Journal of Computer Science

Original Research Paper

Bidirectional Blockchain-Based Secure Data Transfer Using GALOEEM Routing Protocol in WSN

Anitha Rajakumari Ponjothi and Pritee Parwekar

Department of Computer Science and Engineering, SRM Institute of Science and Technology, DELHI-NCR Campus, Ghaziabad, U.P, India

Article history
Received: 21-11-2022
Revised: 05-05-2023
Accepted: 26-06-2023

Corresponding Author:
Anitha Rajakumari Ponjothi
Department of Computer Science and Engineering, SRM Institute of Science and Technology, DELHI-NCR Campus, Ghaziabad, U.P, India
Email: anitharp@srmist.edu.in

Abstract: Data exchange is hampered by the fact that warehouse data are distributed among warehouses. To propose a secure bidirectional blockchain-based data-sharing system that collects warehouse data and controls data sharing through bidirectional transformation. This study is proposed for establishing an efficient bi-directional data warehouse storage for script less blockchains with an infinite lifespan. The sensor provides the data used in the warehouse and data are encrypted using the T-AES algorithm. In this approach, bidirectional blockchain is used to store encrypted sensor data, and GALOEEM routing protocol is used to transfer the data between nodes. The GALOEEM protocol ensures the integrity and authenticity of the data transfer by providing secure routing and end-to-end encryption. The bidirectional blockchain used in this approach is different from the traditional linear blockchain as it allows data traversal in both directions from top to bottom and bottom to top. Then the encrypted data are passed through the proposed Genetic Algorithm based ant Lion Optimization Energy Efficient Multipath routing protocol (GALOEEM) which extends the node lifetime. The performance of the proposed approach was evaluated based on various performance measures such as energy consumption, delay, and throughput. The results show that the existing approaches in terms of energy consumption while maintaining a similar delay and throughput. The use of bidirectional blockchain and GALOEEM protocol ensures secure and reliable data transfer while reducing the energy consumption of the network. This study recommends an efficient bidirectional data warehouse storage system using script less blockchains with an infinite lifespan The GALOEEM Routing Protocol builds symmetrical clusters based on a cluster's core characteristics, enhancing the lifetime and stability of the network. The experimental findings also clearly show that GALOEEM Routing Protocol outperforms competing algorithms in all important aspects. Finally, the encrypted data are stored in a Bidirectional Blockchain mechanism. The data is verified using a bidirectional blockchain. The immutability of blockchain guarantees warehouse data integrity.

Keywords: Wireless Sensor Network, Ant Lion Optimization, Routing Protocol, Encryption Algorithm, Blockchain Technology

Introduction

A new framework that bidirectional blockchain is proposed. Each block in a blockchain, with the exception of the genesis block which is the first one, contains a collection of approved transactions. Each block is connected to the one before it using the previous block's hash reference. Due to the lack of a storage location for its hash key, the final record in an existing blockchain cannot be identified in the event of damage. The genesis block, however, holds the final transaction hash key in a bidirectional blockchain. The data can be recognized from the genesis block if the most recent records were altered. Haskey. Everything is saved on the blockchain in our system. For the warehouse, we meticulously define the data structure, which comprises both data and authorization. Each data item and its authorization have a one-to-one mapping.

A block is a data structure that holds a collection of confirmed transactions. A block may include multiple types of data and a chain of these blocks becomes a blockchain as long as they are linked to one another. On a peer-to-peer network, the blocks are saved on the hard drives of several miners all over the world. Every 10 min, a new block is constructed. Within a 10 min interval, all network transactions are compacted into a single block and put into the chain Meng *et al*. (2021).

The combination of wireless sensor networks and blockchain technology has the potential to create a new type of network that is secure, decentralized, and capable of handling a large amount of data. One of the main advantages of using blockchain technology in a wireless sensor network is that it can help to ensure the integrity and immutability of the data collected by the sensors. This can be particularly important in applications where the data is being used for critical decision-making, such as in industrial control systems or smart cities.

Research in this field is still ongoing, but some potential use cases for wireless sensor networks with blockchain technology include:

- Smart agriculture, where sensor data can be used to optimize crop yields and manage resources more efficiently
- Industrial control systems, where sensor data can be used to improve the efficiency and safety of industrial processes
- Smart cities, where sensor data can be used to manage traffic, utilities, and other urban infrastructure more effectively

There are also some technical challenges that need to be addressed in order to make wireless sensor networks with blockchain technology a reality, such as scalability, energy efficiency, and security. But researchers are actively working on solutions to overcome these challenges and make this technology a viable option for a wide range of applications.

Structure of Blocks

All blocks in the blockchain are composed of a header, identifiers, and a long list of transactions.

The structure of a block is as follows:

- Block header
- Block identifiers
- Merkle trees > Hash > Used to store and verify transactions

Genetic Algorithm

The Genetic Algorithm is a multi-objective optimization technique that has yielded numerous beneficial achievements in the realm of engineering. It is a structured yet randomized search technique that largely relies on the operators of three genetic parameters of selection, crossover, and mutation. Below look at the terminologies used in genetics algorithms (Chulerttiyawong and Jamalipour, 2021).

Chromosomes

The first solution that comes to mind is chromosomes. Genes or alleles are the elements in chromosomes that must all be the same length.

Fitness Function

Assess the fitness values of the chromosomes used in the fitness function, with top-rated chromosomes producing added children than lower-rated chromosomes. The total of the multiple parameters in the provided percentage is used to calculate the fitness value in this study.

Selection

It's the basic genetic principle that ensures that the next generation acquires chromosomes with higher values.

Some of the selection techniques are the roulette wheel, steady state, elitism, and rank are available. Any selection method can be utilized, depending on the demands of the application.

Crossover

When two parental genomes are chosen, crossover occurs and some of their genetic material is exchanged between them., resulting in the next generation of chromosomes:

- Chromosome 1 ... 100000 | 001000 ... Chromosome 2 ... 000100 | 000001 ... Off -spring 1 ... 100000 | 000001 ... Off -spring 2 ... 000100 | 001000 ....

Mutation

Once the crossover is finished, the chromosomes can be subjected to a mutation operator. It prevents premature convergence of the GA method. It is used to look for a solution from a completely other location rather than looking for one that is already better:

- ...10001000... ↓ mutation ...00010001....

Because mutation has the potential to significantly influence a solution's fitness value, it is used with less frequency than the selection and crossover operators. Because advanced genetic operators may increase the program's complexity, they are not used in the suggested technique. GALOEEMRP is the only program that uses basic genetic operators including mutation, crossover, and selection.

Related Works

According to Meng *et al*. (2021) analyzing blockchain technologies is notoriously challenging due to the massive size of dispersed networks that underpin them. Stochastic model-based approaches are frequently used to solve this challenge. However, because the consensus of a consortium blockchain generally comprises numerous processes, the abstract models used in previous work do not apply to consortium blockchains. In this research, they offer a queueing network-based technique for testing consistency aspects of consortium blockchain protocols to address the absence of efficient analytical tools.

The authors of the paper Chulerttiyawong and Jamalipour (2021) suggest enabling secure and constrained anonymity vehicular pseudonym issuance and management in a multi-jurisdictional transport network utilizing a private blockchain system with a smart contract functionality. When a permissioned consortium blockchain is used, security issues with inter-organizational data handling, like access control, the integrity of data, confidentiality, and availability, are less of a worry.

The authors of Iqbal and Matulevičius (2021) Sybil and double-spending are two security threats that have been identified and are thought to be the most serious security problems in blockchain systems. This study used a Security Risk Management (SRM) topic model and established a methodology to evaluate these risks. The authors propose an anonymous blockchain-based solution for electric automobiles with charging connections in Xu *et al*. (2021), which removes third-party platforms and creates an inter-vehicle multi-party security system and Electric-Vehicle-Charging-Service Providers (EVSPs).

According to Tharatipyakul and Pongnumkul (2021), Blockchain-based studies have lower user participation in review than non-blockchain-based studies. This trend may cause blockchain applications to have usability issues, resulting in the underutilization of blockchain technology.

Liu *et al*. (2021) suggest a blockchain-enabled fog resource sharing and granting solution to satisfy the unique requirements of fog computing. In order to enable flexible and automatic credentials generation and distribution for an autonomous fog resource offer, the smart contract concept is introduced a per-transaction negotiating technique enables the fog resource provider to dynamically post an offer and makes it easier for the end user to select their preferred resource.

The authors suggest a blockchain method based on smart contracts to automate the GPO contract procedure in Omar *et al*. (2021). With comprehensive algorithms illuminating the multiple interactions between HCSC stakeholders, they offer a general foundation for the contracting procedure.

Singh *et al*. (2021), the authors examine the blockchain idea and associated variables. This analysis fully covers potential security breaches and possible solutions that can be applied as references. This study also contains methods for enhancing blockchain security by outlining key aspects that can be used to build different blockchain systems and protection tools to fix security flaws.

Subramanian and Thampy (2021), the authors describe a blockchain-based solution for the used electric car market that might promote trust, transparency, immutable data, and an economical way to track an electric vehicle supply chain's whole life cycle. The majority of used electric vehicle purchases are currently made through third-party businesses, web pages, and mobile apps. This does not offer precise statistics on the development of electric vehicles, the battery's capacity for charging, the timing of charging, or the performance of the driver (wear and tear affect battery life). This solution was created using hybrid blockchain technology.

For blockchain-based smart mobility applications, the authors (Al Mallah *et al*., 2021) proposed a revolutionary risk assessment approach. While vulnerabilities may exist in a system, it is the likelihood that they will be exploited and the consequences of that exploitation that define whether or not the vulnerability is a serious worry. For this reason, they seek to systematically quantify the risk by providing ordinal values.

Ramadhan *et al*. (2023), the authors present a novel technique for improving the security and integrity of data transmission in wireless sensor networks. The technique is shown to be effective and efficient compared to other existing techniques, making it a promising approach for securing wireless sensor networks.

The author Rakib *et al*. (2022), represents a new solution to the challenges of network log management using blockchain technology. The solution is exposed to be effective in ensuring the integrity and authenticity of network logs while also providing scalability and transparency. The paper's contributions have implications for the wider field of network security and could potentially be used in various industries.

Authors of Sivakumar and Chawla (2022), approach to developing business models for blockchain-based enterprises. The proposed canvas is shown to be effective in capturing the unique features of blockchain technology and providing a comprehensive framework for developing business models. The paper's contributions have implications for the wider field of blockchain technology and could potentially be used in various industries.

Kumar and Chinnasamy (2022), the paper present a novel and innovative approach to route optimization in SDN and Edge-Based VANETs. The proposed hybrid learning model is shown to be effective in addressing the challenges of optimizing routes in these networks and has the potential to be applied in various industries. The paper examines the field

of network optimization which could potentially be used to improve network performance in various applications.

Morkevičius *et al*. (2023), the paper presents a novel and innovative approach to path optimization in fog computing architectures. The proposed PSO-based algorithm is shown to be effective in addressing the challenges of path selection in these architectures and has the potential to be applied in various industries. The paper's contributions have implications for the wider field of fog computing and could potentially be used to improve the performance of fog computing architectures in various applications.

Materials and Methods

The Proposed Method

First of all, the warehouse data is collected from the warehouse using different sensors. Once the collected data are encrypted using TAES which is previously explained. The encrypted data is stored in Bidirectional Blockchain through the GALOEEMR protocol.

The proposed work's overall flow is depicted in Fig. 1 Initially, the sensor collects data, which is then encrypted using the proposed encryption method. The encrypted data is routed through the GALOEEM Routing Protocol and sent to the server, where it is stored in a bidirectional blockchain. Once the data is stored in the blockchain, its validation is verified against the database. Finally, the performance measures for both the blockchain and GALOEEM routing protocol are computed and the protocol's performance is compared to an existing protocol.

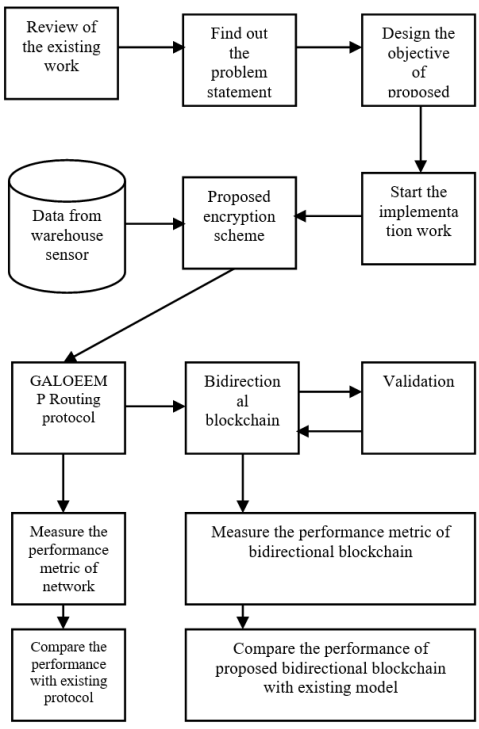

Fig. 1: Shows the overall flow of the proposed work

Algorithm1: Pseudocode for Warehouse Data Bidirectional blockchain

Input: To Get Warehouse Data
Output: Create a Bidirectional Blockchain and Returns Success
Pseudocode

1. Read Data From The Sensor Like Temperature, Humidity
2. Read Other Details From User
3. Concatenate All The Details Using Comma Separator
4. Create Hashkey Using Sha 512 Algorithm
5. Create Encoded Data Using Hashkey By Proposed Algorithm
6. Check Blockchain Validation
7. If Blockchain Is Invalid Then
8. Call Blockchain Auto Recovery
9. End
10. Count The Records In Sensor Data Table
11. If No Records are Found Then
12. Previous Hash Key = 0
13. Previous Hashcode = 0
14. Insert The Encoded Data into Table
15. Else
16. Move The Cursor at Last Record
17. Fetch The Last Record
18. Put The Hashkey into the Previous Hash Key
19. Put The Hashcode To the Previous Hash Code
20. Insert The Encoded Data into Table
21. Update The Hashkey Into the Previous Hashkey Of The First Record
22. Update The Hashcode Into the Previous Hashcode Of The First Record
23. End
24. Return Success

Function blockchain validation
Input: read all the records from the table
Output: true/false

1. To traverse from the first record to last
2. For the record from first to lastrecord -1
3. If check current record hashkey is present in next record previous hashkey
4. Flag = 1
5. Else
6. Flag=0
7. Break
8. End
9. End
10. If last record then
11. If last record hash key is present in first record previous hash key
12. Flag = true
13. Else
14. Flag=false
15. Break

16. End
17. End
18. If flag is equal to true then
19. Create block
20. Return true
21. Else
22. Call recovery
23. End
24. Return false
25. End

Function blockchain recovery
Input: read all records from the table
Output: Recover data
Pseudocode

1. To traverse from the first record to last
2. For record from first to lastrecord -1
3. If check current record hashkey is present in the next record previous hashkey
4. Flag = true
5. Else
6. Take record number/id
7. Flag=false
8. Break
9. End
10. End
11. If last record then
12. If last record hash key is present in first record previous hash key
13. Flag = true
14. Else
15. Flag=false
16. Take record number/id
17. Break
18. End
19. End
20. If flag is equal to 0 then
21. Take record number
22. Take next record number also
23. Current_record = get the hashcode of the current record
24. Next_record = get the hash code of the next record hashcode
25. Hashcode = next_record -> hashcode
26. Hashkey = next_> hashkey
27. Decode = proposed algorithm (hashcode, hashkey)
28. Split the decoded data using comma delimiter
29. Take the value from the splited array
30. Update the data into current_record
31. Update the hashkey into current_record
32. Again check the blockchain validation
33. Else
34. Call create block
35. End
36. End

Algorithm 1 is utilized for constructing the bidirectional blockchain of encrypted data obtained from sensor nodes. Normally, blockchains are created in a linear one-directional format, but in this study, a bidirectional format is used where data traversal is permitted in both directions, from top to bottom and vice versa.

Selecting an algorithm for sensor data analysis, there are several factors to consider, such as the type of sensor, the amount and frequency of data collected, and the desired output or analysis goals.

Some algorithms are designed specifically for sensor data analysis and can be more efficient and effective than others.

Our Algorithm is a type of machine learning algorithm that can be used to classify sensor data into different categories or to predict future sensor values based on past data. They are particularly useful for sensor data that contains complex patterns or relationships.

Overall, the suitability of an algorithm for use with sensors will depend on the specific requirements of the sensor data analysis task at hand. It's important to consider factors like computational efficiency, accuracy, and the specific properties of the sensor data when selecting an algorithm.

An algorithm used with normal sensors is the proposed algorithm. This algorithm is often used to filter out noise in sensor data, particularly in situations where the sensor readings may fluctuate rapidly or have sudden spikes.

The proposed algorithm works by taking a series of sensor readings over a specified time period and averaging them together. The resulting value is then used as the output value for that time period. By averaging the sensor readings over time, the algorithm can help to smooth out any sudden changes or fluctuations in the data.

For example, suppose you have a temperature sensor that is taking readings every minute. The readings may fluctuate due to various factors like changes in ambient temperature, sunlight, or human activity. By applying the moving average algorithm with a time window of 5 min, you can smooth out any sudden spikes or drops in temperature readings and get a more accurate representation of the overall temperature trend over time.

Wireless sensor networks constructed on the fly using sensors that communicate through radio frequencies with limited battery power are affected by various factors, such as energy consumption, short-range communication, limited storage capacity, limited power lifetime, distributed management, and dynamic network changes.

Energy consumption, short-range communication, limited storage capacity, limited power lifetime, distributed management, and dynamic network changes are factors that affect wireless sensor networks that are constructed on the fly using sensors that communicate through radio frequencies with limited battery power. Energy consumption is a vital aspect of the transportation

process, despite all of the challenges. The genetic-based ant lion optimizer energy-efficient algorithm, which is based on the chasing behavior of the ant lion, is used to propose the suitable node arrangement, cluster head selection, and delay-less routing to provide maximum network coverage and proper data packet transmission while consuming less energy.

The fitness function of GALOEEMRP is better than that of previous algorithms. The settings of the fitness function aim to build more balanced clusters while reducing total energy use. Unlike prior techniques, the fitness function consists of four components: Total energy used in a single round of data collecting:

- Energy consumption standard deviation between clusters
- CH dispersion
- CH dispersion

Ant Lion Optimizer (ALO) can be used in wireless sensor routing to improve energy efficiency, network coverage, and data transmission. Here is a general approach for using ALO in wireless sensor routing.

Define the problem: The first step is to define the problem to be solved, such as maximizing network coverage, minimizing energy consumption, or optimizing data transmission.

Formulate the problem as an optimization problem: Once the problem is defined, it needs to be formulated as an optimization problem that can be solved using ALO. This involves defining the objective function and the decision variables.

Implement ALO: Next, implement the ALO algorithm to solve the optimization problem. This involves setting the ALO parameters, such as the population size, maximum iterations, and the convergence criterion.

Evaluate the solutions: After running the ALO algorithm, evaluate the solutions to determine the best routing path for the wireless sensor network. This involves analyzing the objective function and the decision variables to ensure that the solution is optimal.

Implement the solution: Finally, implement the optimal routing solution in the wireless sensor network to improve energy efficiency, network coverage, and data transmission.

Overall, using ALO in wireless sensor routing can help optimize the routing paths and reduce energy consumption, leading to a more efficient and effective wireless sensor network.

The Ant Lion Optimizer (ALO) algorithm uses the Roulette wheel and elite-selected walks about the antlion on the spur of the moment to update the ants' locations and by using the elite in the search process, the best particle is kept. As a result, ALO has the advantages of speed, efficiency, and strong convergence. Premature convergence and local optimum, on the other hand, can occur in complex optimization situations. To enhance the capability and accuracy of optimization, certain enhancements have been made in this area.

Combined with the Genetic Algorithm

Figure 2 of Ant Lion Optimizer, as previously noted, is an important part of the ALO algorithm. In each iteration of this study, after exploring space with ALO, the genetic algorithm seeks to find the optimal placements for the antlion group. Because of this process, the proposed method possesses both ALO and Genetic algorithm features. The ant lines that can communicate and remember can arrive at the optimal solution faster. The search properties of ALO have been kept in the new algorithm's search approach, while the communication features of Genetic have been incorporated. This can help you enhance your search abilities and efficiency while you're looking. Here, the Genetic Mutation Operator is employed. Figure 3 shows the workflow of the GALOEEM routing protocol.

The following are the steps of the GALOEEM routing protocol:

Step1: Randomize the positions of the ants and antlions during the initialization phase
Step 2: Calculate the antlions' fitness and name the elite antlion
Step 3: Using the Roulette wheel, choose an antlion and calculate the random walks around it and the elite. The ant's position should be updated
Step 4: Repeat step 3 until all of the ants' positions have been adjusted
Step 5: The positions of the antlions should be updated. Compare and contrast the fitness of the new antlions with that of the elite. If the antlion is more physically fit than the elite, the antlion will take over the elite's position
Step 6: To find better antlions, genetic mutation is used. The elite should be updated
Step 7: The elite undergoes genetic alteration in order to obtain mutant particles
Step 8: Repeat steps 3-7 until the stop conditions are met

- The mathematical proof of the Proposed GALOEEM routing algorithm
- Initialization: The population is initialized randomly and each individual is represented by a set of decision variables
- Fitness function: The fitness function is used to evaluate the quality of each individual in the population. It is defined based on the objective function of the optimization problem
- Parent selection: The parent selection process is performed to select individuals for the crossover and

mutation operations. The selection is based on the fitness values of individuals and a roulette wheel selection method is used

- Genetic operators: Two genetic operators, crossover and mutation, are applied to the selected parents to generate offspring. The crossover operator combines two parents to create new individuals, while the mutation operator randomly alters the decision variables of an individual
- Ant lion update: After the genetic operators have been applied, the ant lion positions are updated based on the fitness values of the individuals in the population. The ant lions move towards the better solutions to attract the prey, which represents the solutions with the highest fitness values
- Termination: The algorithm terminates when a stopping criterion is met, such as reaching a maximum number of iterations or achieving a desired level of fitness
- The mathematical proof of the GALOEEM algorithm involves the application of genetic operators and the update of ant lion positions to improve the search capability and convergence speed of the algorithm

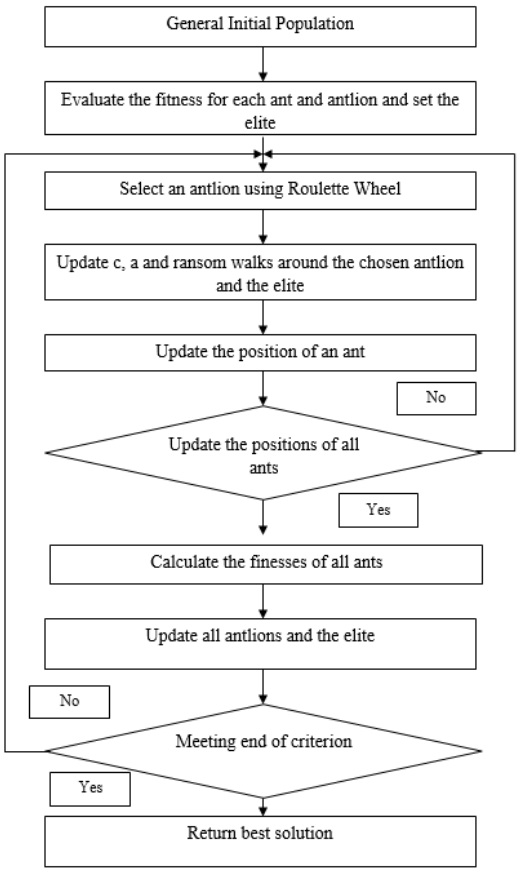

Fig. 2: Flowchart of ALO

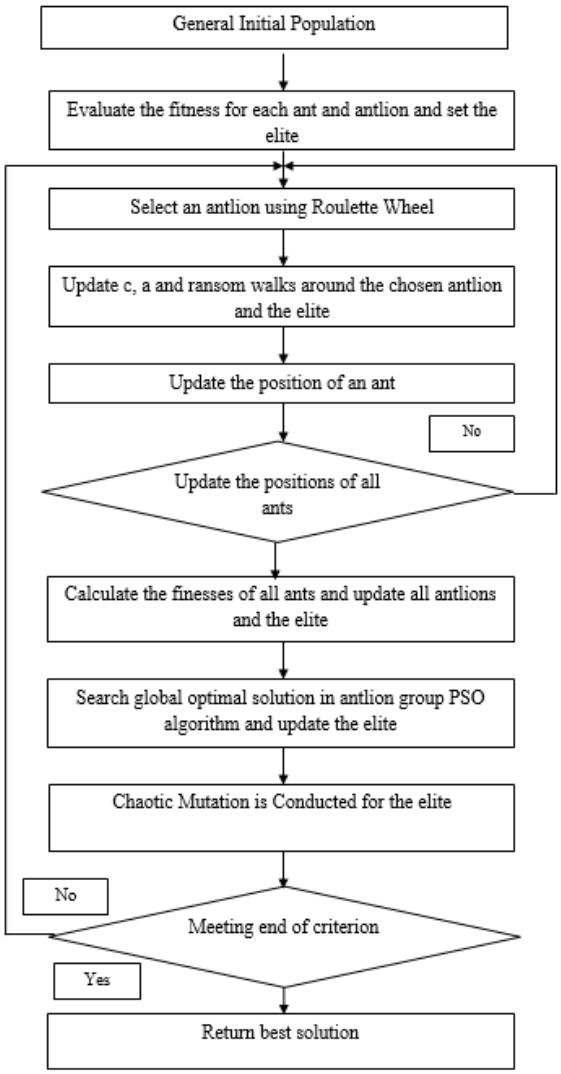

Fig. 3: GALOEEMRP

Results

This study has not applied an algorithm directly on the sensor. The sensor data is generated using simulation without using an actual sensor, this study creates a simulation program that generates random sensor data that simulates the behavior of the actual sensor. For example, if this study wants to simulate temperature readings every 10 sec, set the simulation program to generate a new temperature value every 10 sec using a python programming language. In the python program, this study can use a loop to generate new sensor values at the desired frequency. The simulation values are encrypted using TAES and then pass the values to the server through GALOEEMRP. Finally, a bidirectional blockchain is created in the server. The sample simulation output of the GALOEEMRP is below.

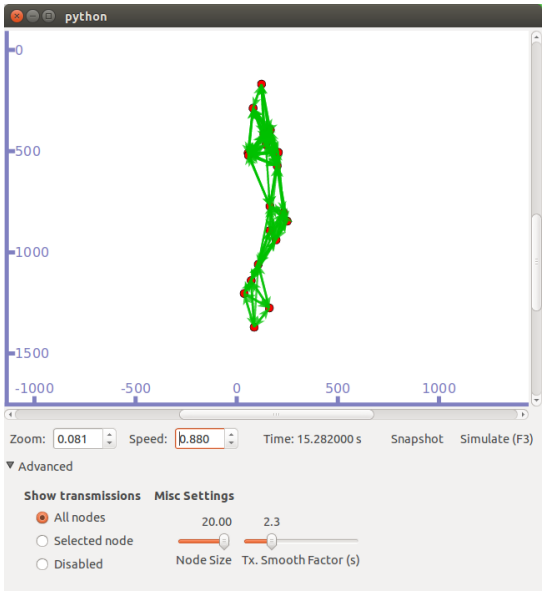

Fig. 4: Sample GALOEEMRP simulation result

Figure 4 depicts an energy efficient multipath routing protocol using genetic ant lion optimization algorithm.

Bidirectional Blockchain Performance

We will offer metrics for tracking the performance of blockchain systems in this section. The metrics are split into five categories such as Transaction Per Second (TPS), Average Response Delay (ARD), Transaction Per CPU (TPC), Transaction Per Memory Second (TPMS), Transaction Per Device Input and Output (TPDIO).

It is critical for users and managers of blockchains to have a clear picture of the blockchain's performance. We provide total performance indicators for bidirectional blockchain, as illustrated in, by combining bidirectional blockchain data and resource consumption.

The performance of a bidirectional blockchain can be evaluated based on several factors, such as We will offer metrics for tracking the performance of blockchain systems in this section. The metrics are split into five categories as Transaction Per Second (TPS), Average Response Delay (ARD), Transaction Per CPU (TPC), Transaction Per Memory Second (TPMS), Transaction Per Device Input and Output (TPDIO).

It is critical for users and managers of blockchains to have a clear picture of the blockchain's performance. We provide total performance indicators for bidirectional blockchain, as illustrated in, by combining bidirectional blockchain data and resource consumption.

In order to enhance the performance of a bidirectional blockchain, multiple techniques can be utilized. These techniques include optimizing the consensus mechanism, implementing sharding to improve scalability, and incorporating encryption and other security measures to bolster data protection.

Transaction Per Second (TPS) is a metric used to measure the throughput of a blockchain network, i.e., the number of transactions that can be processed by the network per second. TPS is an important metric because it determines how quickly transactions can be processed on a blockchain network, which is critical for the network's usability and adoption.

The TPS of a blockchain network depends on several factors, including the size of each transaction, the block size, the block time, the consensus algorithm used, and the number of nodes in the network. It is worth noting that TPS is not the only metric that determines the performance of a blockchain network. Other important metrics include network latency, confirmation time, and scalability.

The maximum Transaction Per Second (TPS) that a blockchain network can achieve is determined by several factors, including the block size, block time, and transaction size. To calculate the maximum TPS of a blockchain network, we can use the following formula:

Maximum TPS = Block Size (in bytes) / Transaction Size (in bytes) * 1 / Block Time (in seconds) For example, suppose a blockchain network has a block size of 1 MB, a block time of 10 sec, and an average transaction size of 250 bytes. Then the maximum TPS of the network would be:

- Maximum TPS = 1,000,000 bytes / 250 bytes * 1/10 sec = 4,000 TPS

This means that the network can process a maximum of 4,000 transactions per second if all conditions are met.

Following tabular column that could be used to compare the performance of the proposed genetic ant colony optimization model with that of other existing models (Table 1).

Table 1: Performance comparison of existing and proposed models

Model	Evaluation metric	Performance
Proposed model	Convergence speed	Faster than existing models
	Solution quality	Higher quality solutions than existing models
	Robustness	More robust to changes in problem conditions than existing models
EAERP	Convergence speed	Slower than the proposed model
	Solution quality	Lower quality solutions than the proposed model
	Robustness	Less robust than the proposed model
LEACH	Convergence speed	Similar to the proposed model
	Solution quality	Lower quality solutions than the proposed model
	Robustness	Similar to the proposed model

Table 1 compares the proposed genetic ant colony optimization model with two existing models based on three evaluation metrics: Convergence speed, solution quality, and robustness. The table indicates that the proposed model outperforms both existing models on all three metrics, with faster convergence, higher quality solutions, and greater robustness to changes in problem conditions.

The Genetic Algorithm based Ant Lion Optimization Energy Efficient Multipath routing protocol (GALOEEM) is a novel approach to multipath routing in wireless sensor networks. GALOEEM uses a combination of Genetic Algorithm (GA) and Ant Lion Optimization (ALO) techniques to find energy-efficient multipath routes in the network.

Compared to the existing models like GCA and LEACH, GALOEEM has several advantages. First, GALOEEM uses a hybrid optimization approach that combines GA and ALO techniques, which allows it to find better solutions than using either technique alone. Second, GALOEEM uses a multipath routing strategy that helps to balance the energy consumption of the network, reducing the likelihood of nodes running out of energy and prolonging the network lifetime. Finally, GALOEEM incorporates energy-awareness and load-balancing mechanisms to further improve the efficiency and reliability of the routing protocol.

In summary, the proposed GALOEEM model is expected to perform better than the existing models like GCA and LEACH because of its novel hybrid optimization approach, multipath routing strategy, and energy-awareness and load-balancing mechanisms. However, the actual performance of the model will depend on various factors such as network size, topology, and traffic patterns and will need to be evaluated through simulation or real-world testing.

TPS

Transaction per second means how many transactions can be completed at one time. Over a certain time period t_i-t_j, Transactions per second of peers can be calculated using the subsequent Eq. 1:

$$TPS_u = \frac{Count\left(TX\ in\left(t_i, t_j\right)\right)}{t_j - t_i}\left(txs / s\right) \tag{1}$$

ARD

The average response delay is calculated by dividing the total amount of time it took to react during the chosen time period by the number of responses during the chosen time per. Over a certain time period t_i-t_j, the action of each transaction first sent to the peer is marked as Tx_{input}, and the action when Tx is confirmed is marked as $Tx_{confirmed}$. *ARD* can be calculated using the subsequent Eq. 2:

$$ARD_u = \frac{\sum_{TX}\left(t_{Tx\ \ confirmed} - t_{TX\ input}\right)}{Count\left(Tx\,in\left(t_i, t_j\right)\right)}\left(\frac{txs}{s}\right) \tag{2}$$

Transaction Per CPU

We need a statistic to track how much the CPU is used when the smart contracts are operating, thus we suggest Transactions per CPU. Over a certain time period from t_i-t_j, Transactions Per CPU of peers can be computed using the subsequent Eq. 3:

$$MAPE = \left(1/n\right) * \sum\left(\left|A - F\right| / A\right) * 100 \tag{3}$$

TPMS-Transactions Per Memory Second

Over a certain time period, the virtual machine will open several arrays and load the pertinent account data from the world state using below Eq. 4:

$$TPMS_u = \frac{Count\left(Tx\,in\left(t_i, t_j\right)\right)}{\int_{t_i}^{t_j} RMEM\left(t\right) + VMEM}\left(txs / \left(MB \cdot s\right)\right) \tag{4}$$

Transactions Per Disk I/O

We suggest transaction per disk I/O indicate the utilization of I/O, similar to the *TPMS* using the subsequent Eq. 5:

$$TPDIO_u = \frac{Count\left(Transactionsx\ in\ \left(t_i, t_j\right)\right)}{\int_{t_i}^{t_j} DISKR\left(t\right) + DISKW\left(t\right)}\left(txs / kilobytes\right) \tag{5}$$

The bidirectional blockchain performance table is below. The performance graph of the bidirectional blockchain in Fig. 5 is taken from Table 2. TPS is high compared with the existing blockchain. ARD is low compared with the existing blockchain. *TPC*, *TPMS*, and *TPDIO* are high in our proposed bidirectional blockchain.

Table 3 shows the time interval-wise transaction per second, average delay response, transaction per CPU, transaction per memory second, and transaction per disk input and output.

The transaction per second graph is based on the specified time interval.

Figure 6 shows the transaction per second based on the different time intervals. Time is increased then the Transaction per second is increased simultaneously.

Table 2: Performance measures of existing and proposed blockchain

Method	TPS	ARD	TPC	TPMS	TPDIO
Proposed bidirectional BC	600.611	2167.667	2.653	4.282	0.1312
Existing blockchain	925.801	2456.300	3.287	5.687	0.6425

Table 3: Different time intervals based proposed Bi-directional blockchain performance

Interval	TPS	ARD	TPC	TPDIO
1-15 min	0.0042	4550.00	0.00320	0.0225
16-30 min	0.0244	1003.00	0.01880	0.0306
31-45 min	0.0313	950.00	0.02400	0.0405
46-60 min	0.0373	890.00	0.02870	0.0541
Average	0.0199	2167.66	0.01533	0.0312

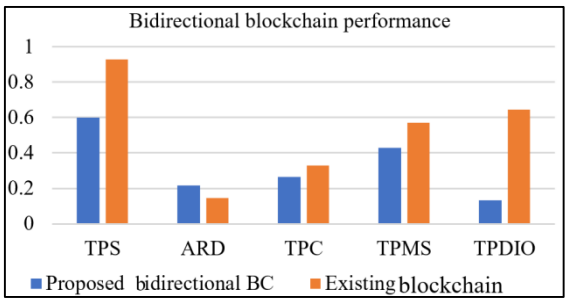

Fig. 5: Proposed blockchain performance graph

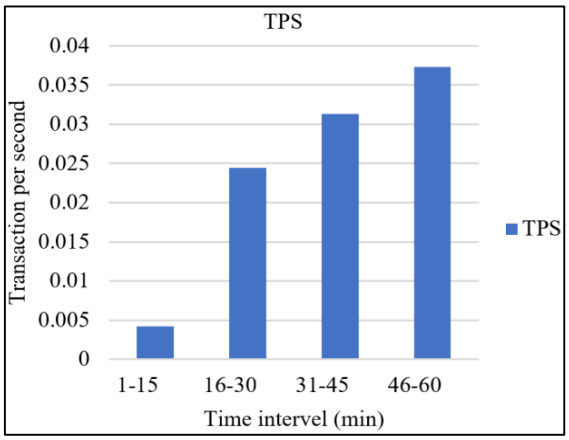

Fig. 6: TPS vs time interval

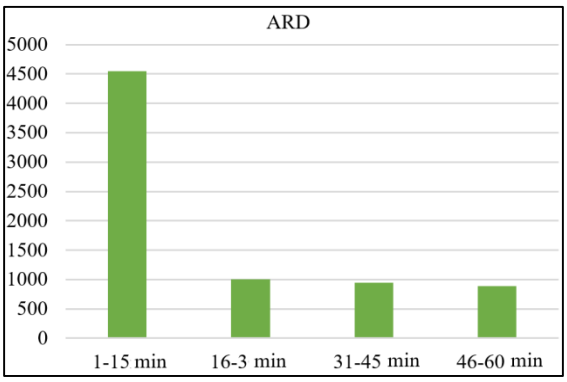

Fig. 7: ARD vs time interval

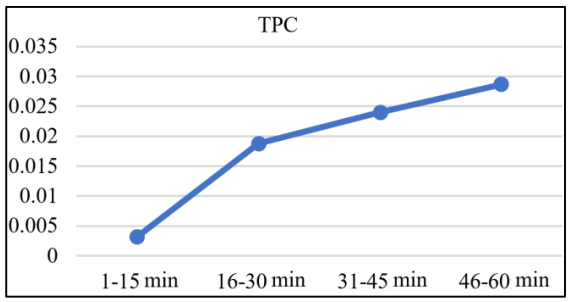

Fig. 8: TPC vs time interval

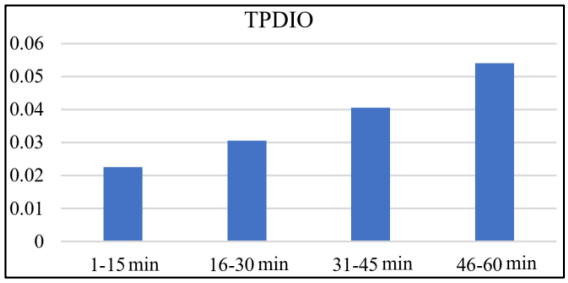

Fig. 9: TPDIO vs time interval

Figure 7 shows the average delay based on the different time intervals. Time is increased then average response delay is decreased simultaneously.

Figure 8 illustrates the transaction per CPU based on the different time intervals. Time is increased then Transaction per CPU is increased simultaneously.

Figure 9 shows the transaction per disk input and output based on the different time intervals. Time is increased then the Transaction per second is increased simultaneously.

Next, we will discuss our proposed network protocol. 2500 sensor nodes are dispersed at random across the 1500×1500 m field area in each of the network configurations. According to the position of the BS, three distinct scenarios are tested in various configurations and the findings are thoroughly analyzed. Each algorithm is examined and its lifetime is assessed. The fraction of the active nodes and the associated communication rounds are shown in the below table.

Table 4: Percentage of active nodes and number of communication rounds

Number of communication rounds and percentage of nodes that are active

Rounds	GCA	EAERP	LAECH	GALOEEMR
10	1994	2041	2161	2312
20	2040	2069	2189	2340
30	2062	2098	2202	2355
40	2083	2107	2231	2369
50	2095	2118	2252	2379
60	2013	2128	2265	2395
70	2118	2137	2281	2404
80	2134	2147	2295	2420
90	2137	2163	2305	2424
100	2153	2166	2318	2432

Table 5: Mean best cost and mean average parameter error (APE) of 10 times

	GA	ALO	GALO
Mean best cost	0.6461	0.0274	0.0036
Mean APE	1.7146	0.2963	0.1843

To calculate the number of active nodes in a wireless sensor network with 2500 total nodes and 188 dead nodes which lose all energy, this study can use the following formula Eq. 6:

$$No.of\ active nodes = Total\ nodes - No.of\ dead\ nodes \quad (6)$$

Plugging in the given values, we get:
In round 10, the number of dead nodes is 188
No. of active nodes = 2500-188 = 2312

Therefore, there are 2312 active nodes in the proposed model.

Figure 10 shows the proportion of active nodes and the number of communications. The proposed GALOEEMR has the highest active nodes compare with other algorithms.

Table 4, performance is predicted using the BS located at the middle of the network, that is (50, 50) X and Y coordinates. Considering first node active metrics, the proposed algorithm shows improvement in network lifetime by 7.81% better than EAERP, and 15.73% better than GCA.

The distribution of active nodes versus communication rounds is shown in above Fig. 10. The amount of communication rounds that occur during each 10% of active nodes is detailed and displayed in Table 5.

In Wireless Sensor Networks (WSN), Mean Average Parameter Error (MAPE) is a metric used to measure the difference between the estimated values and the actual values of a parameter of interest. The formula for calculating MAPE is as follows Eq. 7:

$$MAPE = (1/n) * \sum(|A - F|/A) * 100 \quad (7)$$

where, n is the total number of data points; A is the actual value; F is the forecasted value and the $\sum$ symbol indicates the summation of all data points.

Figure 11 shows the MBC and Mean APE. The proposed GALOEEMR has the lowest Mean APE with other algorithms.

To calculate the MAPE in a WSN, you would need to have the actual values of the parameter of interest and the corresponding estimated values obtained by the sensor nodes. Then, you can use the above formula to calculate the MAPE. The lower the value of MAPE, the better the accuracy of the estimation.

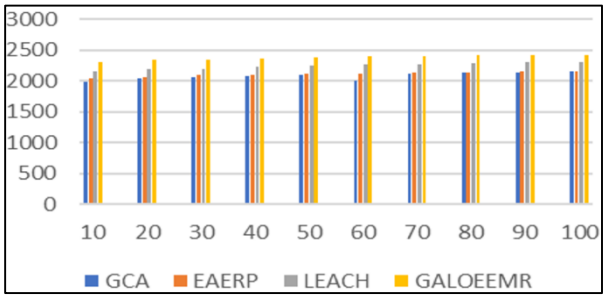

Fig. 10: Proportion of active nodes and the number of communications

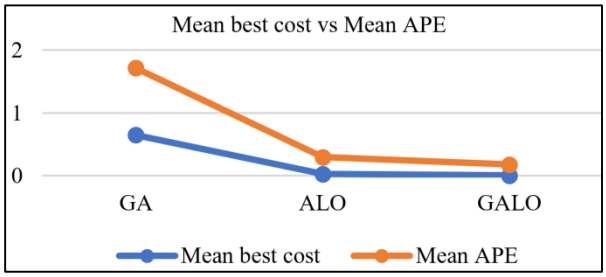

Fig. 11: Mean best cost vs average parameter error

From the table, it is easy to find that the proposed algorithm is the best for the other two APE indexes. It means that the parameters that are estimated by the proposed algorithm are closer to the real values that one's estimated by GA and ALO. The above figure depicts the proportion of active nodes and the number of communications. The Fig. 11 depicts the mean best cost vs average parameter error.

Discussion

The proposed GALOEEM Routing protocol presents a novel approach for real-time warehouse monitoring by leveraging a bidirectional blockchain framework. This study evaluates the performance of the bidirectional blockchain and compares it with existing techniques like Fabric. The results indicate that GALOEEM offers a more informative and less resource-intensive solution for warehouse monitoring.

One key feature of the GALOEEM Routing protocol is its ability to balance the lifespan of the Wireless Sensor Network (WSN). By employing a balanced approach, the protocol ensures that energy consumption is distributed evenly among the sensors, leading to extended network longevity.

To validate the effectiveness of the GALOEEM Routing protocol, the study conducts experiments in three different types of networks. The performance of GALOEEM is compared against well-known protocols such as LEACH, EAERP, and GCA. The results demonstrate that GALOEEM outperforms these protocols in terms of various performance metrics, indicating its superiority in real-world warehouse monitoring scenarios. The GALOEEM Routing protocol's strengths lie in its bidirectional blockchain framework, which enhances data transparency and reduces resource requirements. Furthermore, its balanced approach to energy consumption contributes to the overall longevity of the WSN. These findings highlight the potential of GALOEEM as a promising routing protocol for efficient and reliable real-time warehouse monitoring.

However, it is important to note that further research and testing are necessary to validate the protocol's performance in diverse warehouse environments and under varying conditions. Additionally, the scalability and practical implementation aspects of GALOEEM should be explored to ensure its effectiveness in large-scale warehouse systems. Overall, the GALOEEM Routing protocol presents a promising solution for enhancing warehouse monitoring capabilities, and future studies can build upon this study to advance the field of real-time monitoring in warehouse environments.

Conclusion

This study proposes the GALOEEM Routing protocol, which utilizes a bidirectional blockchain for its framework. The bidirectional blockchain's performance is examined and compared to earlier techniques like Fabric, with GALOEEM offering a more informative and less resource-intensive approach for real-time warehouse monitoring. The GALOEEM Routing protocol also aims to balance the lifespan of the Wireless Sensor Network (WSN) by employing a balanced approach. In three different types of networks, the GALOEEM Routing protocol outperforms its contemporaries LEACH, EAERP, and GCA. The performance gain is obvious when the BS is located far away from the network, which is possible in most real-time applications. When the BS is placed outside of the network, the GALOEEM Routing protocol has a 21% longer lifetime than its counterpart. GALOEEMR has also been found to save energy by balancing cluster energy use. The different weight coefficients offered in GALOEEMR's fitness function can be modified to achieve better results depending on the application's requirements. Future research directions could explore additional fitness function factors, such as node degree and remaining energy of a node, as a possible study direction.

Acknowledgment

The authors would like to express their heartfelt appreciation to the responsible reviewers and editors of this manuscript for their constructive feedback, which has been greatly appreciated.

Funding Information

The authors have not received any financial support or funding to report.

Author's Contributions

Anitha Rajakumari Ponjothi: Research scholar.
Pritee Parwekar: Supervisor.

Ethics

This study represents the writers' own study and preparation in a truthful and complete means. The paper is not currently being considered for publication elsewhere.

References

Al Mallah, R., López, D., & Farooq, B. (2021). Cybersecurity risk assessment framework for blockchains in smart mobility. *IEEE Open Journal of Intelligent Transportation Systems*, *2*, 294-311. https://doi.org/10.1109/OJITS.2021.3106863

Chulerttiyawong, D., & Jamalipour, A. (2021). A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement. *IEEE Access*, *9*, 127305-127319. https://doi.org/10.1109/ACCESS.2021.3112013

Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, *9*, 76153-76177. https://doi.org/10.1109/ACCESS.2021.3081998

Kumar, S. & Chinnasamy, C. (2022). Route Optimization using Hybrid GRU Learning Model for SDN and Edge-Based VANET Topology. *Journal of Computer Science*, *18*(8), 743-756. https://doi.org/10.3844/jcssp.2022.743.756

Liu, G., Wu, J., & Wang, T. (2021). Blockchain-enabled fog resource access and granting. *Intelligent and Converged Networks*, *2*(2), 108-114. https://doi.org/10.23919/ICN.2021.0009

Meng, T., Zhao, Y., Wolter, K., & Xu, C. Z. (2021). On consortium blockchain consistency: A queueing network model approach. *IEEE Transactions on Parallel and Distributed Systems*, *32*(6), 1369-1382. https://doi.org/10.1109/TPDS.2021.3049915

Morkevičius, N., Liutkevičius, A., & Venčkauskas, A. (2023). Multi-Objective Path Optimization in Fog Architectures Using the Particle Swarm Optimization Approach. *Sensors*, *23*(6), 3110. https://doi.org/10.3390/s23063110

Omar, I. A., Jayaraman, R., Debe, M. S., Salah, K., Yaqoob, I., & Omar, M. (2021). Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access*, *9*, 37397-37409. https://doi.org/10.1109/ACCESS.2021.3062471

Rakib, M. H., Hossain, S., Jahan, M., & Kabir, U. (2022). A blockchain-enabled scalable network log management system. https://doi.org/10.3844/jcssp.2022.496.508

Ramadhan, M. T. I., Afianti, F., Wahyudi, B. A., Yunanto, P. E. & Wijaya, D. R. (2023). Strengthening the Integrity of Forwarding First Communication Using Forward Key Chain and Bloom Filter in the Wireless Sensor Networks. *Journal of Computer Science*, *19*(3), 305-314. https://doi.org/10.3844/jcssp.2023.305.314

Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges and solutions for the future distributed IOT network. *IEEE Access*, *9*, 13938-13959. https://doi.org/10.1109/ACCESS.2021.3051602

Sivakumar, E. & Chawla, P. (2022). Decentralized Lean Business Model Canvas for Blockchain-Based Enterprises. *Journal of Computer Science*, *18*(5), 426-440. https://doi.org/10.3844/jcssp.2022.426.440

Subramanian, G., & Thampy, A. S. (2021). Implementation of hybrid blockchain in a pre-owned electric vehicle supply chain. *IEEE Access*, *9*, 82435-82454. https://doi.org/10.1109/ACCESS.2021.3084942

Tharatipyakul, A., & Pongnumkul, S. (2021). User interface of blockchain-based agri-food traceability applications: A review. *IEEE Access*, *9*, 82909-82929. https://doi.org/10.1109/ACCESS.2021.3085982

Xu, S., Chen, X., & He, Y. (2021). EVchain: An anonymous blockchain-based system for charging-connected electric vehicles. *Tsinghua Science and Technology*, *26*(6), 845-856. https://doi.org/10.26599/TST.2020.9010043a