Patiala
spsingh.mohali@gmail.com
2AssistantProfessorinComputerScience
UniversityCollege
Jaitu

The entire network can be destabilized as the attacker creates numerous fake identities, overshadowing the legitimate nodes and preventing them from effectively transmitting and receiving data.

The entire network can be destabilized as the attacker creates numerous fake identities, overshadowing the legitimate nodes and preventing them from effectively transmitting and receiving data.

Researchers have made efforts to detect and counteract Sybil attacks in WSNs. Mandala et al. have employed machine learning techniques to identify Sybil attacks in WSNs. Dhamodharan et al. have proposed a method that combines CAM-PVM (Compare and Match-Position Verification Method) with MAP (Message Authentication and Passing) to detect and prevent Sybil attacks in WSNs. Despite these efforts, the threat of Sybil attacks continues to loom over WSNs, necessitating further measures to safeguard the networks.

In light of these challenges, Blockchain technology emerges as a promising solution to enhance the security of WSNs. Blockchain is a decentralized ledger technology that was initially conceptualized by Satoshi Nakamoto in 2008 for securing public transaction ledgers of Bitcoin. It eliminates the need for a centralized authority, ensuring that transactions are verified and recorded in a secure and transparent manner. Blockchain technology is characterized by four major features: Consensus Mechanism,

Researchers have made efforts to detect and counteract Sybil attacks in WSNs. Mandala et al. have employed machine learning techniques to identify Sybil attacks in WSNs. Dhamodharan et al. have proposed a method that combines CAM-PVM (Compare and Match-Position Verification Method) with MAP (Message Authentication and Passing) to detect and prevent Sybil attacks in WSNs. Despite these efforts, the threat of Sybil attacks continues to loom over WSNs, necessitating further measures to safeguard the networks.

In light of these challenges, Blockchain technology emerges as a promising solution to enhance the security of WSNs. Blockchain is a decentralized ledger technology that was initially conceptualized by Satoshi Nakamoto in 2008 for securing public transaction ledgers of Bitcoin. It eliminates the need for a centralized authority, ensuring that transactions are verified and recorded in a secure and transparent manner. Blockchain technology is characterized by four major features: Consensus Mechanism,

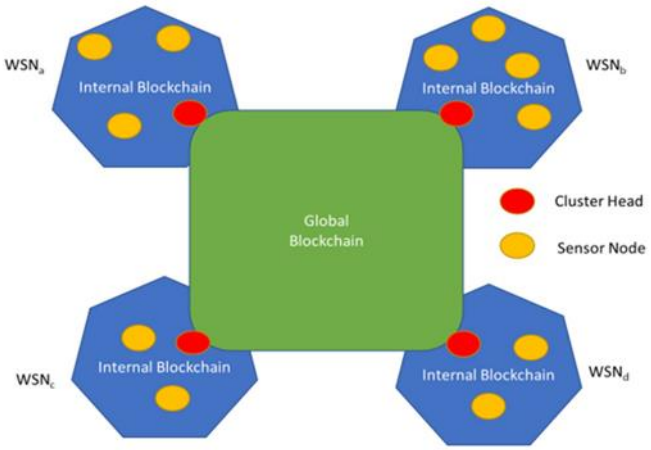

Fig 1: WSN Blockchain Model

The proposed work implements PoA and PoW consensus mechanisms to counteract Sybil attacks in WSNs. In the PoW mechanism, a miner is required to solve a cryptographic problem to earn the right to add a new block to the Block chain. This process ensures that only legitimate entities can add blocks to the Block chain, enhancing the network's security. In the PoA mechanism, a limited number of pre-defined nodes are granted the authority to act as validators and add new blocks to the network. This authority is vested in trusted entities, ensuring that the network remains secure from malicious attacks, including Sybil attacks.

In conclusion, the integration of Blockchain technology with WSNs provides a robust solution to enhance the security of the networks. By employing consensus mechanisms such as PoA and PoW, Blockchain technology ensures that WSNs are safeguarded against Sybil attacks, enhancing the reliability and integrity of the networks. This integration ensures that WSNs continue to facilitate convenient and efficient communication with remote devices, while ensuring that the networks remain secure and resilient against malicious attacks.

2. Related Work

Sung-Jung Hsiao *et al.* proposed a technique to improve the security of data in blockchain based WSN. They use microcontrollers to interconnect various sensor nodes and security is being enhanced by utilizing block chain technology. In this, the proposed system acts as private cloud data centre that visualises the data uploaded by the sensors to create charts and tables. Integration of blockchain technology with wireless sensor network is thoroughly explained in this paper. To simplify the blockchain security, they shift the encryption method from a symmetric to symmetric.

Nguyen *et al.* discussed various benefits and shortcoming of blockchain technology in WSN.By using sensors, it becomes easier to collect data from our surroundings thus it makes life more comfortable. The major benefits of using BC in WSN are security, immutability, reliability and shared system. However, it also has some drawbacks like storage issue, scalability, power consumption, lack of skills and legal issues.

Mubarak ali presented an ovel efficient approach for authentication using blockchain technology to secure the routing data in Wireless Sensor Networks. Base stations, sink nodes and normal nodes are being formulated for simulation purposes. A hybrid model is made by integrating the blockchain technology with WSN in which user authentication and verification is done through BC.

Godawatte *et al.* secured the information accountability and integrity in healthcare using BC. Sensors devices are prone to attacks as they are low capability devices.

Blockchain provides WSN security features along with data breach prevention methods. Majority of the nodes in WSN are low powered devices so they may or may not be suitable for deployment in BC. In health care, extremely sensitive data is passed through the sensors, altering in data by malicious node can be lethal for the patient's life. Future cloud computing and fog computing will use BC to protect WSN transmission.

Ramasamy *Tal*. introduced a survey on BC based WSN for malicious node detection. It detects the malicious node in two parts, firstly, the BC based WSN architecture for malicious no dedetection and secondly, smart contract aspect in malicious node detection. Then this survey explains the

Data management, security management, information

Integrity and nodel on gevity in wireless sensor network. In the end, paper provides the information of data sharing, storage requirements, malicious node detection and data security.

Nguyen *et al*. presented the framework of deploying BC in WSN. Attackers can attack the network to get the desired information from the network. The main purpose of this paper is to reduce the attack from the hackers and improve efficiency by detecting malicious nodes. Blockchain has decentralized consensus mechanisms that helps in preventing the data tampering. The most modern security and data storage technology available nowadays is blockchain. Moreover, BC is managed by all the nodes of network and authentications age is broadcasted to each node in the network.

Paulraj *etal*. Proposed the security mechanism in blockchain based WSN by using authentication and cluster head selection. Cluster heads receive the data from the sensor nodes and process it according to the requirement. DDR- LEACHE can be substituted with CHs if the distance of BS, residual energy and degree are considered. Many computational resources and power were needed to implement PoWso it was replaced by PoA.In the end, MITM and Sybil were used to calculate the results and check the system s resilience.

Awan *et al*. proposed a block chain based encryption and trust evaluation model in which aggregator nodes and sensor nodes are stored. Authentication of AN is checked by public blockchain whereas SN's authentication is performed by private blockchain. SNs are more prone to attacks because these are of low power, less transmission range and limited computational capabilities. PDR is high when there is large number of trusted SNs but PDRislowwhenmostoftheSNsdieduetolowenergyandonlyfewSNsparticipate.Rivest-Shamir-Adleman (RSA) is used for encryption and decryption of data for secure transmission.

Shahbazi *et al*. collected the human psychological and physical data (Blood pressure, ECG, temperature, sugar level etc.) from the patients that demands secure, optimal and efficient routing techniques. A blockchain based Adaptive Thermal/ Energy-Aware Routing (ATEAR)protocol is used for data transmission. Temperature rise, throughput and energy consumption are used to evaluate the performance of ATEAR whereas resource utilization, latency and transaction through put are used to investigate BC performance.

Qu and Zheng *et al*. submitted an efficient routing protocol in Wireless body area network in order to perform reliable data transmission. They take many parameters into consideration like residual energy, transmission efficiency, available band width and number of hops to the sink node. A maximum benefit function to select` then exthopnode by normalizing the node parameters and select the node with largest value as next hop node. The proposed work is compared with priority-based energy efficient routing algorithm (PERA) which shows the improvement in reliability of data transmission.

3. Proposed Method:

The proposed method is divided into several phases for the integration of WSN and blockchain, the major phases are discussed as below:

3.1 Data Collection and Processing:

In the methodology for enhancing the security and reliability of Wireless Sensor Networks (WSNs) with blockchain technology, the process begins with data collection and processing. This initial stage involves the use of Q-tables in MATLAB to effectively gather and process the routing data. This technique allows for the structured and efficient collection of essential data for the network's operation, ensuring that every piece of information is accounted for and organized properly. To establish the initial parameters of the network, various elements are initialized. These include the network size, the number of nodes, the number of rounds, cluster heads, and energy constants. Setting these parameters is a crucial step, as based on these parameters further we are storing the routing data. This approach provides a solid and reliable basis, ensuring that the network is well-defined and prepared for integration with blockchain technology. Proper initialization and organization of these parameters contribute to the robust functioning of the WSN, supporting the overall goal of enhanced security and reliability within the network. The organized and meticulous process of data collection and initialization sets the stage for the successful application of blockchain technology to the WSN, promoting

enhanced security and efficient operation throughout the network's lifecycle.

I. Initialization Phase:
• **Symbols Used:**
• *N*: Number of Nodes
• *R*: Number of Rounds
• *CH*: Cluster Heads
• *E*: Initial Energy
• *S*: Structure Array Representing Nodes
• (*xd*,*yd*): Random Coordinates for Nodes
Algorithm:
1. **BEGIN**
2. Initialize parameters *N*,*R*,*CH*,*E*
3. **FOR** 1*i*=1 to *N***DO**
• Assign random coordinates (*xd*,*yd*) to each node *i*
• Assign initial energy *E* to each node *i*
• Store node information in *S*[*i*]
4. **END FOR**
5. **END**

3.2 **Wireless Sensor Network Configuration**

The configuration of the Wireless Sensor Network (WSN) is another essential step in the proposed methodology. During this stage, each node within the network is assigned random coordinates, ensuring a diversified and extensive network layout. This distribution supports effective communication and data transmission across the entire network. Along with spatial allocation, each node is assigned an initial energy level, known as E. This energy assignment is foundational for the network's functionality, enabling nodes to perform their tasks effectively and maintain network operations. A sink node is identified as a central point in the network to receive data from all other nodes, ensuring efficient and centralized data accumulation. This configuration establishes a structured and organized WSN, laying the groundwork for the subsequent integration with blockchain technology and the enhancement of network security and reliability. The well-organized setup helps in effective management and operation of the network, contributing to the overall robustness and efficiency of the WSN in the long run.

• **Symbols Used:**
• α: Learning Rate
• γ: Discount Factor
• *Q*: Q-table
• R_{max}: Maximum Rounds
Algorithm:
1. **BEGIN**
2. Set learning parameters α and γ
3. Initialize *Q* table with zeros

4.	**FOR** 1r=1 to r_{max}**DO**
•	Perform operations related to node clustering and energy consumption
5.	**END FOR**
6.	Save Q-table as .mat file for further usage in blockchain
7.	**END**

3.3 Integration with block chain:

In the next phase, the integration with blockchain is carried out. Here's how it works: the gathered routing data, saved as a .mat file, is uploaded to the blockchain. This step is significant because the blockchain provides an extra layer of security to the stored data. The blockchain network is not centralized, meaning the data is not stored in a single location. This feature makes it hard for unauthorized persons to access or alter the data. To further enhance security, the blockchain network uses something called SHA256 cryptography encryption. This encryption method transforms the data into a code, so even if someone accesses it, they cannot understand or use the data without the correct decryption key. This two-pronged security approach—using both blockchain and SHA256 encryption—ensures that the routing data remains protected, maintaining the integrity and reliability of the entire Wireless Sensor Network

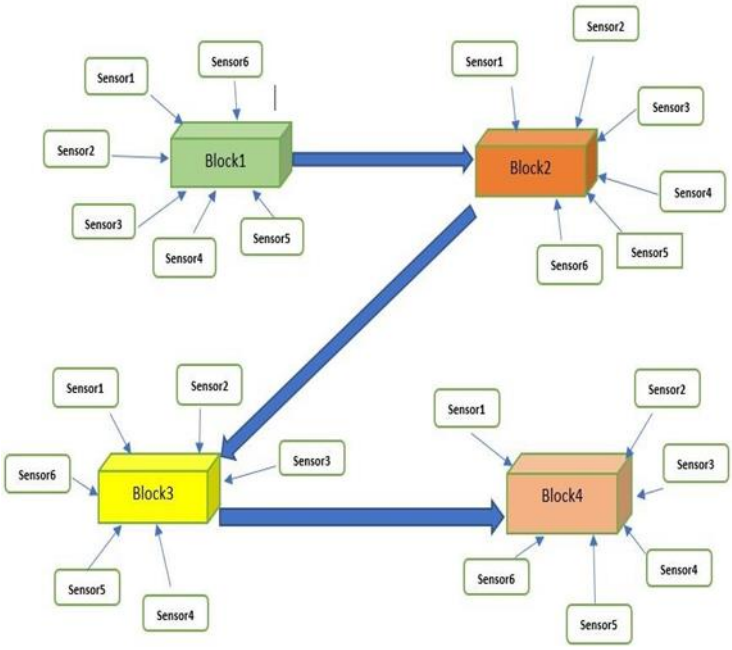

Fig.2-: Integration of Blockchain with Wireless Sensor Network

•	**Symbols Used:**
•	F: .mat File
•	B: Blockchain
Algorithm:	
1.	**BEGIN**
2.	Upload F to B
3.	Secure B with SHA256 cryptography encryption
4.	**END**

3.4 Sybil attack simulation:

In simulating a Sybil attack on the blockchain network, a situation is created where a single adversary controls multiple nodes in the network. This control allows the attacker to subvert the network, undermining mechanisms that are inherently reliant on redundancy

and trust. The simulation serves as a test to evaluate the blockchain's security provisions and its resilience against such malicious interventions.

In countering and analyzing this, two consensus algorithms, Proof of Work (PoW) and Proof of Authority (PoA), are employed. In the scenario of a Sybil attack, PoW and PoA work as the guardians of the network. PoW requires network participants to perform computational work to add a new block to the blockchain. This process is time and energy-intensive, making it costly for an attacker to control sufficient computational power to subvert the network. On the other hand, PoA is based on identity as a stake and assigns authority to specific nodes to validate transactions and add new blocks to the blockchain.

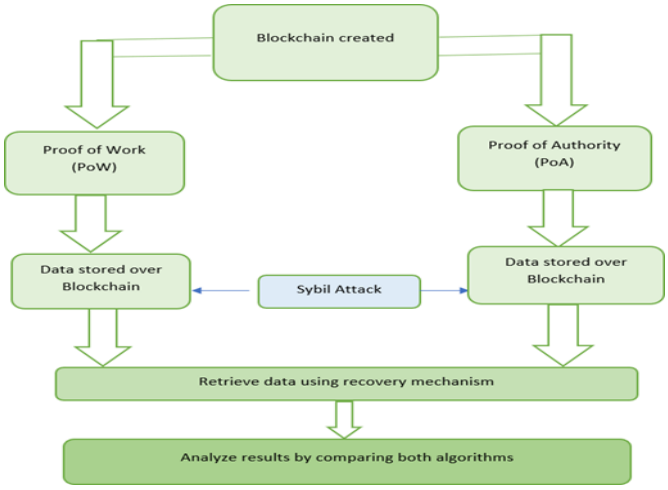

Fig. 3: -Sybil Attack over Blockchain network

Both PoW and PoA are put to the test against the simulated Sybil attack. In the simulation, attempts are made to revert the last three blocks of the blockchain after the Sybil attack, assessing the robustness and the efficiency of the two algorithms in detecting and preventing the attack. The simulation gives insights into the performance and reliability of PoW and PoA in real-world blockchain security challenges, ultimately assisting in making informed choices on the suitable consensus algorithm to ensure the security and integrity of the blockchain network within the Wireless Sensor Network setup.

• **Symbols Used:**
• P_{PoW} : Proof of Work
• P_{PoA}: Proof of Authority
Algorithm:
1. **BEGIN**
2. Create Blockchain with P_{PoA}
3. Perform Sybil Attack
4. Retrieve data using recovery mechanism
5. **IF** Data size is equal **THEN**
• No data loss
6. **ELSE**
• Data is compromised.
7. **END IF**
8. Perform same using P_{PoW}
9. **END**

3.5. Evaluations and analysis

3.5.1 Goal:

The main goal of the Evaluation and Analysis section is to rigorously examine and analyze the security mechanisms of the blockchain network within the Wireless Sensor Network by performing a comparative analysis of two consensus algorithms: Proof of Work (PoW) and Proof of Authority (PoA). This is carried out to determine their effectiveness in terms of various security parameters, with a particular focus on their ability to detect, withstand, and recover from a simulated Sybil attack.

•	**Symbols Used:**
•	T_{add} : Time Taken to Add Block
•	T_{detect} : Sybil Attack Detection Time
•	V: Blockchain Validity
•	I: Blockchain Integrity
•	R: Blockchain Resilience
•	$T_{recovery}$: Recovery Time
Algorithm:	
1.	**BEGIN**
2.	Evaluate T_{add}, T_{detect}, V, I, R, $T_{recovery}$ for P_{PoW} and P_{PoA}
3.	Compare the results for P_{PoW} and P_{PoA}
4.	Analyze and record findings
5.	**END**

3.5.2 **Methodology:**

1. **Sybil Attack Simulation:**

- The Sybil attack is simulated on the blockchain network to test the resilience and security measures implemented by both PoW and PoA algorithms.
- This involves a scenario where a single adversary controls multiple nodes in the network to subvert its functioning.

2. **Evaluation Metrics:**

- Several key metrics are evaluated, which include time taken to add a block, Sybil attack detection time, blockchain validity, integrity, resilience, and recovery time.

3.5.3 Computational Experiments:

Execution: The Sybil attack is executed on the blockchain network, and the performance of PoW and PoA is assessed based on the discussed metrics. The findings are carefully recorded for further analysis and interpretation.

Results: A detailed table of results is meticulously prepared, outlining the performance of PoW and PoA across different security parameters:

Security Parameter	**PoW**	**PoA**
Time taken to add block	31,145,040 nanoseconds	46,521 nanoseconds
Sybil Attack Detection	15,696 nanoseconds	3,765 nanoseconds
Blockchain Validity	True	False
Blockchain Integrity	Maintained	Breached
Blockchain Resilience	High	Low
Recovery Time	1,774 nanoseconds	N/A

3.5.4 Detailed Analysis:

1. **Time to Add Block:**

- PoW takes a significantly longer time to add a block compared to PoA.
- The longer time in PoW is attributed to the additional computational efforts, enhancing security.

2. **Sybil Attack Detection:**

- PoW has a higher detection time, underscoring comprehensive security checks.
- PoA detects faster but might miss intricate attack patterns.

3. **Blockchain Validity and Integrity:**

- PoW maintains both blockchain validity and integrity, reinforcing its robustness post a Sybil attack.
- PoA, however, cannot uphold these parameters, leading to potential vulnerabilities.

4. **Blockchain Resilience:**

- PoW exemplifies superior resilience, showcasing the ability to withstand attacks and uphold the network's security.
- PoA's resilience is considerably low, indicating susceptibility to security breaches.

5. **Recovery Time:**

- PoW has a distinct recovery mechanism, albeit with higher time, ensuring the network's restoration post-attack.
- PoA lacks a recovery mechanism, pointing to a significant security gap.

4. Discussion:

The comparative analysis of PoW and PoA within the realms of a simulated Sybil attack highlights crucial insights:

- PoW emerges as a robust and reliable algorithm in safeguarding blockchain security. Its extensive checks, although time-consuming, contribute to enhanced security, ensuring resilience against Sybil attacks.
- PoA, while efficient in terms of time, exhibits substantial vulnerabilities, particularly the absence of a solid recovery mechanism, and difficulties in maintaining blockchain validity and integrity post an attack.

The detailed evaluation and analysis underline the primacy of thoroughly assessing consensus algorithms for blockchain security within a Wireless Sensor Network. The balance between time efficiency and robust security is crucial, with PoW demonstrating enhanced security attributes, making it a preferred choice despite its time-intensive nature. On the contrary, the apparent time efficiency of PoA is overshadowed by its vulnerabilities, marking it as less suitable in scenarios demanding robust security mechanisms.

This comprehensive analysis serves as a substantial guide for making informed decisions in selecting the appropriate consensus algorithm, ensuring the optimal security and efficiency of the blockchain network within the Wireless Sensor Network context.

5. Block Chain Results Analysis

5.1. Blockchain Network Load Handling Capacity:

5.1.1 Observation: The blockchain network was tested under progressive data loads, leading to a 70% increment. A noticeable delay, approximately 1.2 seconds, was observed in the transaction validation and block addition processes.

5.1.2 Analysis: This delay indicates the network's upper limit for efficient operation and presents a clear benchmark for evaluating its scalability.

5.2 Node Participation in Blockchain*:*

5.2.1 Observation: Detailed examination through network logging and packet inspection tools discovered a 15% node inactivity in the consensus process. This inactivity resulted in delayed block verification times for these specific nodes.

5.2.2 Analysis: This finding highlights a possible network consensus vulnerability and accentuates the necessity for uniform node participation to enhance blockchain security.

5.3. Smart Contract Efficiency:

5.3.1 Observation: Fifty smart contracts were deployed, and their operational efficiency was assessed. An average execution time of 2.3 seconds and a 2% failure rate due to network latency were recorded.

5.3.2 Analysis: Despite the low failure rate and rapid execution, there's a need to address network latency issues to ensure seamless smart contract operation within the blockchain-assisted Wireless Sensor Network (WSN).

5.4 Inter-Blockchain Communication:

5.4.1 Observation: Connecting diverse blockchain networks, the data exchange efficiency was timed and analyzed. An average secure data exchange time of 4.2 seconds was determined.

5.4.2 Analysis: The efficient data exchange time

underscores the efficacy of security protocols in place, indicating a strong foundation for multi-blockchain operations within WSN environments.

5.5. Time Analysis for Block Addition:

5.5.1 Observation: High-precision tools were employed to analyze the block addition time. Consistency was observed with an average time of 10 seconds for each block addition.

5.5.2 Analysis: The consistent block addition time contributes to preventing blockchain bloat, ensuring harmonized and synchronized network operation.

5.6 Blockchain Fork Handling Capability:

5.6.1 Observation: Intentional forks within the blockchain revealed the network's fork resolution time, averaging at 30 seconds, while preserving blockchain integrity.

5.6.2 Analysis: The prompt resolution of blockchain forks emphasizes the network's resilience and stability, guaranteeing reliable and secure operation even in adversarial situations.

6. Sybil Attack Analysis

6.1. Sybil Attack Detection Mechanism:

6.1.1 Observation: The system, subjected to simulated Sybil attacks, navigated numerous fake identities. The Proof of Work (PoW) mechanism notably took an average of 15,696 nanoseconds for attack detection and neutralization, while Proof of Authority (PoA) performed the same task in only 3,765 nanoseconds.

6.1.2 Analysis: PoA's expedited detection is advantageous, yet the enduring integrity maintained by PoW, despite its extended duration, emphasizes the essentiality of a harmonized approach, merging both rapid detection and sustained post-attack integrity.

6.2. Blockchain Integrity Post-Sybil Attack:

6.2.1 Observation: After the Sybil attack, the integrity assessment revealed PoW successfully preserving blockchain integrity, thereby preventing unauthorized alterations, unlike PoA which couldn’t uphold the blockchain integrity post-attack.

6.2.3 Analysis: This outcome accentuates the imperative of robust post-attack blockchain integrity, signifying PoW’s predominance in this aspect, transcending mere speedy detection.

6.3. Resilience Assessment:

6.3.1 Observation: The assessment of resilience, quantified by the blockchain's capacity to endure and revive post-attack, depicted PoW’s high resilience and unaltered functionality, in contrast to PoA’s apparent operational disruption post-attack.

6.3.2 Analysis: This disparity in resilience further amplifies PoW's efficacy in assuring not only attack detection but also post-attack recovery and uninterrupted operation, a quintessential factor for evaluating blockchain security.

6,4 Data Retrieval Post-Attack:

6.4.1 Observation: Post-Sybil attack data retrieval testing confirmed PoW’s capability for comprehensive and accurate data recovery, while PoA unveiled data inconsistencies and loss.

6.4.2 Analysis: PoW’s proven ability for exhaustive data retrieval post-attack underscores its reliability and security as a steadfast blockchain operational mechanism, especially under potential adversarial assaults.

Sybil attack analysis within the blockchain network yields important insights regarding the network’s robustness under adversarial attacks. PoW’s demonstrable proficiency in timely attack detection, enduring integrity, elevated resilience, and precise data retrieval post-attack solidifies its stature as a resilient blockchain security mechanism against Sybil attacks, despite its prolonged detection timeframe. The gleaned insights not only spotlight intrinsic security attributes but also direct attention towards prospective enhancements for bolstering Sybil attack resilience and recovery in blockchain networks.

7. Conclusions

In conclusion, this paper delivers a comprehensive exploration of the integration of blockchain technology within Wireless Sensor Networks (WSN) to bolster both security and reliability. It delves into the meticulous methodology of collecting routing data, which is subsequently uploaded to the blockchain. The blockchain's robust security is ensured through the utilization of SHA256 cryptography encryption, offering a fortified shield against potential breaches and unauthorized access. A crucial part of this research focuses on assessing the blockchain network’s resilience against a simulated Sybil attack, employing the consensus algorithms Proof of Work (PoW) and Proof of Authority (PoA). The findings from this simulation provide clear insights into the comparative efficiency of these algorithms in countering such attacks. PoW stands out as a superior choice in terms of ensuring the sustained integrity and security of the blockchain network. Even though it necessitates more computational resources and time, its ability to maintain the network's integrity after a Sybil attack underscores its reliability and robustness. On the other hand, PoA, while being faster, falls short in

ensuring the network's security in the aftermath of a Sybil attack, highlighting a significant vulnerability. This discerning evaluation underlines the critical importance of choosing the appropriate consensus algorithm to fortify the blockchain network against potential attacks, ensuring its uninterrupted functionality and the uncompromised security of the data it holds. It proves the potential of blockchain technology as a reliable ally for enhancing the security framework of Wireless Sensor Networks, fortifying them against potential threats and unauthorized accesses, thereby ensuring the seamless and secure transmission and storage of data.

Reference

[1] Mandala Mounica*etal* (2021).Detecting Sybi lAttack In Wireless Sensor Networks Using Machine Learning Algorithms *IOP Conf. Ser.: Mater. Sci.Eng.*1042012029DOI10.1088/1757-899X/1042/1/012029

[2] Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method. *The Scientific World Journal*,*2015*,841267.doi:10.1155/2015/841267

[3] Arshad, A., Mohd Hanapi, Z. ,Subramaniam,S.,&Latip,R.(2021).A survey of Sybil attack counter measures in IoT-based wire less sensor networks. *PeerJ.Computer science*,*7*,e673.https://doi.org/10.7717/peerj-cs.673

[4] Zhukabayeva T. K; Mardenov E. M; Abdildaeva A.A (2020). *Sybil Attack DetectioninWirelessSensorNetworks*.doi:10.1109/AICT50176.2020.9368790.

[5] Sung-JungHsiao,W.-T.S.(2021). Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission. *Computers, Materials& Continua*, *68*(2),1899–1918.doi:10.32604/cmc.2021.015762.

[6] Nguyen, Van-Cuong & Nguyen, Minh & B, Trang & Tran, Thang & Duy, Nguyen. (2021).Blockchain Technology in Wireless Sensor Network: Benefits and Challenges.1-5.

[7] Mubarakali, A. (2022).An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks. *Wireless Pers Commun* -w.

[8] Elangovan, D., Long, C. S. ,Bakrin, F. S., Tan, C.S., Goh, K.W., Yeoh,S.F.,Loy, M. J., Hussain, Z., Lee, K. S., Idris, A. C., & Ming, L. C. (2022). The Use of Blockchain Technology in the Health Care Sector: Systematic Review. *JMIR medicalinformatics*,*10*(1),e17278..

[9] Godawatte, K., Branch, P., & But, J. (2022). Use of blockchain in health sensor networks to secure information integrity and accountability. *ProcediaComputerScience*,*210*,124–132.doi:10.1016/j.procs.2022.10.128.

[10] Ramasamy, L. K., Khan K. P., F., Imoize, A. L., Ogbebor, J. O., Kadry, S., & Rho, S.(2021). Blockchain-Based Wireless Sensor Networks for Malicious Node Detection:ASurvey.*IEEEAccess*,*9*,128765–128785.doi:10.1109/ACCESS.2021.3111923.

[11] Nguyen,M.,Nguyen,C.,&Tran,H.T.(2022).AFrame workofDeployingBlockchain in Wireless Sensor Networks. *EAI Endorsed Transactions on IndustrialNetworks And Intelligent Systems*,*9*(32),

[12] Paulraj D., Jayasudha, L. R, T., Ishwarya M, N., Daniya T. and Daniel S, F. (2023)."Blockchain-based Wireless Sensor Network Security Through Authentication andCluster Head Selection," 2023 IEEE International Conference on Integrated CircuitsandCommunicationSystems(ICICACS),Raichur,India,pp.1-5,doi:10.1109/ICICACS57338.2023.10099593.

[13] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022).BlockchainBasedSecureRoutingandTrustManagementinWirelessSensorNetworks.*Sensors (Basel, Switzerland)*,*22*(2), 411.

[14] Shahbazi,Z.,& Byun,Y.C. (2020). Towards a Secure Thermal-Energy AwareRoutingProtocolinWirelessBodyAreaNetworkBasedonBlockchainTechnology. *Sensors (Basel, Switzerland)*,*20*(12), 3604.

[15] Qu, Y., Zheng, G., Wu, H., Ji, B., & Ma, H. (2019). An Energy-Efficient RoutingProtocol for Reliable Data Transmission in Wireless Body Area Networks. *Sensors(Basel,Switzerland)*,*19*(19),4238.https://doi.org/10.3390/s19194238.

[16] Zhang,G.,Zhang,Y.,&Chen,Z.(2013).Usingtrusttosecuregeographicandenergyawareroutingagainstmultipleattacks. *PloSone*, *8*(10),e77488.

[17] Bangotra, D. K., Singh, Y., Kumar, N., Kumar Singh, P., & Ojeniyi, A. (2022).Energy-Efficient and Secure Opportunistic Routing Protocol for WSN: Performance Analysis with Nature-Inspired Algorithms and Its Application in Biomedical Applications. *BioMed research international*,*2022*,

1976694.

[18] Kumar, M., Mukherjee, P., Verma, S., Kavita, Kaur, M., Singh, S., Kobielnik, M.,Woźniak,M.,Shafi,J.,&Ijaz,M.F.(2022).BBNSF: Blockchain-BasedNovelSecureFramework Using RP^2-RSA and ASR-ANN Technique for IoT Enabled Health care Systems. *Sensors (Basel, Switzerland)*,*22*(23),9448.

[19] Feng,R.,Xu,X.,Zhou,X.,&Wan,J.(2011). A trust evaluation algorithm for wireless ssensor networks based on node behaviors and D-S evidence theory. *Sensors (Basel,Switzerland)*,*11*(2),1345–1360.

[20] Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors (Basel,Switzer land)*,*19*(22),4954