Blockchain-implied Architecture for Secure and Energy Efficient Processing of IoT Data in Pervasive WSNs

Sushovan Das[1] and Uttam Kr. Mondal[2]

[1]*College of Engineering and Management, Kolaghat, Purba Medinipur, India,*
[2]*Vidyasagar University, Midnapur, India*

https://doi.org/10.26636/jtit.2025.4.2194

Abstract — Pervasive wireless sensor networks (PWSNs) are essential for real-time data transmission in Internet of Things (IoT) environments. However, conventional centralized models, while energy efficient, often face challenges related to data integrity and security. This paper proposes a decentralized blockchain-based architecture aimed at enhancing secure IoT data processing at the base station while preserving energy efficiency. The system utilizes a blockchain network among sink nodes and its operation is divided into four stages: deployment of a virtual machine on leaf nodes for real-time data collection, generation of hash keys to ensure secure transmission to sink nodes, implementation of a universal virtual machine (UVM) at the sink layer for block formation, and development of an integrated authentication and consensus module within the UVM. The proposed framework ensures efficient, verifiable and efficient data handling. Performance is evaluated using sensor node energy efficiency (SNEN), blockchain energy consumption level (BCLE), blockchain transmission efficiency (BCTE), and packet delivery in sink nodes (PDSN). Experimental results demonstrate improved energy efficiency in the sensor zone, reduced blockchain latency, and improved throughput, establishing a robust and secure model for data handling in PWSNs.

Keywords — blockchain, data integration, energy efficiency, Internet of Things, pervasive WSN

1. Introduction

The huge growth in the number of Internet of Things (IoT) devices has caused an unprecedented increase in the generation of data collected from such environments as smart cities, healthcare, agriculture and industrial automation. However, the management and integration of these heterogeneous data sets is a difficult task due to issues concerning data integrity, security, and interoperability. To address these issues, the use of blockchain technology [1], [2] combined with a cryptographic hash key [3], [4] is a promising solution.

Blockchain technology provides secure data transmission through a complex encryption system [5], similar to a meticulous accounting ledger of a company. It carefully monitors and records all transactions on a peer-to-peer network. Each block in the chain contains data about its creation time and is connected to the previous block through a unique hash code and transaction details. Once recorded on the network, the data is immutable. Blockchain is designed to prevent fraud and data tampering attempts. It requires complex computational processes, such as data encryption [6], [7] and decryption in a distributed environment, leading to higher energy consumption compared to the conventional approach of a centralized network structure often used in WSNs. However, the centralized network structure may compromise the security of data integration.

This paper proposes a hybrid model for pervasive wireless sensor networks (PWSN) that utilizes a decentralized network structure [8]–[10]. The PWSN is divided into multiple sensor zones, each with a sink node. These sink nodes are connected through a cloud environment, forming a distributed network. Within each sensor zone, a centralized network is replicated, with sensor nodes acting as leaf nodes. These leaf nodes are responsible for data preparation tasks such as hash generation, compression, and transmission to the respective sink node, thus reducing energy consumption compared to a fully distributed blockchain implementation. To address energy and computational complexity issues, the sink nodes, which are high-end computers powered by the mains, participate in the creation and integration of blockchain data for the entire PWSN. The model addresses the challenges of trustworthiness, privacy, and interoperability of IoT data using blockchain technology and hash functions.

The key contributions of this research are as follows:

- Design of a decentralized architecture for PWSN.
- Developing algorithms for energy-efficient data collection and preparation using semantic technology at the leaf nodes.
- Incorporating cryptographic hash functions before data transmission to sink nodes.
- Designing a universal virtual machine (UVM) for sink nodes to manage data storage and blockchain integration.
- Integrating authentication and consensus modules within the UVM for secure block validation.

2. Literature Survey

The authors of [11] conducted an in-depth survey of blockchain technology, including its history, consensus algo-

rithms, cryptography, and various blockchain applications. The work also emphasized blockchain security, covering risk analysis, security risk categories, real attacks, bug analysis, and recent security measures. Article [12] investigated the integration of blockchain technology into wireless sensor networks (WSN), highlighting its advantages and potential challenges.

The authors of [13] showed the use of the blockchain technology to improve the security of WSNs. This research smoothly incorporated blockchain into data transfer processes, forming a highly secure structure for WSNs. By implementing a blockchain-based transaction ledger, sensor data is converted into unalterable records. The new system they proposed is excellent in the aggregation and analysis of sensor data, significantly increasing the reliability of the entire wireless sensing network architecture.

As a result, the study concluded that blockchain technology can be an effective solution to the security problem of distributed storage data. In [14], a thorough examination of the role of blockchain in the metaverse is conducted. The authors presented the basic principles of blockchain and the metaverse to demonstrate how blockchain solutions can address issues such as storage, integrity, security, and interoperability.

In [15], the authors suggest a way to strengthen data security in WSNs by incorporating blockchain into data transmission, leading to a highly secure wireless sensor network. Paper [16] presented a novel blockchain-based architecture to address the storage issues of massive IoT data. This decentralized system uses blockchain immutability, security, transparency, and automation, providing reliable data management.

The research demonstrated remarkable results, making it a scalable solution for IoT data storage. It is protocol-agnostic, allowing easy integration into various IoT applications, and revolutionizing data management in the IoT domain.

The survey conducted in [17] starts by introducing traditional WSN solutions and then delves into how blockchain technology can be used to improve data management. It also looks at the important role of blockchain in strengthening security. It begins by examining centralized WSN models and the security issues they face. After that, a thorough investigation of blockchain-based WSN solutions is presented, designed to address various security aspects, such as access control, preservation of information integrity, assurance of privacy, and extension of the longevity of WSN nodes.

Researchers in [18] investigated the impact of security protocols on wireless sensor networks and their ability to collect and analyze data. This study offers a concise overview of data aggregation and data compression using blockchain technology in WSNs for secure data transmission. The authors of [19] combined blockchain and IoT to create a distributed storage architecture that would protect the integrity and security of WSN data storage in edge computing. Paper [20] provides an overview of the protocols used to integrate blockchain technology with IoT. The researchers studied the consensus protocols used to create blockchains for IoT applications.

The study in [21] introduces a blockchain-based incentive system for WSNs. This system uses two blockchains: one to store node data and the other to manage data access. To reduce the storage requirements of network nodes, the preserving hash functions are used to compare stored data with new data blocks, and the latter are stored in nodes closest to existing data. The authors of [22] suggested a cryptographic iterative hash function system to improve the security of WSNs when transmitting sensor data on the blockchain. To improve sensor security, the Merkle tree algorithm was used in the investigation.

In [23], the authors proposed a hybrid blockchain-based model that incorporates a mutual authentication scheme to identify the cluster head node in a pervasive wireless sensor environment. In [24], a new and effective authentication system is proposed that uses blockchain technology to improve security in WSNs, essential components of the IoT network. The proposed approach established a hierarchical blockchain network with local and global chains, allowing secure connections among nodes in various communication scenarios, such as user authentication, identity verification, and cluster node validation.

The authors of [25] proposed a decentralized blockchain-based system that integrates authentication and privacy protocols for secure communication in WSNs enabled by the Internet of Things. This system includes a registration, certification, and revocation process for secure communication between sensor nodes and the central base station (BS) in a cloud environment. The performance of the solution was evaluated on metrics such as detection accuracy, certification delay, and computational and communication overhead.

In [26], a blockchain-based system is proposed for registration, authentication, data sharing, and non-repudiation in the Internet of Wireless Sensor Things (IoWST). The nodes were divided into three categories: sensor nodes, cluster heads, and coordinators. A consortium blockchain was established on the coordinators to store legitimate node identities and to enable the execution of smart contracts for authentication, data sharing, and non-repudiation among the sensor nodes. Ambient node data were stored using an AI-based interplanetary file system (IPFS).

Paper [27] offers a complete understanding of cybersecurity in WSNs, with a focus on modern machine learning (ML) and blockchain (BC) security approaches. It examines 171 recent studies on WSN security and investigates the incorporation of BC and ML into a lightweight security framework, with an emphasis on cyberattack detection and prevention within WSNs, as well as potential efficient BC and ML algorithms.

In [28], the authors proposed a new approach that combines linear network coding (LNC) with WSNs and blockchain-enabled IoT devices. This method was designed to reduce the energy consumption at each network node by applying LNC techniques. The authors conducted a thorough evaluation of the effectiveness and reliability of the model compared to other existing approaches. This study showed remarkable progress in several essential performance indicators, such as a larger number of active nodes, improved packet delivery

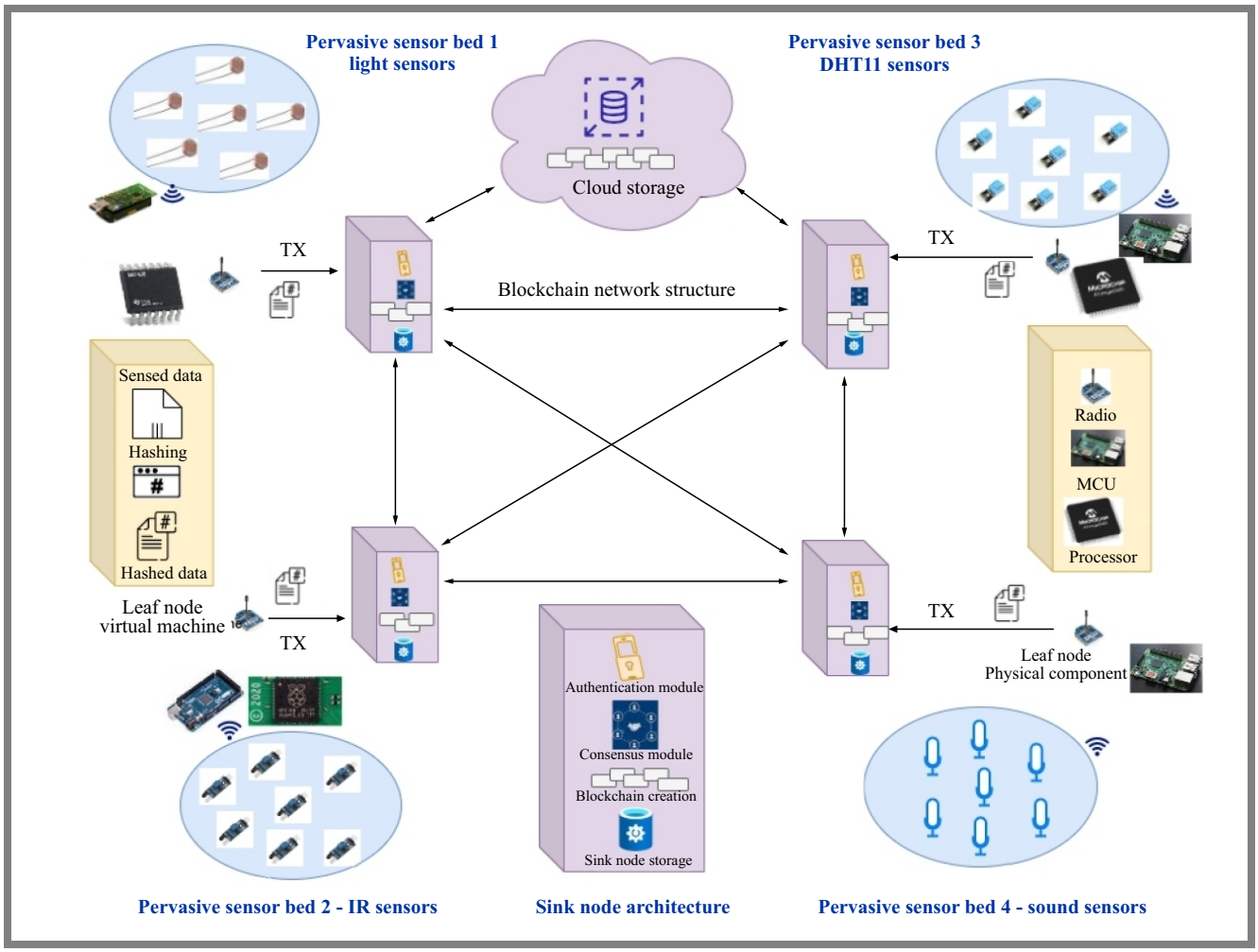

Fig. 1. System architecture (data integration using blockchain).

rate, increased throughput, and optimized remaining energy compared to current methods.

The authors of [29] proposed a new energy-efficient data collection mechanism (EEDAM) that uses the blockchain technology. This mechanism is designed to save energy resources by aggregating data at the cluster level. Edge computing is used to provide low-latency, trust-enhanced services to the IoT ecosystem. Blockchain integration is implemented in the cloud server to guarantee that the edge computing infrastructure is authenticated by the blockchain, thus providing a secure and reliable set of services to IoT devices.

The work described in [30] highlights the promising integration of IoT and BC in structural health monitoring, particularly for underground structures. The proposed blockchain-IoT network, with its locally centralized and globally decentralized features, offers a path toward more efficient, scalable, and secure SHM practices.

In summary, all papers mentioned above discussed the combination of BC with WSNs and IoT systems in the context of data management and energy efficiency. The results of these studies have been encouraging, suggesting that blockchain may be a beneficial solution to overcome difficulties and enhance the abilities of WSNs and IoT devices. Blockchain continues to open up the possibility of a more secure and reliable wireless sensing and IoT environment through data aggregation, security improvements, or efficient data management.

3. System Architecture

Figure 1 provides an overview of the architecture of the proposed model system. The network topology used in this model differs from that of conventional WSNs. On closer inspection, it is clear that the proposed topology follows a decentralized structure that includes sink nodes only. However, within the sensor zone, which extends up to the sink node, the conventional network topology used by PWSN is still in effect.

Figure 1 shows a system with four sensor zones, each connected to its own sink node. Every zone is equipped with multiple sensors, each with its own microcontroller and XBee radio technology, which form leaf nodes. These leaf nodes are connected directly to the sink nodes which are part of a decentralized network that is connected to a cloud environment with centralized cloud storage. Additionally, each sink node has local storage capabilities to efficiently manage data.

4. Methodology

The proposed method is structured into three distinct subsystems, each dedicated to a specific role: the data acquisition process at the leaf nodes and the subsequent creation of data blocks for the blockchain. The second subsystem deals with the reception of data blocks, verification of their authenticity, and their incorporation into the blockchain, while the third subsystem is responsible for disseminating the blockchain to cloud storage and local storage of sink nodes, ensuring its availability and redundancy.

4.1. Data Sensing and Data Block Creation

Different sensors are used in the WSN to capture signals emitted by the source devices. Each sensor has its own event and time ontology, allowing it to accurately determine its active state. This event and time ontology is incorporated into the virtual machine configuration of the sink node to reduce the amount of detected data, resulting in lower processing requirements, lower transmission overhead and thus reduced energy consumption. In this paper, the only CPU usage needed is for the generation of data blocks, which does not significantly affect energy consumption. Additionally, the sensed data blocks can be converted into the JSON format, reducing their size, and thus decreasing the energy needed for transmission. Algorithm 1 illustrates how data sensing, data block formation, and JSON data packet formatting are done in sequence.

The steps are described below:

- At each leaf node, the event and time ontology are preloaded, and the sensor is read in a specific time frame that is in line with the ontology.
- Leaf nodes sustain their sleep cycle effectively to minimize energy consumption.
- The leaf nodes collected the detected information and populated the values of the object generated from the SensorData class.
- The SensorData object is linked to the object created from the DataBlock object.
- Calculate the hash represented by Eq. (1) for SensorData using the SHA256 hash function.
- The data block is given the calculated hash as its current hash, whereas the previous hash is left blank for the sink node.
- The data block is then changed to the JSON format to decrease the packet size.
- The block is transmitted to the sink node for further processing.

4.2. Blockchain Formation and Data Integration

This work will exclude the consideration of energy requirements for sink nodes in WSNs, as they operate without relying on battery power. The sink nodes are established using a medium-range server configuration, incorporating a Python-designed virtual machine, and utilizing JSON files for storage.

Algorithm 1 Data block creation using hashing at leaf node

Require: Sensor devices, microcontroller
Ensure: DataBlock with generated hash sent to sink node
LeafVM $lvm \leftarrow$ LEAFVM(Microcontroller.devices)
SNode $ps \leftarrow$ PervasiveSensorNode(Sensor.devices)
empty SensorData object $sd \leftarrow$ Null
DataBlock $db \leftarrow$ DataBlock(lvm)
while lvm.devicePower() **and** lvm.isActive() **do**
  lvm.adaptiveDutyCycling()
  lvm.dataSampling()
  lvm.sleepScheduling()
  $sd \leftarrow$ SensorData($lvm.read(ps)$)
  db.sensorData $\leftarrow sd$
  db.previousHash $\leftarrow$ Null ▷ Assigned at sink node
  db.currentHash $\leftarrow db$.generateCurrentHash()
  ps.transmitToSinkNode(db)
end while
End

All the sink nodes, together with a central cloud storage system, will be configured using a decentralized network topology. The cloud storage system will also function as a node within this decentralized network. Blockchains will be stored in both the cloud storage system and the local storage of the sink nodes.

This proposed technique operates in a manner such that each sensor node in the network is not replicated to other sink nodes in the network. However, the information from the last hash will be shared among all the sink nodes, allowing the chain to be created by the information from the current hash, the previous hash, and the last hash of the DataBlock in a synchronized schedule, which reduces storage requirements by dividing it among the number of sink nodes. The diagram presented in Fig. 2 shows the functional block of this approach. Algorithm 2 describes the steps taken by the sink nodes to authenticate the data blocks, add them to the blockchain, notify other sink nodes, and store the block securely in the local sink nodes and last hash globally to all sink nodes and in the cloud.

The steps are described below:

- Receive data blocks from the leaf node in a JSON packet.
- Compute the hash represented by Eq. (1) for the data block, which is described in the DataBlock class and contains the sensor data specified in the SensorData class.
- Compare the hash from DataBlock to the hash that has been calculated.
- If the hash that is calculated and the hash that is compared are the same, it can be confirmed that the data block is genuine and has not been modified.
- Obtain the last hash from the blockchain from either a local storage or the network. Since the last hash is global to all sink nodes, the value will be the same throughout the network.
- Assign the last hash of the blockchain to the previous hash of the data block to be integrated.

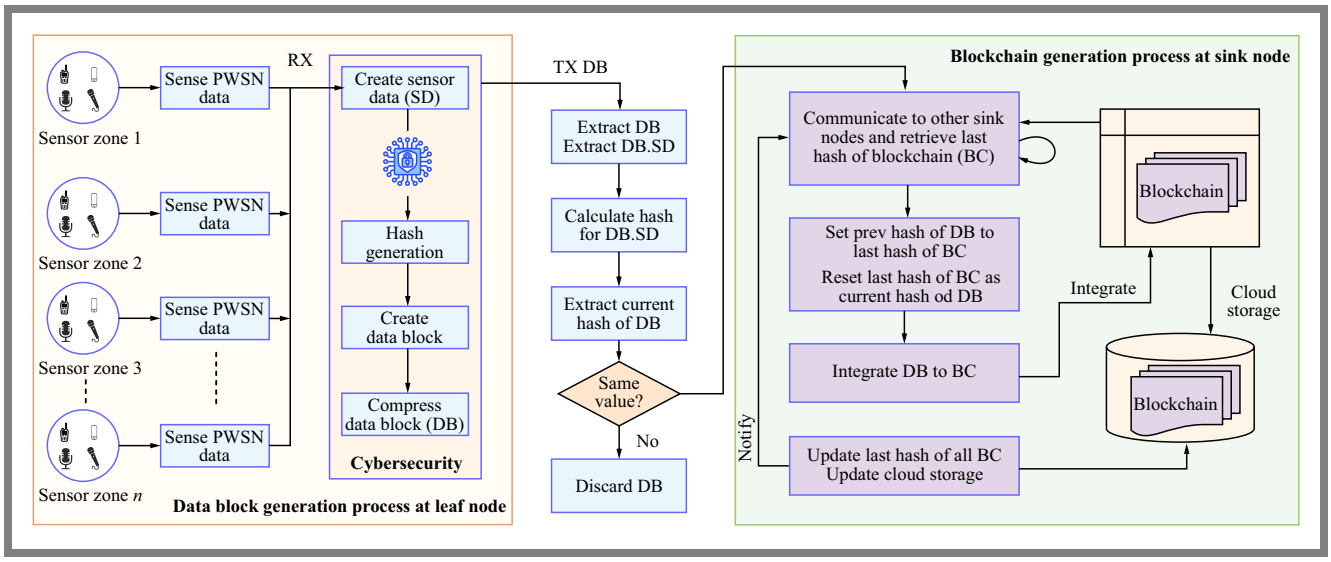

Fig. 2. Functional block diagram representing the blockchain at the sink node.

- Reset the last hash of the blockchain as the current hash of the data block.
- Notify and update the last hash of the blockchain of the entire network's sink node.
- Integrate the DataBlock to the "BlockChain"
- Store the DataBlock in the internal storage of the sink node.
- Store a copy of DataBlock to the cloud storage.
- The seven steps mentioned above must be coordinated with other sink nodes to guarantee that the integration of DataBlock to BlockChain and updating of the last hash of blockchain of the entire network are synchronized.

4.3. Transmission of Blockchain

The proposed model utilizes a standard cloud storage platform, such as Amazon S3 or Google Cloud, to maintain a backup of the blockchain core. Thus, even if a sink node fails, the sensor data remains accessible to users. The process $transmitCloudStorage()$, as described in Algorithm 2, demonstrates the transmission of the blockchain data to cloud storage. Furthermore, this approach includes web-based and mobile user interfaces to ensure user access to the sensor data.

4.4. Mathematical Model of the Proposed Architecture

The model captures energy consumption, blockchain latency, throughput, and data sensitivity using a set of well-defined performance metrics and equations.

Each sensor node collects environmental data, which is encapsulated in a data block. To ensure integrity and non-repudiation, a cryptographic hash is generated using the SHA256 algorithm:

$$\mathcal{H}(SD) = \text{SHA256}\big[\text{encode}(SD)\big] \,, \tag{1}$$

Algorithm 2 Blockchain creation and synchronization at sink node.

Require: Received DataBlock from leaf node
Ensure: Verified blockchain updated across all sink nodes

```
SinkVM svm ← SinkVM(SinkNode.devices)
local blockchain bc ← svm.getLocalBlockchain()
db ← svm.receiveBlock()
while svm.isActive() do
    if db = Null then
        db ← svm.receiveBlock()
    end if
    if bc = Null then
        db.previousHash ← Null
        bc.lastHash ← db.currentHash
        bc.bindFirstBlock(db)
    else
        bc.lastHash ← svm.getLastHashFromNetwork()
        if svm.authenticateBlock(db) then
            db.previousHash ← bc.lastHash
            bc.lastHash ← db.currentHash
            bc.appendBlock(db)
        end if
    end if
    svm.storeLocal(bc)
    svm.syncWithCloud(bc.lastHash)
    svm.notifyAllSinkNodes(bc.lastHash)
end while
```

where SD is the sensor data object:

$$SD = f(index, timestamp, sensedData, sensorId, location) \,. \tag{2}$$

The total energy consumed by a sensor node during sensing, processing, and transmission is given by:

$$E_{\text{node}} = \gamma \cdot \left[t_{\text{pac}} \cdot P_{\text{pac}} + t_{\text{sd}} \cdot P_{\text{sd}} + t_{\text{tx}} \cdot P_{\text{tx}} \right] , \tag{3}$$

where:

- $t_{\text{pac}}, t_{\text{sd}}, t_{\text{tx}}$ – time required for processor activation, data sensing, and data transmission,
- $P_{\text{pac}}, P_{\text{sd}}, P_{\text{tx}}$ – power consumption in watts for each respective operation,
- γ – adjustment factor based on the number of cycles or events.

Probability of data sensing:

$$P_{ds} = \frac{N_{sensed}}{N_{total}} \,. \tag{4}$$

Effective energy consumption:

$$E_{\text{eff}} = P_{ds} \cdot E_{\text{node}} \,. \tag{5}$$

Sensor node energy efficiency (SNEN):

$$\text{SNEN} = \left(1 - \frac{E_{\text{eff}}}{E_{\text{node}}}\right) \cdot 100\% \,. \tag{6}$$

Blockchain latency efficiency across sink nodes is modeled as follows:

$$\text{BCLE} = \frac{1}{n} \sum_{i=1}^{n} \frac{BT_i + TPT_i + NPT_i + TQT_i}{TTPT_i} \,, \tag{7}$$

where:

- BT – block time,
- TPT – transaction processing time,
- NPT – network propagation time,
- TQT – transaction queue time,
- $TTPT$ – total time to process a transaction.

Blockchain throughput efficiency (BCTE) evaluates the data handling capacity:

$$\text{BCTE} = \frac{1}{n} \sum_{i=1}^{n} \left(\frac{TPS_i}{TPT_i} \cdot (1 - BPR_i) \cdot (1 - LPR_i) \right) , \tag{8}$$

where:

- TPS – transactions per second,
- BPR – block processing rate,
- LPR – latency processing rate.

Pervasive data sensitivity (PDSN) measures the effectiveness of data compression and sensitivity across the sensor zones:

$$\text{PDSN} = \sum_{sZ}^{eZ} \sum_{t=t_{\text{in}}}^{t_d} \left(1 - \frac{sdSize\big(sEvent(t)\big)}{dbSize(t)} \right) \cdot 100\% \,. \tag{9}$$

Data block size:

$$dbSize(t) = P(sData) \cdot CR \cdot sdSize\big(sEvent(t)\big) \,, \tag{10}$$

where:

- $sdSize()$ – sensed data size,
- CR – compression ratio due to JSON encoding,
- $P(sData)$ – probability of sensing a relevant event.

5. Experimental Results and Performance Evaluation

The experiment integrates the sensed data using the proposed model, as well as the conventional PWSN model and actual blockchain models. The proposed hybrid offers good energy efficiency and its performance is measured by means of the sensor node energy efficiency (SNEN) metric with calculated energy efficiency. Equation (3) is used for computing the energy of the proposed model, whereas the probability of data sensing is expressed as Eq. (4).

Estimates of the consumed energy and energy efficiency are calculated using Eqs. (5) and (6), respectively. The efficiency of blockchain latency (BCLE) in PWSN can be affected by various elements that are exclusive to PWSN settings. This research uses Eq. (7) which takes into account the factors specified in Tab. 1. The present experiment evaluates the efficiency of blockchain throughput (BCTE) considering the factors listed in Tab. 1 and a corresponding equation has been formulated for the proposed model in Eq. (8). This research established that the effectiveness of data sensitivity (PDSN) for PWSN can be determined using Eq. (9), by means of which the decrease in data size (the size of events that occur in all sensor zones over a certain period of time) is calculated at some intervals, as is the size of the blockchain created by the proposed approach.

5.1. Experimental Setup

This research introduces three distinct sensor zones, each with its own set of sensor nodes. The first zone consists of six TelosB Mote (TPR2420) units, each with an MSP430 microcontroller as well as TPR2420 sensors for light, humidity, and temperature monitoring. The second zone has six Arduino Mega platforms, DHT11 sensors, and XBee radio modules for data transmission. The third zone consists of three Raspberry Pi boards, IR sensors, and XBee radio modules.

To facilitate data processing and transmission, each microcontroller at these sensor nodes will be integrated with a common virtual machine written in Python. This virtual machine will generate data blocks using hash functions and transmit them efficiently. Additionally, three high-end computers, each with a virtual machine of sink nodes written in Python, will serve as sink nodes for the three sensor zones to create a blockchain. The computers will store the blockchain locally in a JSON file, and the sink nodes will be interconnected via the Internet and linked to a cloud storage system hosted by Google Cloud for data storage and analysis.

Each experiment was carried out over a period of approximately 60 min of continuous operation. For every sensor zone, measurements were repeated ten times and the reported results represent mean values. Network traffic was evenly distributed among the sink nodes, with each handling 100 – 120 transactions per session. Latency and throughput were monitored in real time using the Python-based virtual machine module to ensure statistical consistency.

Tab. 1. Parameters considered to calculate performance metrics for the proposed model.

Symbol	Full form	Description
Parameters used in Eqs. (3), (4), and (6) to calculate SNEN		
E()	Energy function	Energy calculation in Joules
P()	Probability function	Probability of sensing event
t()	Time function	Time to process/transmit/receive
power()	Power function	Electrical power estimation in watts
Parameters used in Eq. (7) to calculate BCLE – blockchain latency efficiency		
BT	Block time	Average time to add new block to the blockchain
TPT	Transaction processing time	Time to process and validate transaction
NPT	Network propagation time	Time to take information about new block
TQT	Transaction queue time	Time to wait to be included in the block
TTP	Total time to process	Total time for confirmation on the blockchain
Parameters used in Eq. (8) to calculate BCTE – blockchain throughput efficiency		
TPS	Transaction per second	Number of transactions per second by sink node
TPT	Transaction processing time	Time to process and validate transaction
BPR	Block processing rate	Rate of addition of new blocks the blockchain
LPR	Latency processing rate	Rate of impact of latency within PWSN
Parameters used in Eq. (9) to calculate PDSN – pervasive data sensitivity		
sZ	Starting sensor zone	Index number for starting sensor zone
eZ	Ending sensor zone	Index number for ending sensor zone
t_d	Time duration	Total duration of entire PWSN
t_{in}	Sensing interval	Event sensing interval due to event semantic
sdSize()	Sensed event's data size	Function to measure data size
sEvent()	Sensed event	Event occurs at time t
dbSize()	Data block size	Function to measure data block for the event detected at time t
P(sData)	Probability of sensing data	Function to measure probability of event sensing
CR	Compression ratio	Compression ratio due to JSON data representation
RR	Reduction ratio	RR = P(sData) · CR

5.2. Experimental Results

The results of the experiment are evaluated using the setup described in Subsection 5.1 and Eqs. (3) to (8), respectively. Energy evaluations are conducted using the TelosB Mote, ATMEGA2560 MCU, XBee Pro, and Raspberry Pi platform data sheets to determine energy consumption. Table 2 presents the energy consumption at the leaf nodes in the sensor zone for single event sensing and data block formation with and without the hash. The average time required for detection, processing and transmission was calculated, and then the energy was determined in Joules. Figure 3 shows the data block created at the leaf node, along with the hash and the total time taken to generate the data block.

```
Data block details
Data block index: 1695780562
Data block size: 421 bytes
Sensor data size: 247 bytes
Hash size: 115 bytes
Data block index: 1695780562
Sensor ID: 10
Sensor zone ID: 1
Sensor lattitude: 22 25 58.5192
Sensor longitude: 87 51 35.5896
Sensor type: Temperature
Sensor value: 25.5
Hash:f87f9bb31f284b4169382679f7dd413f827a52a3f3cb67842b119b8
e8f2fe376
Processor active time: 0.18215274810791016 seconds
```

Fig. 3. Details of the data block generated at the leaf node.

Figure 4 shows the part of the blockchain generated by the entire network. It illustrates the structure of the DataBlock together with the corresponding SensorData. It reveals the present hash, the prior hash, and the last hash of the entire network. The last hash will be the same as the current hash if the synchronization functions correctly. The figure demonstrates

Tab. 2. Energy consumption (SD, TX, PAC) for a single DataBlock at the leaf node.

Energy consumption at leaf node (hash mode)				
Mode	Power [W]	Size [bytes]	Time [s]	Energy [J]
Data sensing (SD)	0.1925	247	0.0079	0.00152152
Data transmit (TX)	0.875	421	0.0134	0.011788
Processor active (PAC)	6.5	NA	0.201	1.3065
Total energy at leaf node				1.3198
Energy consumption at leaf node (no hash)				
Mode	Power [W]	Size [bytes]	Time [s]	Energy [J]
Data sensing (SD)	0.1925	211	0.0067	0.00129976
Data transmit (TX)	0.875	247	0.0079	0.006916
Average PAC	6.5	NA	0.171	1.1115
Total energy at leaf node				1.1197

that they are the same in all cases. If the last hash and the current hash do not match, this implies that the mismatched data block has not been included in the blockchain due to potential data manipulation.

Table 3 and Fig. 5 demonstrate the average energy consumption at the leaf nodes with different time intervals in various sensor zones. The energy is calculated by using a hash, without a hash, and with the use of the proposed hybrid model. aSNEN – see Eq. (6) – is also calculated for the proposed model using Tab. 3. The figure clearly indicates that a sing hash in PWSN is more energy-intensive than traditional PWSN, while the hybrid model proposed in this work significantly reduces the energy consumed in the sensor zones. The table shows that the energy efficiency for the sensor nodes (SNEN) is ≈40%.

Table 4 provides the blockchain latency (BCLE) for all sink nodes involved in the PWSN using Eq. (7), together with the average block creation time (BT), transaction processing time (TPT), network processing time (NPT), transaction queue time for the specified time intervals and total number of events. The total time taken to process a blockchain is also calculated. The proposed hybrid technique yields an average BCLE of

Tab. 3. Energy consumption using hash and percentage of SNEN.

Time	Inter-val	Total event	P(sEvent)	Energy using hash	Energy hy-brid	SNEN
200	4	50	0.61	65.99	40.25	39%
400	5	80	0.59	105.58	62.29	41%
600	4	150	0.67	197.97	132.64	33%
800	5	160	0.52	211.17	109.81	48%
1000	4	250	0.52	329.95	171.57	48%

Fig. 4. Blockchain generated by the proposed model for PWSN.

80%, which is significantly better than in a scenario in which blockchain is used with the traditional PWSN model.

Equation (8) is used to calculate the average blockchain throughput (BCTE) for all sink nodes in the network, i.e. the transactions per second (TPS) of all sink nodes. Then, the total processing time (TPT) and blockchain processing time (BPT) are calculated and the average latency rate (LPR) calculated in Tab. 5 is used. The average BCTE is ≈37% for the proposed hybrid model, which is also significantly better than when using blockchain with the traditional PWSN model.

Equation (9) determines the prevalence of data sensitivity shown in Tab. 6, indicating the percentage of data reduction achieved by the proposed technique. This calculation is based on the actual data size of events that occurred across the network over a period of time, as well as the actual blockchain

Tab. 4. Blockchain latency efficiency (BCLE) for the whole network

Time	Total event	BT [s]	TPT [s]	NPT [s]	TQT [s]	TTP [s]	BCLE
200	50	2.65	1.05	10.05	1.55	12.67	82.84%
400	80	4.40	2.16	16.4	2.32	21.25	84.08%
600	150	8.10	4.20	29.85	3.60	40.20	87.86%
800	160	8.16	3.84	34.08	4.16	42.08	83.75%
1000	250	14.00	5.75	52.75	6.75	67.00	84.54%

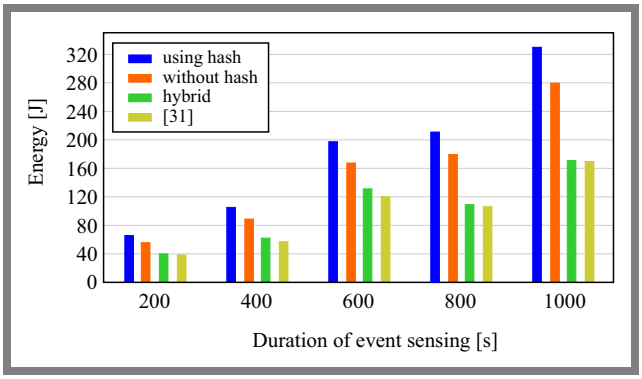

Fig. 5. Sensor zone energy comparison with [31].

size, which includes data blocks. The results suggest that the proposed technique is capable of reducing the size of the data approximately by 30%.

5.3. Comparison and Performance Analysis

This study focuses mainly on evaluating the energy efficiency within the sensor zone, particularly with respect to battery-operated leaf nodes. Although most of the research related to data integration using blockchain in ubiquitous wireless sensor networks tends to emphasize aspects such as integrity, security, and overall network life expectancy, this work takes a distinctive approach by directly comparing its energy efficiency within the sensor zone with the technique introduced in [31]. Figure 5 presents a comparison of the average energy consumption of the leaf nodes within the sensor zones in four different modes: with hash use, without hash use, using the proposed hybrid model and using the model introduced in [31].

Despite the fact that the proposed model includes hash usage for the creation of data blocks, which is known to require more energy for data processing and transmission, the figure shows that it consumes less energy than the scenarios of using hash exclusively and adhering to traditional methods, i.e. [31]. This is further supported by the comparison of energy efficiency in Fig. 6, calculated on the basis of Eq. (6) and the data represented in Tab. 3, which shows that the proposed model has an efficiency approximately 10% higher than [31].

Tab. 5. Blockchain throughput efficiency (BCTE) for the entire network.

Time	Interval	TPS	TPT [s]	BPR [s]	LPR	BCTE [%]
200	4	0.25	0.084	0.053	0.823	49.88
400	5	0.20	0.105	0.055	0.841	28.62
600	4	0.25	0.084	0.054	0.879	34.06
800	5	0.20	0.105	0.051	0.838	29.28
1000	4	0.25	0.084	0.056	0.845	43.54

Tab. 6. Pervasive data sensitivity (PDSN) for the whole network.

Duration	Event data size [bytes]	RR factor	Data block size [bytes]	PDSN
200	29640	0.53	19995	32.53%
400	74100	0.59	55648	24.90%
600	88920	0.54	61119	31.26%
800	148200	0.57	107524	27.44%
1000	148200	0.58	109411	26.17%

In order to fully evaluate the performance of the proposed hybrid model, this work draws a comparison with the technique introduced in [16], which also aims to improve the security and management of IoT data through a decentralized blockchain-based architecture.

To compute BCLE and BCTE for the approach from [16], this work relies on the data provided in their figures, and for the proposed model, this work uses Eqs. (7) and (8). The resulting BCLE values are presented in Tab. 4, and the BCTE values are detailed in Tab. 5. Based on the calculations and analysis, this work compiles the findings into a comparative graph shown in Fig. 7. In particular, the BCLE values for both models are quite similar. However, the proposed model exhibits a BCTE that is ≈25% better than that of the model proposed in [16].

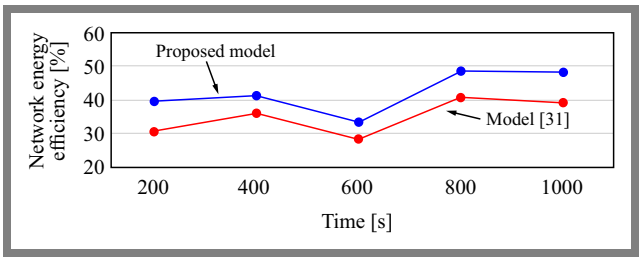

Fig. 6. Comparison of network energy efficiency.

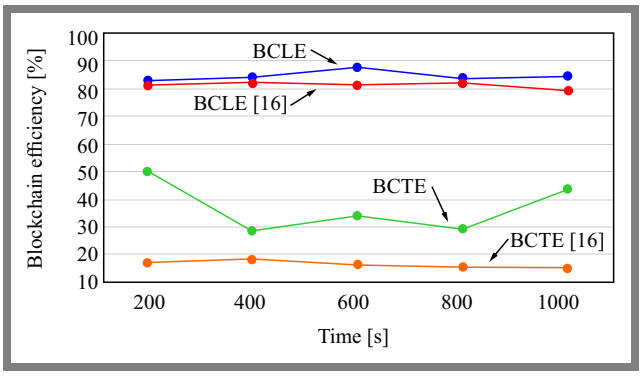

Fig. 7. Comparison of BCLE and BCTE metrics for the proposed model with [16].

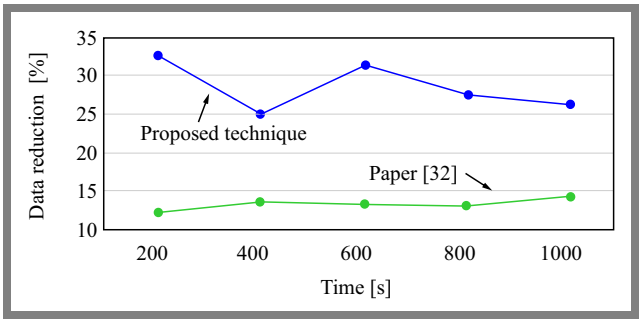

Fig. 8. Comparison of the data reduction percentage with [32].

The proposed technique utilizes the blockchain technology, increasing the amount of transmitted data. To address this problem, the proposed technique introduces a semantic mechanism to reduce the volume of data and creates a data block using the JSON format. The authors of [32] utilize semantic rules to reduce the weight of sensor data in different environments. Figure 8 shows that the proposed technique offers a significant improvement in terms of the data reduction percentage (≈20%) compared to [32].

6. Conclusion and Future Scope

This paper presented a novel hybrid architecture for pervasive wireless sensor networks (PWSNs) that integrates the blockchain technology to achieve secure and energy-efficient IoT data processing. The proposed design combines decentralized sink-node blockchain management with centralized sensing zones, providing both security and energy efficiency.

Implementation using TelosB Mote and Raspberry Pi devices demonstrated real-time data integration, while experimental results validated the model's higher energy efficiency, reduced latency, and improved throughput compared to existing methods.

Future studies will extend this prototype by incorporating consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) to analyze their impact on energy consumption and latency, thus improving the robustness and adaptability of blockchain-enabled PWSNs.

References

[1] D. Berdik *et al.*, "A Survey on Blockchain for Information Systems Management and Security", *Information Processing and Management*, vol. 58, art. no. 102397, 2021 (https://doi.org/10.1016/j.ipm.2020.102397).

[2] S. Darla and C. Naveena, "Survey on Securing Internet of Things through Blockchain Technology", *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2022 (https://doi.org/10.1109/ICEARS53579.2022.9752316).

[3] T.K. Araghi, D. Megías, and A. Rosales, "Evaluation and Analysis of Reversible Watermarking Techniques in WSN for Secure, Lightweight Design of IoT Applications: A Survey", *Advances in Information and Communication*, vol. 652, pp. 695–708, 2023 (https://doi.org/10.1007/978-3-031-28073-3_47).

[4] S. Kumar and V. Singh, "A Review of Digital Signature and Hash Function Based Approach for Secure Routing in VANET", *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, Coimbatore, India, 2021 (https://doi.org/10.1109/ICAIS50930.2021.9395882).

[5] A.A. Monrat, O. Schelän, and K. Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities", *IEEE Access*, vol. 7, pp. 117134–117151, 2019 (https://doi.org/10.1109/ACCESS.2019.2936094).

[6] A.K. Sharma and S. Mittal, "Cryptography and Network Security Hash Function Applications, Attacks and Advances: A Review", *2019 Third International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2019 (https://doi.org/10.1109/ICISC44355.2019.9036448).

[7] A. Singh and S. Gupta, "Learning to Hash: A Comprehensive Survey of Deep Learning-based Hashing Methods", *Knowledge and Information Systems*, vol. 64, pp. 2565–2597, 2022 (https://doi.org/10.1007/s10115-022-01734-0).

[8] S. Das and U. Mondal, "Acoustic Data Acquisition and Integration for Semantic Organization of Sentimental Data and Analysis in a PWSN", *Multimedia Tools and Applications*, vol. 84, pp. 26755–26777, 2024 (https://doi.org/10.1007/s11042-024-20229-4).

[9] S. Das and U. Mondal, "Energy Efficient Acoustic Sensor Data Integration in Hybrid Mode Operated Pervasive Wireless Sensor Network", *Telecommunication Systems*, vol. 87, pp. 61–72, 2024 (https://doi.org/10.1007/s11235-024-01165-y).

[10] S. Das and U. Mondal, "Pilot Agent Implied Efficient Data Communication in Pervasive Acoustic Wireless Sensor Network", *Telecommunication Systems*, vol. 88, art. no. 50, 2025 (https://doi.org/10.1007/s11235-025-01281-3).

[11] H. Guo and X. Yu, "A Survey on Blockchain Technology and its Security", *Blockchain: Research and Applications*, vol. 3, 2022 (https://doi.org/10.1016/j.bcra.2022.100067).

[12] C.V. Nguyen *et al.*, "Blockchain technology in wireless sensor network: benefits and challenges", *ICSES Transactions on Computer Networks and Communications*, vol. 10, pp. 1–4, 2021.

[13] S. Hsiao and W. Sung, "Utilizing Blockchain Technology to Improve WSN Security for Sensor Data Transmission", *Computers, Materials & Continua*, vol. 68, pp. 1899–1918, 2021 (https://doi.org/10.32604/cmc.2021.015762).

[14] T. Huynh-The *et al.*, "Blockchain for the Metaverse: A Review", *Future Generation Computer Systems*, vol. 143, pp. 401–419, 2023 (https://doi.org/10.1016/j.future.2023.02.008).

[15] S. Hsiao and W. Sung, "Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks", *IEEE Access*, vol. 9, pp. 72326–72341, 2021 (https://doi.org/10.1109/ACCESS.2021.3079708).

[16] A. Maftei, A. Lavric, A. Petrariu, and V. Popa, "Massive Data Storage Solution for IoT Devices Using Blockchain Technologies", *Sensors*, vol. 23, art. no. 1570, 2023 (https://doi.org/10.3390/s23031570).

[17] L.K. Ramasamy *et al.*, "Blockchain-based Wireless Sensor Networks for Malicious Node Detection: A Survey", *IEEE Access*, vol. 9, pp. 128765–128785, 2021 (https://doi.org/10.1109/ACCESS.2021.3111923).

[18] B. Sudheer and K. Sujatha, "A Brief Survey on Data Aggregation and Data Compression Models Using Blockchain Model in Wireless Sensor Network", *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, Uttarakhand, India, 2023 (https://doi.org/10.1109/ICIDCA56705.2023.10100009).

[19] O. Khalaf and G. Abdulsahib, "Optimized Dynamic Storage of Data (ODSD) in IoT Based on Blockchain for Wireless Sensor Networks", *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2858–2873, 2021 (https://doi.org/10.1007/s12083-021-01115-4).

[20] M. Madhi, A. Al-Bakry, and A. Farhan, "IoT Conception Based on Blockchain Technology: A Review", *Al-Mansour Journal*, vol. 39, pp. 1–9, 2023 (https://muc.edu.iq/oldwebsite/mucj/39/english/e4-b39.pdf).

[21] Y. Ren *et al.*, "Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks", *Mobile Information Systems*, 2018 (https://doi.org/10.1155/2018/6874158).

[22] M. Rajhi and A. Hakami, "A Cryptographic Iterative Hash Function Scheme for Wireless Sensor Network (WSNs) Security Enhancement for Sensor Data Transmission in Blockchain", *TechRxiv*, 2022 (https://doi.org/10.36227/techrxiv.19323308.v1).

[23] Z. Cui *et al.*, "A Hybrid Blockchain-based Identity Authentication Scheme for multi-WSN", *IEEE Transactions on Services Computing*, vol. 13, pp. 241–251, 2020 (https://doi.org/10.1109/TSC.2020.2964537).

[24] A. Mubarakali, "An Efficient Authentication Scheme Using Blockchain Technology for Wireless Sensor Networks", *Wireless Personal Communications*, vol. 127, pp. 255–269, 2021 (https://doi.org/10.1007/s11277-021-08212-w).

[25] R. Goyat *et al.*, "Blockchain-based Data Storage with Privacy and Authentication in Internet of Things", *IEEE Internet of Things Journal*, vol. 9, pp. 14203–14215, 2020 (https://doi.org/10.1109/JIOT.2020.3019074).

[26] A. Khan, N. Javaid, M. Khan, and I. Ullah, "A Blockchain Scheme for Authentication, Data Sharing and Nonrepudiation to Secure Internet of Wireless Sensor Things", *Cluster Computing*, vol. 26, pp. 945–960, 2023 (https://doi.org/10.1007/s10586-022-03722-z).

[27] S. Ismail, D. Dawoud, and H. Reza, "Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review", *Future Internet*, vol. 15, art. no. 200, 2023 (https://doi.org/10.3390/fi15060200).

[28] N. Alghamdi and M. Khan, "Energy-efficient and Blockchain Enabled Model for Internet of Things (IoT) in Smart Cities", *Computers, Materials and Continua*, vol. 66, pp. 2509–2524, 2021 (https://doi.org/10.32604/cmc.2021.014180).

[29] A. Ahmed *et al.*, "An Energy-efficient Data Aggregation Mechanism for IoT Secured by Blockchain", *IEEE Access*, vol. 10, pp. 11404–11419, 2022 (https://doi.org/10.1109/ACCESS.2022.3146295).

[30] B. Jo, R. Khan, and Y. Lee, "Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring", *Sensors*, vol. 18, art. no. 4268, 2018 (https://doi.org/10.3390/s18124268).

[31] M.S. Andhare *et al.*, "Design and Implementation of Wireless Sensor Network for Environmental Monitoring", *International Journal of Health Sciences*, vol. 6, pp. 3158–3169, 2022 (https://doi.org/10.53730/ijhs.v6ns4.9085).

[32] G. Urkude and M. Pandey, "Contextual Triple Inference Using a Semantic Reasoner Rule to Reduce the Weight of Semantically Annotated Data on Fail-safe Gateway for WSN", *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 5107–5121, 2021 (https://doi.org/10.1007/s12652-020-02836-9).

Sushovan Das, M.Tech.
Department of CSE
https://orcid.org/0000-0003-2759-3902
E-mail: das.sushovan@gmail.com
College of Engineering and Management, Kolaghat, Purba Medinipur, India
https://www.cemkolaghat.in

Uttam Kr. Mondal, Ph.D.
Department of Computer Science
https://orcid.org/0000-0002-7807-3002
E-mail: uttam_ku_82@yahoo.co.in
Vidyasagar University, Midnapur, India
https://www.vidyasagar.ac.in