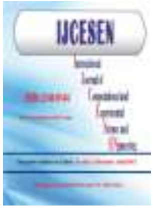
International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.1 (2025) pp. 181-194
http://www.ijcesen.com



ISSN: 2149-9144

Research Article

Blockchain-Enabled Secure Data Aggregation Routing (BSDAR) Protocol for IoT-Integrated Next-Generation Sensor Networks for Enhanced Security

N. Vidhya[1]*, C. Meenakshi[2]

[1]Research Scholar, Department of Computer Applications,Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India
* **Corresponding Author Email:** suresh@sasapublications.com **– ORCID:** 0009-0002-1578-8913

[2]Associate Professor, Department of Computer Applications, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India
Email: cmeenakshi.scs@velsuniv.ac.in **- ORCID:**0009-0006-1566-1399

Article Info:

DOI: 10.22399/ijcesen.722
Received : 03 October 2024
Accepted : 19 December 2024

Keywords :

Blockchain Technology,
Secure Data Aggregation,
Routing Protocols,
IoT Networks,
Energy Efficiency and Big Data,
Analytic.

Abstract:

WSNs, due to their special characteristics as compared to conventional networks, have become the focus of extensive research. A large-scale IoT forms the backbone of billions of resource-constrained next-generation sensors interconnected with each other. Their large-scale deployments remain one of the most serious challenges to existing security mechanisms due to the dynamic characteristics of IoT devices, which could not provide efficient protection against malicious adversaries. Besides, conventional routing protocols are vulnerable to various security threats from the unreliability and open-access nature of the internet. This research article presents a novel blockchain-enabled secure data aggregation model protocol for routing in IoT-integrated next-generation networks using sensor nodes. The BSDAR protocol is capable of improving energy routing performance while ensuring strong node-level data shield against malicious attacks. It first organizes the networking nodal points into autonomous clusters of different radii to effectively avoid energy holes around the BS. Then, the protocol uses the A-star based heuristics strategy to construct well-organized and non-looping routing paths. The BSDAR protocol has integrated blockchain technology with the goal of ensuring the security of the data communication process. In that, end-to-end communication is preserved by a decentralized and tamper-proof approach against malicious nodes. The simulation results prove that BSDAR significantly outperforms existing solutions in energy consumption, throughput, network lifetime and time complexity, thus presenting a promising solution for secure and scalable IoT deployments.

1. Introduction

Through sensing operations, wireless networks of sensors (WSNs) can transfer data among nodes that collect sensors (SNs) and the base stations (BS) or another SNs. However, in terms of consumption of electricity and energy dissipation, transmitting information in WSNs frequently necessitates a large amount of energy [1]. SNs use event monitoring to gather data from their surroundings, which they then send to the BS or the subsequent SN. These networks send data via the World Wide Web or sensor actuators [2], and they frequently function in hazardous areas. Field surveillance, disaster recovery, healthcare, homeland security, agriculture, home automation, environmental monitoring, petroleum refinery monitoring, and industrial operations are just a few of the many uses for WSNs. WSNs encounter a number of difficulties as a result of their deployment in these environments, mainly those associated with resource limitations such as low battery life and computing capacity.

The redundant data created during event monitoring is a key issue in WSNs, as it causes excessive use of energy and congestion in the networks when transferred to the base station (BS) [3]. In addition to depleting SNs' power, redundant data transmission lowers the network's overall efficiency. Local data aggregation—where identical packets of information are gathered and only one copy is transmitted—becomes crucial to address this. After that, an aggregator node is created, which is in charge of eliminating redundant data using statistical, probabilistic, or artificial intelligence techniques [4].

Through pre-transmission removal of duplicate data, the WSN greatly increases its energy efficiency. Moreover, data must go over several hops in order to reach the BS, and sending redundant data over these hops adds even more inefficiency. Preventing redundant transfer of information not only saves network latency but also lowers energy usage. As a result, this strategy improves overall performance and increases the network's lifespan [5]. In Wireless Sensor Networks (WSNs), secure data aggregation (SDA) is essential for energy conservation since it effectively controls the aggregation of detected data via aggregator nodes. Ensuring data availability, secrecy, and integrity while reducing communication overhead (CO) is the main goal of SDA [6]. Through the integration of security control methods like permission and authentication, SDA ensures privacy protection and guards against potential security breaches and cyberattacks. Energy efficiency preservation in the network is greatly aided by the safely aggregating data collected via aggregator nodes. When combining the sensed information, BS makes use of a security control system. In WSNs, confidence control measures like validation and authorization approach are used in secure data aggregation (SDA). Therefore, in a WSN, secure data aggregation minimizes communication overhead (CO) while guaranteeing anonymity, reliability, and accessibility for privacy preservation [7]. Therefore, detected data is used in safe data aggregation, avoiding transmission overhead. As a result, SDA improves the SN's energy consumption while gathering sensed data. Furthermore, SDA protocols are essential. They serve as a firewall, authenticating and approving valid SN data to protect privacy from any network flaws or cyberattacks. This restriction of security management techniques, including secure node permission, makes the lifespan of the WSN a major problem. This difficulty stems from the requirement to accept valid, approved, and authenticated sensor nodes (SN) in order to transmit data securely throughout the network. This raises privacy issues. Therefore, in order to manage data aggregation challenges, effectively address data privacy concerns in order to domain QoS provisioning in the network, a privacy-preserving safe data aggregation approach is desperately needed. Further research into security design is necessary because secure data aggregate is an essential paradigm that eliminates data redundancy and stops unnecessary energy consumption. In order to maintain privacy, researchers have developed privacy-preserving time-series data aggregation algorithms for WSN and submitted encoded values to facilitate the data aggregate. A procedure for data aggregation determines the total SNs of the participants. However, because of restrictions on the network's verification and authorization security control methods, it requires access to discover the contents of the data, which results in communication overhead (CO). However, owing of the limited capabilities of sensor nodes, CO is a major worry in WSNs. CO is decreased via secure data aggregate and SN privacy preservation that lengthen network lifetime. Lowering CO results in detected information in data aggregation, which supports critical WSN application decision-making. However, the final aggregation results' accuracy matters a lot. In order to provide safe data aggregation, researchers developed the Environmentally friendly and high-accuracy (EEHA) technique [8]. EEHA seeks to minimize communication overhead and accomplish precise data aggregation without disclosing private sensor information. The goals of the suggested EEHA to lower communication overhead were met. However, from the perspective of privacy-preserving secure data aggregation security, the suggested solution only partially applicable to real-world scenarios.

For WSNs built by hacked sensor nodes, false sub-aggregate values pose a security risk. Significant mistakes are produced at the base station in this kind of attack. Because each SN in the network must be authorized by the EEHA protocol, fake sub-aggregate attacks limit the nodes' ability to authenticate and obtain authorization. A fake sub-aggregate error summary diffusion (SD) [9] technique only decreased false errors in WSNs due to restricted authorization. The algorithm used by the base station (BS) to safely compute the sum in the face of susceptible or compromised assaults is known as SD. In order to prevent the contributions from conceded sensors in the aggregation hierarchy, the SD algorithm additionally assisted in calculating the true aggregate. Cyber threats, on the other hand, are well-known vulnerabilities or assaults that jeopardize the confidentiality and integrity of legitimate nodes because of weak authentication and permission. Examples of these are the sybil node and sinkhole node. The sent data from the sensor node are therefore not safe.

Three specific key contributions of the research have been highlighted below:

- This paper proposes a blockchain-enabled secure protocol for data aggregation route protocol, BSDAR, for IoT-integrated sensor networks. The blockchain-based approach ensures a decentralized and tamper-proof mechanism for robust data protection with secure end-to-end communication. The proposed protocol BSDAR is based on integrating blockchain to effectively handle various security challenges due to large-scale deployment of IoT devices and threats from malicious nodes.

- BSDAR is based on an effective clustering strategy; that is, it groups the entire network into independent clusters of variable radii. Hence, energy holes around BS can effectively be prevented by this protocol, improving the routing performance of its energy. In order to optimize network routing and minimize delays, it employs the A-star heuristics technique to obtain effective loop-free routing paths.
- The simulation results demonstrate that, in most critical performance metrics such as energy consumpting, network lifetime, end-to-end delay, and packet drop ratio, BSDAR outperforms the existing state-of-the-art solutions. This advancement marks the efficiency of BSDAR in balancing energy efficiency with secure data aggregation, hence making it a promising solution toward scalable and secure IoT deployments.

Related works

The relevant research on the suggested model that is currently available is provided in this section. The authors in [10] suggested protecting data and key private (PDKP) for gathering data for wireless detectors that collected data and privacy protections for key in data aggregation in WSN. PDKP uses encrypted data and does so without sharing any part of the data or its key with other SNs by employing simple techniques. The protocol shields the key from a competitor and the data content with little computational cost. There is no authorization or authentication system in the PDKP approach that is being suggested. The authors of [11] proposed the Energy-efficient and Secure Data Collecting Algorithm (EPDA) as a way to lower energy usage and lengthen network lifespan. Nodes for sensors were placed in a tree and connected to the nodes that represent the leaves of the tree to form chains. To ensure network anonymity, the chains' tail SN nodes were cut, and the EPDA solely used sensed data. Nevertheless, permission and authentication methods are absent from the proposed method. In order to shield keys and information in data aggregation to preserve data and crucial privacy in wireless sensors with multiple sinks, the authors of [12] introduced the concept of secure data aggregates for preserving data and key confidentiality (SAPDKP). The overhead of processing and transmission is reduced when there are multiple drains. Nevertheless, data integrity, freshness, and confidentiality [13], as well as data authentication, are security problems. SAPDKP employs a simple encryption and aggregation method and does not use any permission security features.

Instead of addressing a realistic simulation of an actual case, the authors of [14] solely addressed the privacy-preserving average consensus (PPAC) [15] issue; they failed to tackle a one-dimensional state. Therefore, they suggested using multidimensional confidentiality average consensus in wireless sensor networks (MPPAC). MPPAC divides nodes into two groups: sink nodes and normal nodes. MPPAC was used to introduce the RSA algorithm and a super-increasing series to the network. The RSA achieved anonymity by maintaining average consensus only across sink nodes; nevertheless, the suggested method necessitated authorization and authentication procedures. Managing any complex measurement in the sensors was made possible in large part by this super-increasing sequencing.

In order to create an efficient aggregate of data in WSNs that preserves both confidentiality and integrity, the authors of [16] proposed an ensemble approach for multiple applications (PIMA) in WSNs. PIMA leverages homomorphic security for combining hybridized sensor data into real WSN applications. The suggested protocol needed to utilize sensors placed in diverse environments and meet the requirements of a multi-application environment. To ensure the quality of the collected information and preserve data privacy, PIMA used homomorphic MAC and Paillier encryption. Nevertheless, no security measures for authentication or authorization were in place. For WSNs, the authors of [17] suggested a concept for an energy-efficient and privacy-preserving data aggregator (EPSDA). The EPSDA was developed as a solution to energy-intensive aggregator node decryption, which exposes a significant quantity of confidential data to network adversaries and produces unreliable results. These restrictions were overcome by the suggested EPSDA protocol, which carried out direct aggregates on the homomorphic encryption-encrypted data.

Old data transfers via the network were prohibited by the EPSDA. Nevertheless, the plan did not include any suggested methods for authorization or authentication. The authors of [18] presented CBDA (chain-based data aggregation), a unique environmentally friendly and privacy-preserving data aggregation mechanism for WSNs.

Sensor nodes (SNs) were arranged into tree topologies by CBDA, where leaf nodes progressively reconnected to form chain topologies. By compiling and dividing sensing data into smaller pieces, tail nodes in the network maintain data privacy. In the suggested design, the CBDA approach did not make use of any authentication or permission mechanisms.

Two primary methods are used in the privacy-preserving safe data aggregation approach: the first uses cryptography to enable the process of aggregation to decode the data aggregate or sum using various keys. The second method prevents data breaches by applying the differentiated privacy strategy [19].

As a result, the authors of [20] presented secure data aggregation watermarking (SDAW), an energy-preserving technique based on homogeneous WSNs. To ensure integrity and authentication, SDAW used flimsy, lightweight watermarking without encryption. Because the network's authorization is limited, malicious nodes may try to inject fake data in an effort to trick other nodes and obtain crucial information. There was no authentication or authorization security mechanism included in the planned SDAW.

As a result, malevolent or adversarial nodes in WSNs compromise data and raise concerns about confidentiality. The compromised data increases the network's energy consumption, which in turn increases transmission overhead. A workable secure data aggregation (SDA) technique was put forth in as a remedy for compromised data in order to protect data privacy and stop excessive energy use. Concerns about communication cost resulted from this SDA approach's usage of additive homomorphic, identity-based authentication and batch validation approaches with a suggested methodology to filter fake data inserted by rogue nodes without authorization.

Nevertheless, an identification and authorization system is required by the suggested SDAAA security mechanism technique. WSNs need to be made aware of and look into these design issues using secure secure data formation protocols and popular methods like SD, EEHA, HAS, IIF, and RHC.

From the related work outlined, the research gaps noted include:

- A large number of protocols have weak mechanisms for authentication and authorization.
- Some of them do not take into consideration multi-dimensional network scenarios; hence, their usability becomes limited.
- Most of these systems do not have integrated measures for security and efficiency, hence compromising data integrity.
- Large-scale and diverse network environments have challenged all exiting techniques.
- This does not provide enough protection against malicious node activities since it would affect network security and energy efficiency.

2. Material and Methods

2.1 Proposed BSDAR taxonomy

The proposed BSDAR protocol's framework is explained in this section. An early topology construction approach is given in the first section. The second section explains how the A-star heuristic algorithm generates dynamic routing trees. Node level data security is built with the least amount of processing and computational overheads in the final section. A few network presumptions are addressed before delving into the detailed design of the suggested LSDAR protocol.

The following are the constrains of the proposed work.

- Each and every sensor node is consistent, stationary, and distributed randomly.
- Positioning algorithms or GPS are utilized to determine the node's location.
- BS is not limited by resources in any way.
- RSSI can be used to modify the transmission control of sensor nodes.
- Symmetric communication lines are used to transmit data.

2.2 Organization of BSDAR protocol

As illustrated in Figure 1, the LSDAR protocol's structure consists of components for data security, heuristic routing trees, and initial topology creation. Sensor nodes establish their initial routes in the first component to point at the location of the base station. Consequently, every node builds its neighbor table by putting relevant data in storage. Additionally, sensor nodes break down into clusters of different sizes based on different radii. Adjacent clusters to the BS may therefore be weaker than distant ones. Therefore, by reducing the energy consumption of forwarders that are situated close to BS, the suggested procedure lowers the likelihood of an energy hole. To calculate the evaluation function f(n), the LSDAR protocol's second component uses a weighted combination of RSSI and residual energy attributes to launch the A-star heuristic routing tree algorithm. As a result, low-cost and energy-efficient networks are preferred when choosing forwarders. Furthermore, by assessing the status of nodes and network limitations, the values of attributes are changed dynamically. The suggested standards for forwarder selection significantly increase network availability and ensure the effectiveness of data broadcast. In the third part, data protection against hostile nodes is offered by investigating the XOR mathematical operation among communication devices.

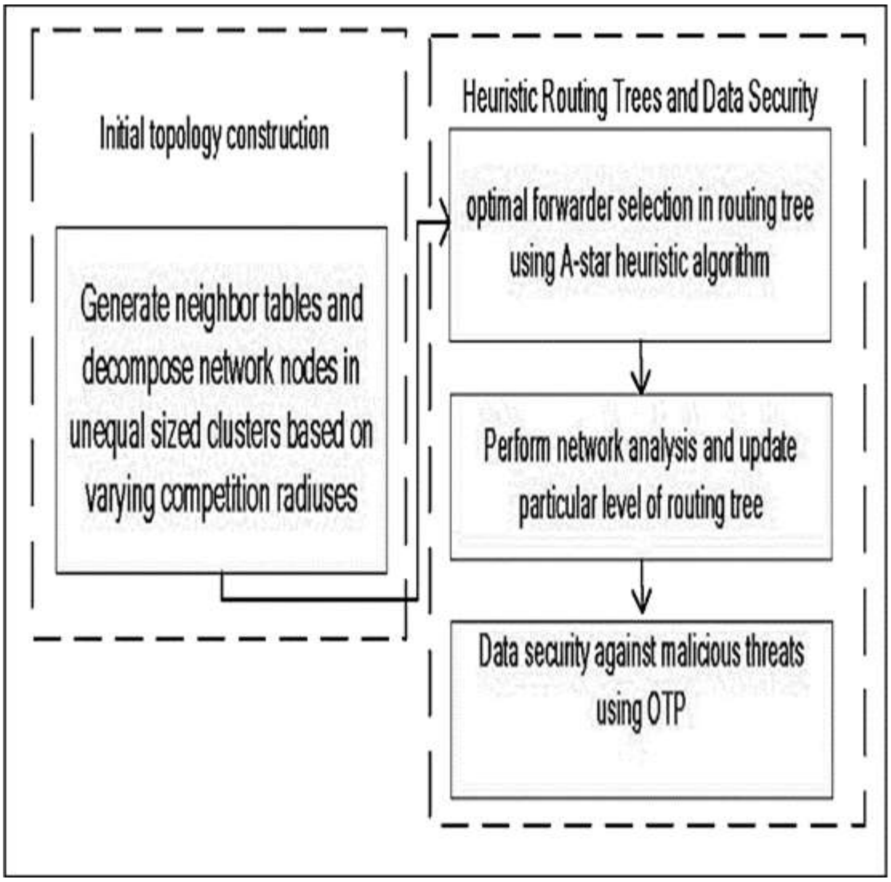

Initial topology construction
Generate neighbor tables and decompose network nodes in unequal sized clusters based on varying competition radiuses
Heuristic Routing Trees and Data Security
optimal forwarder selection in routing tree using A-star heuristic algorithm
Perform network analysis and update particular level of routing tree
Data security against malicious threats using OTP

Figure 1. *BSDAR Protocol model*

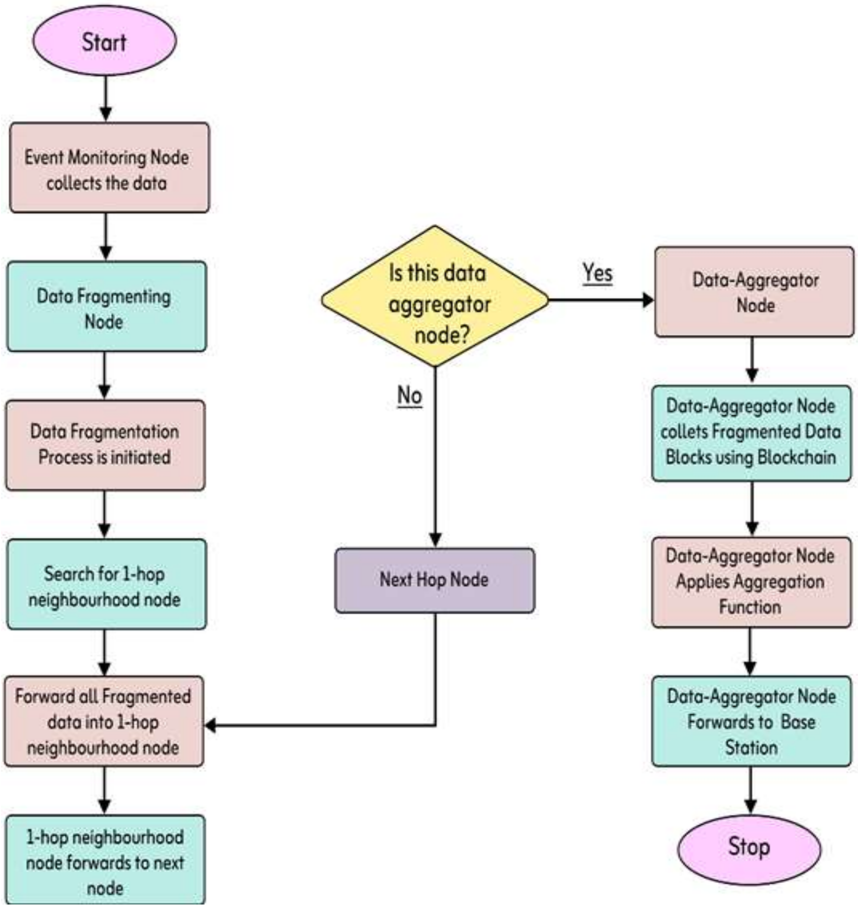

Start
Event Monitoring Node collects the data
Data Fragmenting Node
Data Fragmentation Process is initiated
Search for 1-hop neighbourhood node
Forward all Fragmented data into 1-hop neighbourhood node
1-hop neighbourhood node forwards to next node
Is this data aggregator node?
Yes
No
Next Hop Node
Data-Aggregator Node
Data-Aggregator Node collets Fragmented Data Blocks using Blockchain
Data-Aggregator Node Applies Aggregation Function
Data-Aggregator Node Forwards to Base Station
Stop

Figure 2. *Blockchain integration flow with BSDAR*

2.3 Phase 1: initial topology construction

The first element is that the location of the BS and its neighbors must be known by all sensor nodes. As a result, for the routing structure, each node builds its neighbor table. First, by sending an announcement message with position and ID data, BS starts the process of constructing the topology. A node's distance from a base station is calculated using the RSSI value. The process of developing a network only involves the development of the initial topology once. The network field is separated into variable sections as depicted in Figure 2 in accordance with each node's competition radius Rc, which must be determined during nodes decomposition and is shown in Eq. (1).

$$Rc = 1 - (disti\ to\ BS/distmax)Rmax \qquad (1)$$

Distmax is the farthest nodes distance from BS, Rmax is the maximum radius, and disti to BS indicates the node's distance from BS in Eq. (1). Because of this, nodes within Rc's range compete with one another to become cluster chiefs. As the first cluster heads, the LSDAR procedure then chooses the nodes with the highest residual energy inside the Rc range. The size of the cluster is also a function of distance from the base station because of computing at different rates. As the cluster heads' distance from the base station rises, the LSDAR procedure subsequently reduces the group size closer to the BS and increases it. Following the announcement of their information in the network field, the chosen cluster heads formed clusters by sending cluster_join messages to the closest cluster heads from regular nodes. Time Division Multiple Access (TDMA) slots are assigned to each of the chosen cluster heads in order to facilitate data transmission. In multi-hop communication, the purpose of unequal cluster creation is to counteract the non-uniform energy consumption of cluster heads in the neighborhood of the base station. Furthermore, the tiny clusters close to the BS suggest that there are fewer cluster members and less intra-cluster data forwarding. This balances the load distribution across cluster heads, so resolving the energy whole problem.

2.4 Phase 2: Routing based on heuristics

This part of the LSDAR procedure builds a dynamic routing tree using the A-star method to determine the best route from cluster heads to the base station. The key objective of the suggested approach is to create a heuristic route trees and identify, from a pool of options, the best node to use as a forwarder in order to ensure network scalability and dependability. Moreover, the suggested method restructures just specific routing tree edges with negligible communication overhead and dynamically measures the network limitations.

The undirected graph G (S,V,W), which is made up of nodes with sensors S, wireless links E, and efficiency metrics W to assess the wireless links, illustrates the routing tree T process. Since e(n_i, n_j)∈ E indicates that ni and nj are data forwarders, it can be inferred that there is direct communication between the $n_i$and n_j nodes for the purpose of sending and receiving data packages. A route tree is set up so that connections between forwarders are made based on the best criteria and that no forwarder has a cycle.

A-star, a Best First Searching (BFS) algorithm, finds the quickest routing path from the source node to the destination depending on the cost value (Allouche et al., 2015; Russell & Norvig, 2016). Using the remaining energy and RSSI parameters, we optimize A-star's routing decision in the suggested solution. The suggested method keeps the pathways that originate from the source nodes and spreads them out one edge at a time till the destination receives the data packets. There are two lists in the A-star algorithm: an OPEN list and a CLOSED list. Every node that has been assessed is added to a CLOSED list, and the nodes that still require evaluation before being routed are added to an OPEN list. As demonstrated in Eq. (2), the A-star method determines the best routing path based on the g n( ) and h n( ) functions.

$$f(n) = g(n) + h(n) \qquad (2)$$

The function of assessment of the A-star method is represented by Eq. (2), where n denotes the next node that requires evaluation, g(n) represents the price of moving from the basic-source node to the next node, and h(n) is a conservative value derived from the straight line distance between the next node and the destination. According to Eq. (3), the suggested LSDAR method maximizes the g(n) operation in a weighted manner taking into account the residual energy e_n and the signal that was received intensity indicators $RSSI_n$ components.

$$g(n) = a^{*}e_n + \beta^{*}RSSI_n \qquad (3)$$

In equation (3), where α+β = 1, both β and α are weighting issues that indicate their contribution to the routing choice for the forwarder selection process utilizing the A-star method. Consequently, 100% must be the sum of both α and β. The values of e_n and $RSSI_n$ fall within the same range corresponding to the calculated g (n) value, which is between 0.0 and 1.0. First, the LSDAR protocol contributes to the network lifetime by assessing the neighbor's remaining energy status when making routing decisions. For example, if c_e is the quantity of energy consumed to transmit n data bits and $init_e$ is the starting energy, LSDAR uses Equation (4) to calculate the residual energy e_n.

$$e_n = init_{e-\sum_i^n c_i} \qquad (4)$$

In addition, the LSDAR protocol makes use of RSSI as a connection quality factor to improve packet reception ratios and lower retransmission rates. In order to build a dynamic route tree, the LSDAR protocol uses limited control messages to save transmission power by choosing the forwarder according to the highest possible evaluation function Max(f(n)). Instead of flooding the chosen forwarder, a unicast message is forwarded to them. The chosen forwarder nodes receives information packets from its downstream neighbor, combines them with its own, and then sends the combined data packets toward the destination in accordance with the evaluation functional f(n). Furthermore, the LSDAR protocol analyzes the network and updates the routing tree's central locations in response to changing circumstances. Every node unicasts several probing packets to the forwarder of its choice on a regular interval to determine routing holes. It then record the Estimated Transmission Count (ETX) (De Couto et al., 2005) as indicated by Equation (5). Essentially, the rates for forward delivery D_f and reverse distribution D_r ratios are used by ETX to calculate the link value. When the recorded ETX value surpasses a predetermined threshold, the forwarder selection process is re-started by the source node using the f (n) value. Algorithm 1 controls LSDAR protocol's elements.

$$ETX_{ij} = \left(\frac{1}{D_f * D_r}\right) \qquad (5)$$

2.5 Data security algorithmic phase

Given the unreliability of the Internet and the fact that thousands or even hundreds of thousands of nodes can use it at once, data security is a crucial limitation in Internet of Things integrated next-generation sensor networks. In order to speed up the route re-discovery process and raise network overhead, rogue nodes may attempt to reduce network connectivity. Malicious nodes may also modify data packets prior to, during, or even after transmission. The data security in the suggested protocol is accomplished at the BS and cluster levels. Imagining a scenario in which there are all of the tclusters encircling the BS. Clusters located closer to the base station (BS) have the ability to send encrypted data directly, while clusters farther away from the BS must use multi-hop routes to deliver encrypted data. The BS creates t randomized secret keys ($k_1 \dots\dots\dots k_i$) of b bits, which is identical to the size of the data packet, in order to confirm secure data transfer. The heads of each cluster receive their respective secret keys. XOR is used to encrypt information D_n from the nth closest head of the cluster.

$$E_n = k_n + D_n \qquad (6)$$

Likewise, the information originating from the remote nodes is safely transmitted to the base station via a multi-hoping routing method, employing the identical XOR encoded technique as specified in Equation (6). The closest cluster head receives encrypted information from a distant cluster head. The host group h will use its own secret key, "k_h," to encrypt the data after receiving it encrypted using Equation (7).

$$E_n = k_h + E_t \qquad (7)$$

Up until it reaches the BS, the encryption moves from every group to the closest cluster. The decryption procedure begins when BS gets the encrypted data packages from a certain cluster head. Using the XOR method of the encrypted information with each key and Equation (8), BS is able to decrypt the data.

$$D_t = k_1 + E_2 + k_3, \dots. + E_n \qquad (8)$$

2.6 Block-Chain Methodology for Fundamental Ledger Operations

Block-chain is a type of decentralized and distributed ledger technology. It records the transactions conducted by several nodes of a network. Each block in this chain contains many transactions, each having a cryptographic link to its previous block, thus forming a sort of unbroken chain. The major features of block-chain technology include:

1. Decentralization: This block-chain is a network of nodes, with every node having a full copy of the ledger - in contrast to conventional databases managed by some authority. It further cements robustness and security into the system.

2. Immutability: Once a block is added to a block-chain, it can hardly be changed or deleted with respect to its data, without changing all subsequent blocks. This is due to the fact that cryptographic hashing provides immutability, which *secures a* block in such a way that each block is inculcated into the previous block.

Algorithm 1: Algorithm for Blockchain-Enabled Secure Data Aggregation Routing (BSDAR)

```
Step 1: Initialization
    1.  Input Parameters:
            • No: of nodes NNN
            • No: of clusters kkk
            • Cluster radii
            • Block-chain parameters
            • A-star heuristics parameters
    2.  Network Setup:
            • Deploy NNN sensor nodes in the network area.
            • Define the base station (BS) location.
            • Initialize block-chain ledger for data transactions.

Step 2: Node Clustering
    1.  Cluster Formation:
            • Divide the network into clusters with varying radii around the BS.
            • Assign nodes to clusters based on their distance from the cluster center.
            • Ensure that each node is assigned to a cluster with minimum distance to the cluster head.
    2.  Cluster Head Selection:
            • Select a cluster head (CH) for each cluster based on criteria such as remaining energy, node degree, or
              node centrality.
            • Use a consensus mechanism to validate the selection of CH.
Step 3: Routing Path Construction
    1.  A-star Heuristics Initialization:
            • Initialize the A-star algorithm with the start node (source) and the end node (BS).
            • Define cost function based on factors such as distance, energy consumption, and path reliability.
    2.  Path Calculation:
            • Use the A-star algorithm to compute efficient, loop-free routing paths from nodes to the BS.
            • Update routing paths dynamically as the network topology changes.
Step 4: Data Aggregation and Block-chain Integration
    1.  Data Aggregation:
            • Nodes collect and aggregate data within their respective clusters.
            • Cluster heads aggregate data from all nodes in their cluster and prepare it for transmission.
    2.  Data Transmission and Block-chain Logging:
            • Encrypt aggregated data before transmission.
            • Log data transactions in the block-chain ledger to ensure data integrity and tamper-proofing.
            • Use the block-chain to verify and authenticate data transmissions.
Step 5: Security and Data Protection
    1.  Data Encryption:
            • Apply encryption techniques to secure data during transmission.
            • Use the block-chain to store encryption keys securely.
    2.  Malicious Node Detection:
            • Monitor network activity for signs of malicious behavior.
            • Use consensus and verification mechanisms to handle data from suspected malicious nodes.
Step 6: Performance Evaluation
    1.  Simulation and Testing:
            • Run simulations to test BSDAR protocol performance.
            • Evaluate metrics such as energy consumption, network lifetime, end-to-end delay, and packet drop
              ratio.
    2.  Result Analysis:
            • Compare BSDAR results with other state-of-the-art solutions.
            • Adjust parameters and refine the protocol based on performance feedback.
Step 7: Iteration and Optimization
    1.  Algorithm Refinement:
            • Continuously refine clustering, routing, and data aggregation methods based on simulation results.
            • Optimize block-chain integration for improved efficiency and security.
    2.  Protocol Updates:
            • Update the BSDAR protocol to address new challenges and improve performance based on ongoing
              research and development.
```

3. Accord(consensus) Mechanism: The consensus algorithms, such as Proof of Work and Proof of Stake, are used by block-chain networks to validate the transactions occurring on the network and further add them to the block-chain. The use of a consensus mechanism guarantees that all nodes in the network reach an agreement on the validity of transactions to prevent any fraudulent activities.

4. Transparency: All the transactions recorded on the block-chain are visible to any participant of the network. This transparency ensures audibility and verifiability of all the transactions by any participant, hence trusting the participants and accountability of transactions.

5. Security: Block-chain utilizes cryptography techniques in securing the data. Each transaction is encrypted and hashed with a hash function, where each subsequent transaction links to the previous, making tampering with data by unauthorized parties almost impossible.

2.7 Block-Chain Integration in BSDAR

The BSDAR protocol avails block-chain technology in the basic integration of data aggregation and routing with security and integrity in IoT sensor networks. Further, the incorporation of block-chain addresses some important critical dimensions, which include but are not limited to the following:

Integrity of Data and Authentication

The block-chain ledger logs every transaction of data in a tamper-proof manner. This ascertains that all data collected from sensor nodes would be recorded in a non-repudiable fashion such that it will be traceable back to the creator.

Encryption: Data sent over the network by every device is first encrypted prior to logging on the block-chain. Encryption of data in this manner protects it against unauthorized access and manipulation.

Secure Data Communication

Self-executing scripts on the block-chain that enforce pre-defined rules and agreements; smart contracts will be applied to validate data aggregation and routing protocols in BSDAR to ensure that only valid data can be processed and transmitted.

Consensus Mechanism: Block-chain's consensus algorithm ensures that the majority of nodes agree to the validity of the data before adding them to the block-chain; this guarantees malicious nodes cannot corrupt the data.

Malicious Node Mitigation

Since block-chain is tamper proof, the manipulations in data or introduction of fake data by malicious nodes are traceable. Block-chain, being transparent, is thus used independently by network participants to verify and validate data.

Energy Efficiency and Optimization

BSDAR provides avoidance of redundant checking and retransmission required for the purpose of data integrity and authentication by utilizing block-chain; hence, it optimizes energy consumption within the network.

Efficient Routing: Block-chain can efficiently enable routing by maintaining a secure, valid record of the past in transactions, hence this enables pathfinding and data aggregation more effectively. Likewise, Block-chain technology secures the BSDAR protocol by offering a tamper-proof, transparent record of data exchanges. With this integration, integrity ensuring the data from tampering secures the processes of data aggregation and routing efficiently.

3. Results and Discussions

3.1 Empirical Results

Several simulations were performed for the proposed BSDAR protocol evaluation in realistic large-scale IoT-integrated WSN scenarios. The OMNeT++ simulator was chosen for the simulations because it is very well-suited for modelling and analysis of network behavior under various conditions. It was meant to test the performance of BSDAR in energy consumption, network lifetime, end-to-end delay, and packet drop ratio in contrast to other state-of-the-art protocols such as SD, EEHA, HAS, IIF, and RHC.

The proposed BSDAR protocol is evaluated for energy consumption, network lifetime, end-to-end delay, and packet drop ratio. Energy consumption was the critical factor whereby the approach needed to consume the least possible power at all sensor nodes to maximize the time for which the network could be operational. Network lifetime can be defined in terms of time for which the network can stay up, and this largely depends on the fact that it needs to avoid energy holes at the BS for its efficient routing. Another relevant metric was the end-to-end delay, the time taken for data packets going from source to destination, where optimization of this aspect used an A* heuristics algorithm for the purposes of a loop-free and efficient routing. Then, the drop packet ratio was taken, which determines the amount of lost data packet during transmission, then studied to show data integrity and reliability in the presence of malicious nodes and network congestion. In general, the BSDAR protocol outperformed the other state-of-the-art solutions in terms of these performance metrics. This table 1 summarizes the key parameters and features involved in the simulation setup.

3.2 Throughput assessment

Figure 3 depicts the average quantity performance of the suggested BSDAR approach and reflects how much the competing protocols data transmission rates have increased. Indeed, for this purpose, the achieved average throughput by the BSDAR approach is 444 kb/s, which proves that the proposed approach can manage the flow within the WSN to guarantee a high-speed and reliable communication. This is quite observable when compared with other procedures such as SD, EEHA, HAS, IIF, and RHC, which have a little lower throughput, ranging between 415 and 443 kb/s. As the number of sensor nodes increases, the protocol BSDAR outperforms others. This matter is vital because, for large-scale networks, it is required to keep the throughput high for the data aggregation and the transmission to be effective. The routing mechanisms are optimized in BSDAR for less congestion and packet loss; hence, superior throughput performance. Also, its authentication and authorization processes for controlling data aggregation in a secured manner without introducing significant overheads have been designed in such a manner that makes it maintain high throughput even in scenarios with a large number of sensor nodes. This in turn reduces energy losses due to redundant and malicious data transmission by ensuring only authenticated data is being transmitted, further increasing the efficiency of the network. Figure 3 summarizes that the BSDAR protocol offers efficiency in handling high-throughput data transmission, especially for scalability in the network, in comparison with other renowned protocols.

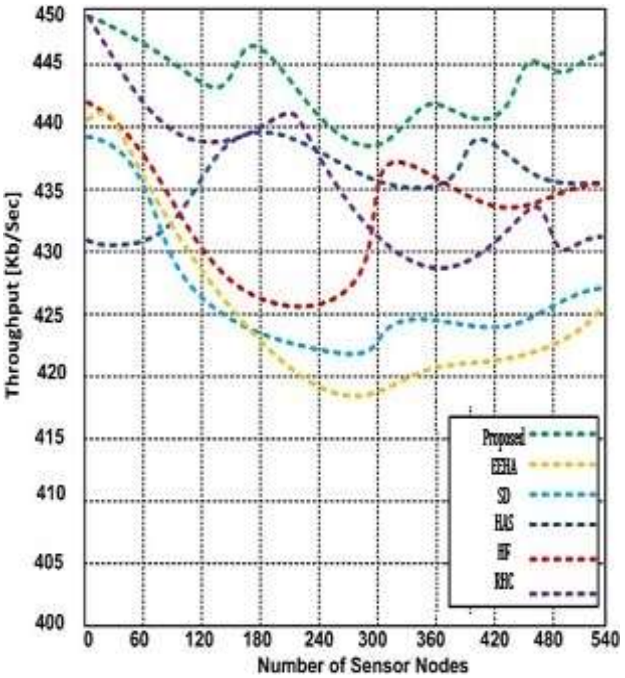


Figure 3. *Throughput computation*

3.3 Energy utilization assessment

Figure 4 shows the effect of malicious nodes on the energy consumption of WSN, for scenarios where 2% of nodes in the network have been compromised. Generally speaking, malicious nodes increase the energy expenditure of the network because of many overheads involved in handling and securing data against possible attacks.

The proposed BSDAR approach, in this adversarial setting, has been observed to consume about 2.91 joules of energy over 36 rounds of event monitoring. This can be interpreted as a fair energy efficiency boost compared to the rivaling approaches such as SD, EEHA, HAS, IIF, and RHC with each of them consuming energy in the range of 3.5 to 3.94 joules in similar event-monitoring scenarios. This may be due to the strong security mechanisms it possesses, coupled with low resultant energy overhead. Energy efficiency in the BSDAR protocol is achieved by the application of efficient data aggregation techniques and secure routing strategies that minimize the resultant energy expenditure in transmitting and processing data. Hence, the proposed BSDAR approach helps in reducing extra consumption of energy that might result from dealing with compromised nodes through actualizing of data authentication and managing of data without the influence of malicious input. This is because most competing protocols are prone to heightened energy consumption based on poor measures put in place while handling malicious nodes. Such approaches may require additional energy in verifying data through security measures, retransmissions, and/or repair mechanisms, thus predisposing them to high energy utilization. Figure 4 thus shows the added value of BSDAR in maintaining energy efficiency under adversarial conditions, hence showing its suitability for energy consumption optimization while ensuring security and performance.

3.4 Resilience vs network lifespan assessment

Figure 5 illustrates the performance of the BSDAR approach in a malicious attack condition wherein 5% of the nodes in WSN are compromised by malicious actors. The figure shows the impact of such a malicious attack on network resilience and the percentage of the network affected. In this regard, the BSDAR approach reflects a much lower network impact when compared with other competitive methods.

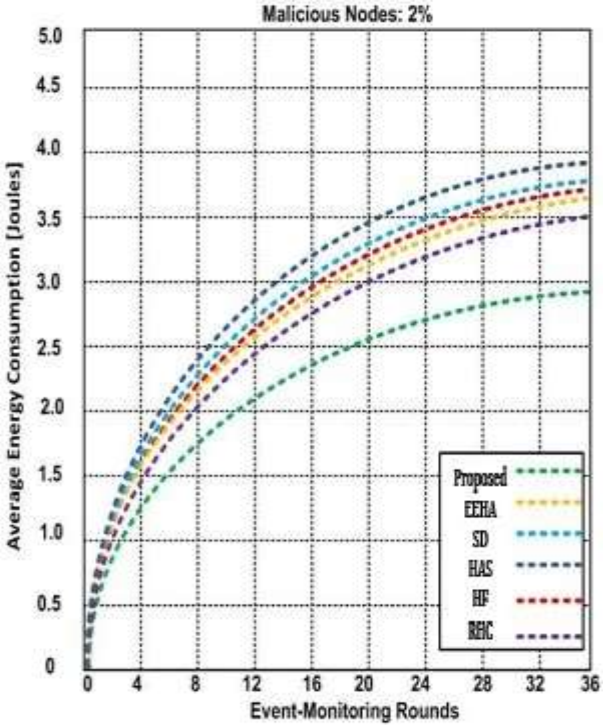


Figure 4. Energy utilization computation

The named approach of BSDAR allows only 2.62% of the network to be impacted because of malicious nodes. Thus, in comparison, the percentage of impact on the network is lower it shows that this BSDAR approach works more effectively in performance and integrity when there is a considerable portion of compromised nodes within the network. Moreover, the resilience time of the BSDAR approach is reported as 0.9%. Once more, this metric will reflect the time during which the network could keep up its functionality working effectively in the presence of malicious nodes. The greater the value of resilience time, the longer the BSDAR approach will maintain the functionality and performance of the network longer under adversary conditions, thus assuring even better stability and reliability.

In contrast, other competing approaches like SD, EEHA, HAS, IIF, and RHC demonstrate a higher range of network impact that lies between 3.68% and 4.38%. These methods show less effective handling of malicious nodes in action, thus compromising a higher percentage of the network. Even though the resilience times for all these methods are the same, at 0.9%, their higher percentages of affected networks demonstrate that they are less efficient in mitigating the adverse effects caused by malicious nodes. Figure 5, in general, reinforces that the BSDAR approach minimizes the malicious nodes' impacts and offers more resiliency in the network. The two higher reduction factors of the affected network percentage and consistent resilient time make the current approach more capable of sustaining network security and efficiency under tough conditions.

Table 1. *Simulation setup for the experiment*

Simulation Parameter	Value/Description
Simulator	OMNET++
Programming Language	C++
Number of Simulation Scenarios	8
WSN Application Scenario	Intelligent Healthcare
Simulation Goals	Secure Data Aggregation, Authentication, and Authorization with block-chain
Protocols Compared	SD, EEHA, HAS, IIF, RHC
Key Metrics Evaluated	Security, QoS, Energy Efficiency, Throughput, Performance, Large-Scale Deployment
Node Type	Next-Generation IoT Sensor Nodes
Routing Protocol	BSDAR (Block-chain-Enabled Secure Data Aggregation Routing)
Routing Path Construction	A-star Heuristics Algorithm
Blockchain Integration	Ensures data protection and tamper-proof communication
Performance Metrics	Energy Consumption, Network Lifetime, End-to-End Delay, Packet Drop Ratio
Security Features	Strong node-level protection, decentralized communication
Number of Nodes	Variable (for large-scale deployment testing)
Energy Efficiency Focus	Avoiding energy holes around BS

Table 2. *Tabulation of assessment ranges*

Metrics	Proposed BSDAR Approach	SD	EEHA	HAS	IIF	RHC
Average Throughput (kb/s)	444	415	417	420	430	443
Energy Consumption (Joules)	2.91 (over 36 rounds)	3.5	3.6	3.7	3.8	3.94
Affected Network (%)	2.62	3.68	3.75	3.80	4.0	4.38
Resilience Time (%)	0.9	0.9	0.9	0.9	0.9	0.9

This table 2 clearly delineates the performance of the proposed BSDAR approach against various competing approaches in terms of throughput, energy consumption, network impact, and resilience time.

3.5 Time complexity assessment

The time complexity for BSDAR approach is O (n log n). Indicates that running time of an algorithm increases the logarithmic with respect to n, which defines the number of nodes in the link. In simple terms, it means that when the No.of nodes grows, the time taken by the approach to perform the respective operations increases very gradually. This efficiency in logarithmic growth, compared to linear or quadratic time complexities, makes BSDAR especially suitable for large-scale networks, where the speed of processing with least computational overhead is vital. The O (n log n). Complexity reflects an effective way to handle and aggregate data with reduced computational demand; hence, the better scalability and performance.

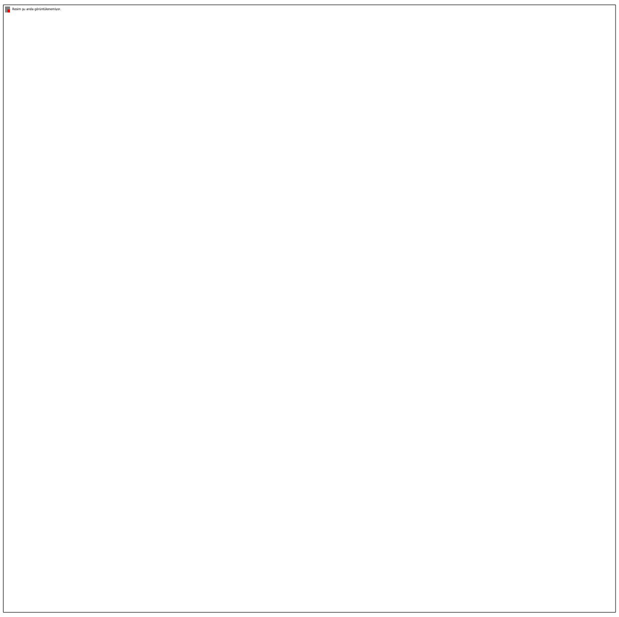


Figure 5. *Resilience vs network lifespan computation*

4. Conclusions

This research work proposes the BSDAR protocol, which highly improves the performance and security in next-generation sensor networks integrated with IoT. Detailed simulation using the OMNeT++ platform showed that BSDAR outperformed others in several key performance metrics such as throughput, energy consumption, network lifetime, and resistance against malicious attacks. Innovation in the use of blockchain technology in the BSDAR protocol provides a tamper-proof approach for data communication in a decentralized manner, as it does effectively mitigate security threats and enhance protection at the node level. In BSDAR, the organization of nodes in dynamic clusters and the use of the A* heuristics algorithm for routing have minimized energy holes and optimized routes, hence prolonging network lifetime and reducing energy consumption. This protocol has proven to be efficient and robust with the result of an average throughput of 444 kb/s and energy consumption of 2.91 joules over 36 rounds, in comparison with other methods. Besides this, adding more strength to the BSDAR against adversarial attack, which comprises merely 2.62% of the network by malfunctioning nodes, a rate that is higher compared with the rest of the protocols. Performance metrics are consistent, as evident from the resiliency of BSDAR in preserving the integrity and functionality of the network even in the presence of an adversary. In general, BSDAR can be considered a promising solution for scalable, secure IoT deployments based on advanced blockchain integrations with efficient data aggregation and routing techniques. Its well-balanced approach to security, performance, and energy efficiency underlines its potential to improve sensor networks' robustness and reliability at large scale in many applications. Blockchain has been studied and reported in the literature [21].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Chithaluru, P., Al-Turjman, F., Dugyala, R., Stephan, T., Kumar, M., & Dhatterwal, J. S. (2024). An

enhanced consortium blockchain diversity mining technique for IoT metadata aggregation. *Future Generation Computer Systems*. 152: 239-253. DOI:10.1016/j.future.2023.10.020

[2] Bojič Burgos, J., & Pustišek, M. (2024). Decentralized IoT Data Authentication with Signature Aggregation. *Sensors*. 24(3): 1037. DOI:10.3390/s24031037

[3] Bobde, Y., Narayanan, G., Jati, M., Raj, R. S. P., Cvitić, I., & Peraković, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics*. 13(4): 687. DOI:10.3390/electronics13040687

[4] Kulurkar, P., kumar Dixit, C., Bharathi, V. C., Monikavishnuvarthini, A., Dhakne, A., & Preethi, P. (2023). AI based elderly fall prediction system using wearable sensors: A smart home-care technology with IOT. *Measurement: Sensors*. 25: 100614. DOI:10.1016/j.measen.2022.100614

[5] Preethi, P., & Asokan, R. (2020, December). Neural network oriented roni prediction for embedding process with hex code encryption in dicom images. *In Proceedings of the 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India*. 18-19. DOI:10.1109/ICACCCN51052.2020.9362880

[6] Asokan, R., & Preethi, P. (2021). Deep learning with conceptual view in meta data for content categorization. *In Deep Learning Applications and Intelligent Decision Making in Engineering*. 176-191. IGI global. DOI:10.4018/978-1-7998-2108-3.ch007

[7] Palanisamy, P., Padmanabhan, A., Ramasamy, A., & Subramaniam, S. (2023). Remote patient activity monitoring system by integrating IoT sensors and artificial intelligence techniques. *Sensors*. 23(13): 5869. DOI: 10.3390/s23135869

[8] Bai, D. P., & Preethi, P. (2016). Security enhancement of health information exchange based on cloud computing system. *International Journal of Scientific Engineering and Research*. 4(10): 79-82.

[9] Preethi, P., Asokan, R., Thillaiarasu, N., & Saravanan, T. (2021). An effective digit recognition model using enhanced convolutional neural network based chaotic grey wolf optimization. *Journal of Intelligent & Fuzzy Systems*. 41(2): 3727-3737. DOI:10.3233/JIFS-211242

[10] Akila, V.; Sheela, T. (2017, May 13). Preserving data and key privacy in Data Aggregation forWireless Sensor Networks. *In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICT), Chennai, India*. 282–287. DOI:10.1109/ICCCT2.2017.7972286

[11] Akila, V.; Sheela, T. (2019, February 21-22). Secure Data Aggregation to Preserve Data and Key Privacy in Wireless Sensor Networks with Multiple Sinks. *In Proceedings of the 2019 3rd International Conference on Computing and Communications Technologies (ICT), Chennai, India*. 86–93. DOI:10.1109/iccct2.2019.8824992

[12] C, V.; Premi, G.; Solainayagi, P.; Srinivasan, C.; Kuppusamy, P. (2023, August 18-19). Data Privacy and Confidentiality in Healthcare Applications of IoT-Enabled Wireless Sensor Networks. *In Proceedings of the 2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon), Singapore, Singapore*. 610–614. DOI:10.1109/SmartTechCon57526.2023.10391743

[13] Elmahdi, E.; Yoo, S.-M.; Sharshembiev, K.; Kim, Y.-K.; Jeong, G.-H. (2019, July 14-17). Protecting Data Integrity for Multi-Application Environment inWireless Sensor Networks. *In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA*. 90–95. DOI:10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00037

[14] Ruan, M.; Gao, H.;Wang, Y. (2019). Secure and Privacy-Preserving Consensus. *IEEE Trans. Autom. Control*. 64(10): 4035–4049. DOI: 10.1109/TAC.2019.2890887

[15] Zhou, Q.; Qin, X.; Liu, G.; Cheng, H.; Zhao, H. (2019, August 9-11). An Efficient Privacy and Integrity Preserving Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks. *In Proceedings of the 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China*. 291–297. DOI: 10.1109/SmartIoT.2019.00051

[16] Phakade, S.V.; Singla, C.R.; Rajankar, O. (2022, August 26-28). Design of Privacy and Energy-Efficient DATA Aggregators for Wireless Sensor Networks. *In Proceedings of the 2022 2nd Asian Conference on Innovation in Technology (ASIANCON), Ravet, India*. 1–5. DOI:10.1109/ASIANCON55314.2022.9909044

[17] Hu, S.; Liu, L.; Fang, L.; Zhou, F.; Ye, R. (2020). A Novel Energy-Efficient and Privacy-Preserving Data Aggregation for WSNs. *IEEE Access*. 8: 802–813. DOI: 10.1109/ACCESS.2019.2961512

[18] Shi, E.; Chan, H.T.H.; Rieffel, E.; Chow, R.; Song, D. (2011). Privacy-preserving aggregation of time-series data. *In Annual Network & Distributed System Security Symposium (NDSS); Internet Society: Reston, VA, USA.*

[19] Boubiche, D.E.; Boubiche, S.; Toral-Cruz, H.; Pathan, A.-S.K.; Bilami, A.; Athmani, S. (2015). SDAW: Secure data aggregation watermarking-based scheme in homogeneous WSNs. *Telecommun. Syst*. 59(2). DOI:10.1007/s11235-015-0047-0

[20] Shim, K.-A.; Park, C.-M. (2014). A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst*. 26(8): 1-1. DOI:10.1109/TPDS.2014.2346764

[21]TAKAOĞLU, M., ÖZYAVAŞ, A., AJLOUNİ, N., DURSUN, T., TAKAOĞLU, F., & DEMİR, S. (2023). OTA 2.0: An Advanced and Secure Blockchain Steganography Algorithm . *International Journal of Computational and Experimental Science and Engineering*, 9(4), 419–434. Retrieved from https://ijcesen.com/index.php/ijcesen/article/view/289