Journal of Scientific & Industrial Research
Vol. 83, May 2024, pp. 567-580
DOI: 10.56042/jsir.v83i5.711

Block chain Technology for Trusted Network in Wireless Sensor Network

Shivaprasad Sakharam More[1]*, Priyanka Shivaprasad More[1,2] & Pooja Bagane[3]

[1]DKTE Society's Textile and Engineering Institute, Ichalkaranji, Maharashtra, India
[2]Lovely Professional University (LPU), Phagwara, Punjab, India
[3]Symbiosis Institute of Technology, Constituent of Symbiosis International (Deemed University), Pune, India

Received 18 April 2023; revised 19 December 2023; accepted 02 April 2024

Block chain technology can provide an efficient security mechanism for creating a trusted network in Wireless Sensor Networks (WSNs). By utilizing distributed ledger technology, network nodes can securely exchange and verify information. This study further explores the potential of block chain technology in enhancing the security and trustworthiness of WSNs. An efficient security mechanism using block chain technology can be implemented in WSNs to establish a trusted network. Block chain ensures secure communication by providing decentralized consensus, data integrity, and tamper-proof verification. This mechanism mitigates common WSN security issues such as unauthorized access, data tampering, and node impersonation. This system aims to establish a trusted network by decentralizing security measures, ensuring data authenticity and integrity, and preventing various attacks such as tampering, spoofing, and data manipulation. The study suggested a block chain-enabled trusted algorithm for clustered-based Energy-Efficient Routing Protocol (EERP) in a WSN by locating the ideal Cluster Head (CH) in the network. For the accurate CH selection, several techniques like Mayfly Water Wave Optimisation (MF-WWO), Rivets-Shamir Adleman (RSA) are utilized to secure data transfer. MATLAB software has been used for simulation. The findings illustrated that the Particle Swarm Optimization (PSO) algorithm has the highest fitness value of 97%. The upcoming possibility of efficient security mechanisms using block chain technology in WSNs includes enhanced data integrity, confidentiality, and availability.

Keywords: Cluster head, Data integrity, Energy-efficient routing protocol, Mayfly water wave optimization, Rivest-shamir adleman

Introduction

The WSNs is now a high-profile research subject due to their potential for widespread application and incorporation of several technologies, including sensing, wireless communication, and computation in communication, microelectronics, databases, networks, etc.[1] A protected restriction conspires given trust evaluation for WSNs utilizing block chain innovation including utilizing a decentralized record to guarantee the uprightness and reliability of sensor hub estimations. This strategy empowers secure and exact restriction by confirming the tactile information through agreement instruments and approving the reliability of taking an interesting hub, consequently alleviating possible assaults and guaranteeing dependable limitation results.[2] The utilization of block chain technology to improve the security of WSNs by distinguishing and mitigating malicious attacks is a promising approach that offers enhanced resilience and integrity to network communication and data transmission. The block chain takes into account straightforward and unchanging records of information trades inside the organization, empowering the recognizable proof of any strange or unapproved exercises. By utilizing the decentralized idea of block chain, this plan gives a energetic and reliable answer for upgrading the general security of WSNs.[3] This approach ensures optimized storage by eliminating the need for a central database and distributing data across multiple nodes in the network. It provides secure and efficient storage, enhancing the performance and scalability of IoT systems. Using Block chain technology, signature, voting detection, and heuristic approaches are employed to determine the best medications for spotting criminal activity and security risks.[4]

The integration of block chain and biometrics in a WSN allows for secure and efficient library management. Block chain technology ensures transparency, immutability, and data morality, enabling reliable tracking of book borrowing and returning.[5] Biometric authentication adds an extra layer of security by using unique physical characteristics to verify users' identities accurately. Distributed safety measures are preferred to centralised ones because centralized systems are prone to single-point failure.[6]

*Author for Correspondence
E-mail: shivaprasadmore@gmail.com

The block chain-enabled energy-efficient Red Deer algorithm leverages clustering protocol to enhance the performance of pervasive WSNs. It utilizes block chain technology to ensure secure and transparent data transfer, reducing energy consumption and prolonging the lifespan of sensors. This protocol improves the overall efficiency and dependability of the network, enabling seamless communication and data gathering across the Sensor Nodes (SN).[7] A block chain based protected pattern for sensor data in WSNs utilizes block chain technology to ensure the integrity, confidentiality, and reliability of sensor data. It enables decentralized storage and tamper-proofing of sensor data, safeguarding against unauthorized access or tampering. This model leverages the transparency and immutability features of block chain to enhance the security and trustworthiness of sensor data in WSNs.[8]

Trust management has recently been a widely applied method of ensuring the safety of the routing network. The fundamental strategy for every node is to exploit and maintain a trust model that keeps track of the trust levels of the nearby routing nodes and decides on routing. This technique can successfully influence the routing node to select comparatively reliable routing links centered on the belief values.[9] A hybrid block chain based identity authentication scheme for multi-WSN. The scheme combines the benefits of block chain technology with the security of identity authentication in multi-WSN environments. It provides a secure and decentralized solution for verifying the identity of nodes in the network.[10]

Block chain Mechanism in a WSN is a decentralized and transparent system that confirms data integrity and security by storing and verifying the sensor data across multiple nodes. Symmetric Encryption is a kind of encryption algorithm used to secure the communication between sensors and the network by utilizing a shared secret key for both encryption and decryption, providing efficient and secure data transmission.[11] Block chain Secure Range-Free Localization in WSNs refers to a method that uses block chain technology to ensure secure and accurate localization in WSNs, the absence of the need for range information. It eliminates the necessity for distance measurements between the nodes, improving efficiency while maintaining security. This approach harnesses the benefits of block chain, such as transparency, immutability, and decentralized control to enhance localization algorithms in WSNs.[12] Block chain innovation can upgrade WSNs by giving secure information encryption and verification, guaranteeing the trustworthiness of gathered sensor information. Block chain can enable trust less data sharing and secure tamper-proof communication between vehicles in Vehicular Ad Hoc Networks (VANets) with the IoT frameworks. In medical services, block chain can work with secure and productive sharing of clinical records, guaranteeing protection and further developing interoperability between various medical services suppliers.[13] A genuine IoT node connects to another appropriate IoT node, some of which may be malicious. This can cause network blocking and prevent some IoT devices from accessing some data streaming, which may have an impact on how IoT devices are authenticated.[14] The attackers are consequently in charge of an important amount of IoT devices that are all outfitted with the most recent block chain technology, in contrast to centralized systems. It can be deduced that Denial of Services (DoS) attacks are exceedingly challenging to carry out via a peer-to-peer network without affecting the block chain security and the entire network due to a great amount of IoT devices.[15] The WSNs have appeared as a powerful technology for collecting and monitoring data from various environments. There are several challenges to be addressed to develop an efficient security mechanism utilizing block chain technology in WSNs. The problem highlights the lack of a trusted network infrastructure in WSNs and the potential of block chain technology to address this. Further research and development efforts are needed to design an efficient security mechanism that leverages the benefits of block chain while addressing the challenges specific to WSNs.

Literature Survey

The WSNs are prone to security threats due to their open nature. To ensure a trusted network, an efficient security mechanism using block chain technology can be implemented. A hybrid deep learning work built on block chain and metaheuristics was designed by Revanesh *et al.*[16] Block chain technology is applied to manage the discrete routing evidence of the network, while Salp swarm intelligence is exploited to find the best route. To understand the variations between the network's nodes, the convolution neural network is also included. Ramasamy *et al.*[17] explored current Block chain Technology (BT) developments with a particular emphasis on recent research on Block chain-based WSNs (BWSNs). A detached ledger with confirmed and inviolate transaction data is one of its

important points about block chain technology. It concludes with important takeaways on data distribution, storage needs, malicious node identification, and data security for block chain-based applications in networks and IoTs.

Mubarakali *et al.*[18] proposed a block chain network utilized in the security system, although safety measures are quite in the testing stage. The research focused on stopping the attacks, Hierarchical Block Chains (HBC) and WSN for cluster-based were deployed. However, it has limitations because, for sensor nodes (SN) that is circulated randomly, the task is not appropriate. Also, in WSN, fixed and HBCs were built that are only capable of scalability and dependability. Awan *et al.*[19] have developed a trust and encryption assessment approach using a block chain to record the individualities of the Aggregator Nodes (ANs) and SNs. It has both private and public block chains for executing AN and SN authentication.

Chen *et al.*[20] proposed a worm detection method using WSNs empowered by block chain technology. The SN in the local network was verified by each sink node, and the identification information was then securely stored on the block chain. It has limitations e.g., the use of block chain based verification in WSN has certain technological constraints. Furthermore, BT is motionless in its beginning and can present additional issues and difficulties when applied with WSN.

Javaid *et al.*[21] proposed an effective and secure trust model using block chain for wireless sensor IoTs. It offers a routing protocol utilizing the "Dijkstra algorithm" and the "Euclidean distance formula" to determine the shortest path. The trust mechanism upholds WSIoT's security. Hence, the network's nodes will interact safely with the Proof of Authority (PoA) process and requires additional computations that degrade network performance. The Worldwide Standard for the Internet of Things (WSIoTs) employ Inter Planetary File System (IPFS) for dependable and affordable storage.

To discuss the safety and energy needs of IoT devices, Ahmed *et al.*[22] developed an energy-efficient, secure, and data-aggregated architecture that offers a cloud-based system employing block chain technology. The study utilized data correlation reduction and BT to safeguard IoT networks against fraudulent activity. The performance evaluation findings unmistakably demonstrate the strategy, which uses BT to offload the cloud server as more energy efficient. The model is efficient and effective and it swiftly adheres to the key design principles. Hrovatin *et al.*[23] provided a novel block chain-onion routing combination that enables decentralized privacy-preserving data mining across WSNs. This method has the benefit of avoiding issues like only one point of failure and dependence on distant infrastructures, while producing findings that are qualitatively comparable to those produced by conventional data mining approaches.

Rajhi *et al.*[24] proposed a WSN security improvement for sensor data transmission in the block chain. The findings of the study sum up the fact that Merkel-tree algorithm approaches employed in block chain systems would be crucial for implementing data security in WSNs. The "Merkel-Tree algorithms" for cryptography and creating the hash function with the aid of compression functions, the research will guarantee the safety of WSNs. Sangeetha *et al.*[25] proposed the validation of block chain transactions in WSNs using dense neural networks. However, implementing block chain in WSNs poses challenges in terms of computational power and resource constraints, as the distributed nature of block chain transactions and the consensus mechanism require significant energy consumption and may strain the limited resources available in WSN nodes. Yang *et al.*[26] enhanced the robustness and performance of Permanent Magnet Synchronous Motors (PMSM) predictive control systems by accurately compensating for distorted motor parameters. The results showed that the compensated system exhibited better dynamic and static performance when dealing with single or multiple parameter distortions compared to the conventional PMSM predictive control model. This research investigates the potential of dense neural networks as an efficient method for validating blockchain transactions in Wireless Sensor Networks (WSNs). Unlike traditional blockchain networks, WSNs employing Proof of Work (PoW) face significant challenges due to inherent limitations in processing power, memory, and battery life of sensor nodes.

Proposed Research Methodology

Any unattended environment may be applied to create WSNs. Authorized users present have access to dependable SN with appreciation for recent developments in IoT technology.

Ensuring robust security in WSN is paramount, as depicted in Fig. 1. The integration of block chain technology emerges as an efficient mechanism to achieve this goal. The proposed experimental setup

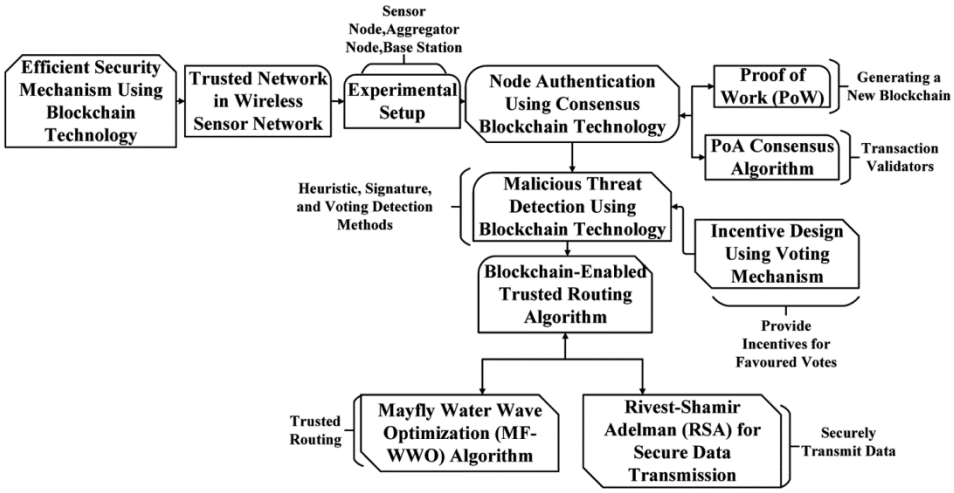

Fig. 1 — Flow diagram of the proposed work

involves sensor nodes, aggregator nodes, and a base station, forming a trusted network. Node authentication is achieved through consensus block chain technology, employing Proof of Work (PoW) for generating a new block chain and the Proof of Authority (PoA) consensus algorithm for transaction validation. This dual-layer authentication approach enhances the overall network integrity. Furthermore, the system employs heuristic, signature, and voting detection methods for malicious threat detection, bolstering the network's resilience against potential attacks. The incorporation of a block chain-enabled trusted routing algorithm, specifically the Mayfly Water Wave Optimization (MF-WWO) algorithm, ensures secure and efficient data transmission. Rivest-Shamir Adelman (RSA) is employed for encrypting and securing data during transmission, adding a layer of protection.

Experimental Setup

In a WSN experimentation setup, the infrastructure typically consists of SN, aggregator nodes, and base stations, each playing crucial roles in data collection and transmission. SN are distributed across the environment to capture relevant data, serving as the network's eyes and ears. These nodes are equipped with sensors to monitor physical parameters and transmit the gathered information to ANs strategically placed in the vicinity. Aggregator nodes collect, process, and summarise data from multiple SNs, reducing redundancy and conserving energy in the process. Finally, the aggregated data is transmitted to the base station, which serves as the central hub for more analysis and decision-making. The capability of

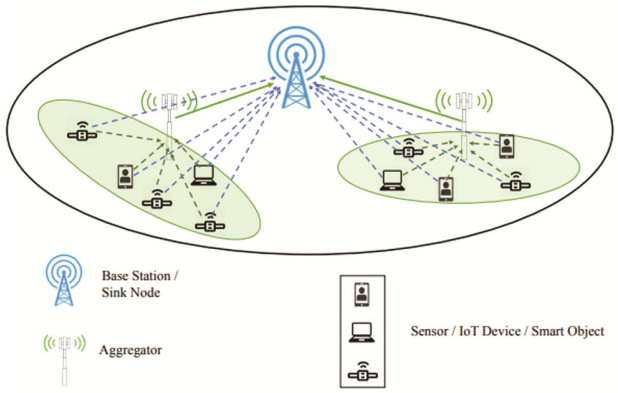

Fig. 2 — Architecture system scheme of WSN

the WSN heavily relies on the seamless coordination and communication among these components, ensuring efficient and reliable data transfer in diverse environmental conditions. Experimentation setups involving WSNs aim to optimize the network's performance, considering factors such as energy efficiency, data accuracy, and overall reliability.

In the illustrated architecture of a WSN as presented in Fig. 2, the base layer comprises SNs responsible for gathering environmental data. Subsequently, these data are transmitted to aggregator nodes for further processing. These ANs employ symmetric encryption algorithms to secure the data before relaying it to the block chain-enabled base stations. The base stations, acting as nodes in the block chain network, validate, timestamp, and store the encrypted data in a decentralized ledger. Block chain ensures data integrity, transparency, and traceability. Additionally, symmetric encryption techniques safeguard the confidentiality of sensitive

Table 1 — Communication and processing characteristics of network nodes

Node Type	ID	Quantity	Communication Protocol
Sensor Node	SNID	20	Data Transmission Rate
Aggregator Node	ANID	5	Transmission Range
Base Station	BSID	1	Processing Capacity

information during transmission. The base station acts as the ultimate destination for the aggregated data, facilitating decision-making processes based on the comprehensive information received from the SN through the aggregator nodes. This collaborative architecture enhances the overall efficiency, reliability, and energy conservation of the WSN.

In Table 1, the structure of the WSN is outlined, comprising three distinct types of nodes, each assigned specific roles aimed at enhancing the efficiency of data transmission and processing. The Sensor Nodes Identification (SNID), totalling 20 in number, are designed for data transmission, forming the foundation of the network. These nodes operate based on a specific communication protocol, ensuring seamless and standardized communication within the network. The Aggregator Nodes Identification (ANID), comprising 5 units, play a pivotal role in consolidating and managing data from several sensor nodes. Their communication protocol is tailored to optimize the transmission range, enabling effective aggregation of information. The network is anchored by a single Base Station (BSID) with high processing capacity, serving as the central hub for data analysis and decision-making. Each node type is equipped with its unique identification (ID) and is configured to operate within specified parameters, creating a well-organized and collaborative wireless sensor network.

Data Storage

The block chain's high storage costs make it impractical for extensive data storage, but its decentralized ledger system offers benefits. Each entity's transaction is recorded in a shared ledger accessible to all network participants. This ledger forms the network's foundation, and real-time updates occur across all entities after each transaction. This ensures security, as attempted alterations by rogue nodes are easily identified. Block chain Technology (BT), provides decentralized, authenticated, and synchronized transaction ledger maintenance. Its widespread use in healthcare, smart cities, finance, and transportation underscores its value in securing diverse sectors. Block chain addresses identity verification challenges for the Mobile Terminal System (MTS), leveraging decentralization, trust, and data encryption.

Node Authentication Using Consensus Block chain Technology

The verification of ANs and SNs uses both public and private block chains. There can only be one cluster network for each SN. Following that, the SNs disseminate the registration request message (SNID, ANID, and BSID). The registering event in the personal block chain initiates the smart contract set up for the SNs' registration procedure. This concept employs two different kinds of block chains to lessen the stress placed on ANs. The ANs perish in the earliest rounds of the prior authentication process since they are in charge of authenticating and registering other ANs. Although BSs, which have influential computational abilities, register and authenticate ANs in suggested architecture, ANs' workload is lightened in this way. As a finding, the suggested model's computational burden is reduced by the coexistence of both block chains.

The Consensus Mechanism (CM) in a block chain network establishes guidelines for uniform adherence. This protocol mandates participant permission for transactions on the decentralized ledger. In a public block chain, decentralized authority necessitates user consensus to validate network activity, ensuring reliability, safety, and effectiveness in online transactions. Various consensus frameworks exist, each adhering to specific standards, and addressing concerns in secure digital transactions. The following list outlines consensus techniques vital for the effective functioning of this model.

- Private block chains use the PoA consensus algorithm for block adding and transaction validation.
- The public block chain uses the PoW consensus algorithm to add blocks to the leader and confirm dealings.

PoA Consensus Algorithm

The Proof of Authority (PoA) consensus protocol selects transaction validators based on their network "reputation," making it suitable for private block chains. Participants unanimously follow PoA to uphold transaction records, especially advantageous for its applicability to private networks. The protocol fortifies user identities, as high-reputation nodes are

chosen for transaction validation, restricting authentication to trusted entities. This promotes a secure environment, encouraging users to safeguard their reputations and discouraging illicit activities. VeChain's PoA algorithm, chosen for the Decision Block chain, ensures rapid block formation every second, a feature extensively detailed on the VeChain Foundation's official website. Time stamped with t_0 is the genesis block. Any block with height $n > 0$ at the time t_n will have a date and time stamp that matches the requirements below:

$$t_n = t_0 + m \cdot \Delta \quad \text{... (1)}$$

where, t_0 is the time at which the primary block is proposed, m represents the position of the block in the block chain and Δ is a fixed time interval.

$$\gamma(n,t) = DPRP(n,t) = hash(n \cdot t) \quad \text{... (2)}$$

where, concatenating two-byte arrays is the operation. VeChainThor generates the block $B(n,t)$, with height n and timestamp t, using a Deterministic Pseudo-Random Process (DPRP) and the idea of "active/inactive" status if a controlling node is a viable option t using this method of a pseudo-random number γ (n,t). Out of two sincere branches, the one chosen by the legitimate branch validation method becomes the trunk. The "longest chain" rule is invalid for there is no computing opposition in PoA. The VeChain Block chain PoA algorithm's substitute for this, which is regarded as superior to the two, is choosing the branch with the greatest number of DA witnesses.

$$\pi_{B(n,t)} = \pi_{PA(B(n,t))} + \left\|A_{B(n,t)}\right\| \quad \text{... (3)}$$

where, $\left\|A_{B(n,t)}\right\|$ computes the number of master nodes that may be present in connection with $B(n,t)$ and may be observed as the number of nodes that observed $B(n,t)$. In conclusion, the bra, the branch with the highest AWN is selected as the trunk, and if both branches have the same AWN, the VeChain Block chain selects the division with the shorter length.

Proof of Work (PoW)

In the procedure of generating a new block for the block chain network, all nodes collaborate to determine the nonce field value, crucial for a valid block hash. Each block chain, such as Bitcoin, imposes specific hash pattern requirements; for example, starting with four or five zeros. Block data, immutable transactional information, necessitates miners to adjust the hash pattern. Imagine a bunch of computers (network nodes) in a competition. They're all trying to solve a complex math puzzle (finding the optimal nonce). This puzzle has a specific requirement (i.e) the answer (hash) needs to start with a certain number of zeros (required zeros). Once a node identifies the correct nonce, it is shared for verification. If everything checks out, a new block containing the transactions is added to the block chain, like adding a new page to a giant public ledger. This completes the transaction process. The computers that solved the puzzle and helped verify everything (consensus-forming nodes or miners) get rewarded for their work.

Malicious Threat Detection Using Block chain Technology

Sensitive data circulates across transceivers, smart devices, and SN in WSNs, making them susceptible to cyber threats. Addressing security challenges, this study proposes a robust solution utilizing Block chain technology. Employing heuristic, signature, and voting detection methods, the system identifies and mitigates security threats. For malware detection, heuristic analysis is initiated when a user assigns an executable file. A Malware Detection System (MDS) on the block chain checks for signatures, assesses maliciousness, and removes the downloaded file accordingly.

Malware detection employs a heuristic approach, analyzing the behaviour of executable files upon user transfer. The user's computer checks the File Hash Value (FHV) against the block chain for potential malice. The elimination decision formula determines whether to erase the file based on the FHV's presence and the severity indicated by the block chain. To put it another way, the file is erased when Eq. (2) is satisfied but not when Eq. (4) is satisfied.

$$M_d \leq M_t \quad \text{… (4)}$$

$$M_d > M_t \quad \text{… (5)}$$

$$0 \leq M_d \leq 1 \quad \text{… (6)}$$

where, M_d refers to the maximum quantity of transactions processed within a particular period.

M_t refers to the total No. of transactions that are shown in a particular period.

Case 1: $V_m + V_b \geq V_t$

The user's system solely utilizes the block chain voting results to determine the stage of malice.

$$M_d = \frac{V_m}{V_m+V_b} \quad \dots (7)$$

where, V_m represents the matrix of user access permissions.

V_b stands represent the integrity and transparency of the block chain.

V_t represents the transaction antiquity of the block chain.

The ability to vote is centralized in traditional voting systems. No one is aware of how to validate that document, so if someone demands to alter or change it, they can do it swiftly. Since the data are kept among numerous nodes, there is no one point of authority. As an outcome, it is impossible to do away with the votes and effectively tally them with other nodes.

Case 2:$V_m + V_b < V_t$

The user's system determines the degree of maliciousness using Eq. (8), the outcomes of block chain voting, and its results for malware detection using heuristic-based techniques. In this case, it is presumed that the MDS produces 1 when the file is malicious and 0 when it is benign, or $D_r \epsilon \{0,1\}$.

$$M_d = \frac{V_m}{V_m+V_b} \times D_r \times R_s \quad \dots (8)$$

where, R_v is a reputation value and R_s is a reputation score that is distinct by the subsequent expressions:

$$R_v = \frac{V_m+V_b}{V_t} \quad \dots (9)$$

$$R_s = 1 - R_v \quad \dots (10)$$

To prevent multiple votes from the same address, user addresses casting ballots are documented on the block chain. However, this safeguard alone is insufficient, as users can create unlimited addresses. Addressing this, a web server, developed with reputable institutions, registers voting addresses and restricts eligible addresses. The server connects to Ethereum's Register smart contract, registering the address. The user then joins the network, gathers signatures, and casts votes. The Vote smart contract checks the Register contract to verify the address. If valid, actions proceed; otherwise, they are rejected. The web server prevents consecutive address registration from similar IPs and uses CAPTCHA to deter bots and malicious users, ensuring a secure voting process.

Incentive Design using Voting Mechanism

To increase user voting incentives for the favoured votes are provided. Voting for a guessed FHV requires a little charge after the user. In this study, set the charge to 0 (i.e., set the gas value to 0), notwithstanding the user's message indicating an execution fee (or "Gas" in Ethereum) is necessary to vote. The voting fees are dispersed among the R_v for each suspected FHV using the Vote smart contract. It inevitably refer to the votes, since the detection result with the furthest votes is the dominating vote and the result with the fewest votes is the inferior vote in this instance. Only users who cast the majority of votes for each R_v are given the voting costs. Voters who cast unsatisfactory votes do not receive their voting costs back. Let's say that there are dominant votes as DV and inferior votes as IV. The following equations are worn to calculate the voting fee $fDIST$ to be dispersed:

$$fDIST = \frac{f_v+R_v}{DV}(for\ dominant\ votes) \quad \dots (11)$$

$$fDIST = 0\ (for\ Inferior\ Votes) \quad \dots (12)$$

$$DV > IV, DV + IV = R_v \quad \dots (13)$$

The previously mentioned reward scheme will encourage users to vote frequently and accurately. As important, the heuristic and voting technique improves the accuracy of finding and eliminating malware.

Block chain-Enabled Trusted Routing Algorithm

The Monitoring Node (MN) is detached from the network by computing the reliance values of SNs. Secure network routing is carried out while taking the sensor node's remaining energy and conviction values into account. This research introduces a new method for secure data transfer in Wireless Sensor Networks (WSNs) that utilizes both clustering and blockchain technology. The method focuses on selecting the most reliable sensor node (called the Cluster Head) within each cluster. By leveraging blockchain, the system ensures trust and security throughout the data transfer process. To safeguard the data as it passes across multiple nodes, blocks are formed at each level. The Mayfly Water Wave Optimisation (MF-WWO) method is employed for precise CH selection. Asymmetric keys-providing cryptosystem Rivest-Shamir Adleman (RSA) is also utilized to secure data transfer.

Mayfly Water Wave Optimization (MF-WWO) Algorithm

The provision of a trusted routing environment is a crucial and challenging problem for WSNs. In WSN routing networks, it is challenging to use dynamic

routing information effectively. For such adaptive routing networks, a self-adaptive routing algorithm is required to increase the routing scheme's capacity for self-adaptation. This article suggests a unique cluster-based secure routing strategy to address the routing and data security issues to get over these obstacles. Using the Improved Mayfly Water Wave Optimization (MF-WWO) algorithm, the best CH is chosen in this scheme constructed on residual energy, online time, reputation, block chain transactions, mobility, and connection.

The Mayfly Algorithm (MA) is a recent bio-inspired population-based method effective in solving diverse engineering problems. Drawing inspiration from mayflies' flight and mating behaviors, MA combines evolutionary algorithms and swarm intelligence, providing a balance between exploitation and exploration. However, its multiple options make parameter selection challenging. This approach identifies the optimal route based on fitness values for distance and time efficiency.

Shallow water wave models serve as an inspiration for the WWO's approach to problem-solving. Imagine being faced with a maximization issue with objective function f without losing generality. The efficient position is calculated using the Eq. (14) by taking the candidate's current position into account with an equal step.

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad \ldots (14)$$

where, $x_i(0)$ is limited between x_{min} and x_{max}. The movement of mayflies on the top of the water to dance is mathematically modeled as follows:

$$v_{ij}(t+1) = v_{ij}(t) + a_1 \times exp\left(-\beta r_g^2\right) \times \left(pbest_{ij} - x_{ij}^t\right) + a_2 \times exp\left(-\beta r_g^2\right) \times \left(gbest_j - xijt, j=1,2,\cdots,n\right. \quad \ldots (15)$$

where, The Equation Defines defines the i^{th} best position candidate had ever visited; $r_p$and r_g describe the Cartesian distance between x_i and $pbest_i$ and x_i and $gbest$; x_{ij}^t and $v_{ij}(t)$ represent the position and the velocity of the i^{th} candidate in measurement j, respectively; and a_1 and a_2 signify where [positive magnetism] coefficients determine the influence of the candidate's social interactions and past experiences (cognitive following) on the calculation. This combined analysis helps identify the ideal position for an individual to succeed at a specific time step $+1$:

This equation aims to identify the optimal position for an individual to achieve success at a given time step (t). Here's how it works:

It considers the "best position" the candidate has encountered previously (based on past experiences).

It calculates the distance between the candidate's current position and other potential locations.

The candidate's current position and movement are factored in using their position and velocity data.

Social and past experiences (cognitive history) are also considered, with varying importance determined by "positive magnetism" coefficients.

By combining these factors, the equation aims to predict the ideal position for the individual's success at a specific point in time:

$$pbest_i = \begin{cases} x_i(t+1), if\ f\left(x_i(t+1)\right) < f(pbest_i) \\ is\ kept\ the\ same, O.W \end{cases} \quad \ldots (16)$$

where, $f(\cdot)$ represents the objective function employed to gauge the solution's quality. Then, the following $gbest_j$ is done to reach the global finest position:

$$gbest = min\{f(pbest_1), f(pbest_2), \cdots, f(pbest_N)\} \quad \ldots (17)$$

The choice of a CH is observed as among the most crucial responsibilities for clustering in a WSN since a CH transmits data to other CHs and routes data from Cluster Members (CM). To calculate the suggested fitness function, the following group of objectives is taken into account:

Residual Energy: Equation 18's description of residual energy refers to the entire remaining energy of the UAV.

$$E_r = E_t - E_c + E_{pr} + E_{ps} \quad \ldots (18)$$

where, E_r is the current residual energy, E_t stands for the total beginning energy. According to the block chain, E_c, E_{pr}, and E_{ps} represent the energy required to process one block, respectively. The CH oversees intra- and inter-cluster communication in the suggested design. Because low residual energy frequently results in dead nodes and shortens the lifecycle of the entire network, CH's residual energy is therefore critical.

Reputation Ranking: The reputation rating is based on transmitted, dropped, and received packets, preventing the choice of a corrupted network as a CH. It aims to offer a reliable method for customers to

choose the most dependable server node. Clients elect a reputable server, communicate, assess the service, and provide a satisfaction rating. Subsequently, the server is rewarded or punished based on satisfaction, impacting its reputation.

$$Q(S_k) = \frac{\overline{\tau_k}}{Length(S_k)^{PLF}} . \%W_k \quad \ldots (19)$$

$Q(S_k)$ describes the excellence of the path S_k ; $\overline{\tau_k}$ entitles the regular trail pheromone of path S_k originate by ant k; PLF ∈ [0, 1] explain a path length influence and $. \%W_k$ represent the percentage of propagation that has designated a similar solution as position k.

The flowchart for the Mayfly Water Wave Optimization (MF-WWO) algorithm is given in Fig. 3 which highlights the sequence of steps involved in executing the algorithm. The process is initiated by creating a population of agent vectors, each representing a probable solution to the optimization problem. In an iterative loop, the algorithm assesses the fitness of these vectors based on their adherence to the optimization objective. Elite agents, exhibiting the highest fitness, undergo perturbation to create new candidate solutions. Comparative fitness evaluation between the candidates and elite agents results in the replacement of lower-performing agents. The algorithm continually refines solutions through local searches, aiming for improved fitness. Termination conditions, such as reaching a maximum iteration limit or finding a satisfactory solution, conclude the process. The algorithm provides the best solution—an elite agent with the highest fitness serving as the optimal solution for further analysis or decision-making.

Rivest-Shamir Adelman (RSA) For Secure Data Transmission

The proposed work employs the RSA mechanism to securely transmit data over the network. The RSA, an uneven key encryption method, utilizes two different keys for decryption and data encryption, enhancing security compared to standard RSA calculations. This enhanced RSA computation offers improved defence against potential attacks, with key generation, encoding, and decoding occurring across three stages.

Data that has to be transferred is encrypted applying the private key after creating the open key. The process for encryption and encryption-decryption is as follows:

- The condition $C^{'} = M^{e}$ and $n^{'}$, M is the primary message, leading to the discovery of the figure content C.

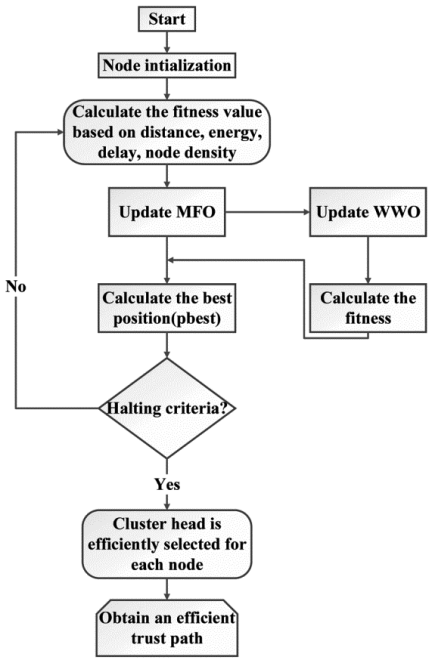

Fig. 3 — Flowchart of MF-WWO Algorithm

Table 2 — Pseudocode of Rivest-Shamir Adelman (RSA)

Algorithm 1: RSA Algorithm

1. Input: Initialize the value of p and q
2. Output: Public key <e, n> and Private key <d, n>
3. Procedure:
4. Select two large prime numbers, p and q.
5. Calculate n as the product of p and q as $(n = p \times q)$.
6. Calculate $\varphi\ (n)$ as (p - 1) x (q - 1).
7. Choose a number e such that $1 < e < \varphi\ (n)$ and gcd $(e, \varphi\ (n)) = 1$.
8. Set the public key as <e, n>using the cypher text C.
9. Calculate D as the modular augmentative inverse of e modulo φ (n) (i.e., D is the solution to $D_e mod\ \varphi\ (n) = 1$).
10. Set the private key as <d, n> to get plain text,$m = c^d mod\ n$
11. Return the public key and private key.

- The condition $M^{'} = C^{d} mod\ n^{'}$may be applied to determine the message M from the content of Figure C.
- The private key needs to be operated to decrypt any content encoded with the open key

The pseudo code of the proposed technique is illustrated in Table 2. This procedure outlines the steps to generate a Public Key (PK) and private key pair for decryption and encryption. The input involves initializing the values of p and q, which are two huge prime numbers. First, the product of p and q is calculated to determine the value of n. Then, the value of $\varphi\ (n)$ is calculated as (p − 1) × (q − 1). Following, a number e is chosen such that it is greater than 1 and less

than $\varphi\ (n)$, and its greatest common divisor with $\varphi\ (n)$ is 1. This ensures that e is comparatively prime to $\varphi\ (n)$. The PK is then set as <e, n>, which is utilized for encryption. This means that d is the resolution to the equation $D_e mod\ \varphi\ (n) = 1)$. In conclusion, the private key is set as <d, n>. This private key is utilized for decryption, where the cypher text is transformed to plaintext using $m = c^d mod\ n$, where c represents the cypher text. The output of this procedure is the set of private key <d, n> and public key <e, n>.

Application of the Proposed Method

The Internet of Things (IoT) is constantly evolving, and recent advancements highlight the critical need for authorized users to access reliable sensor nodes (SNs) while considering resource limitations. This proposal combines data transfer and blockchain technology to create a highly secure node recognition system for Wireless Sensor Networks (WSNs). A recent development in IoT technology realized the significance of authorized users having access to reliable SN while also considering the limitations of their resources. In leveraging the potential of block chain-based technologies to enhance the capabilities of WSNs, through a combination of data transfer and block chain, build a node recognition system that offers an extraordinary level of security for WSNs. By utilizing a blockchain-based ledger of transactions, we can establish a secure and tamper-proof record of sensor data. This data can then be integrated into a sensor data database, creating a robust and dependable foundation for WSN infrastructure. This approach overcomes a major challenge in conventional WSNs – the vulnerability of nodes to failure. The success of this proposed method would be significantly bolstered by the combination of my unique perspective on blockchain and WSN technologies, along with my expertise in secure verification mechanisms and node identity authentication. This data can then be integrated into a sensor data database, creating a robust and dependable foundation for WSN infrastructure. The proposed method's parameters in details provided in Table 3

Table 3 — Parameter analysis of the suggested work

Parameter	Description
M_d	Maximum no of transactions in the period
M_t	Total no of transactions in the period
Δ	Time interval
t_o	Time is taken in the block chain
V_m	Matrix of user access permissions
V_b	The integrity and transparency of the block chain
V_t	Transaction history of the block chain
R_v	Reputation value
R_s	Reputation score
E_r	Current residual energy

Table 4 — Simulation system configuration

MATLAB	Version R2021a
Operation System	Windows 10 Home
Memory Capacity	6GB DDR3
Processor	Intel Core i5 @ 3.5GHz
Simulation Time	10.190 seconds

Results and Discussion

This section talks about simulating the suggested model and evaluating it. A trust assessment mechanism is applied in the proposed model to discover the network's malicious SNs. In addition, an authentication method is proposed to safeguard the network against intrusions. Because the consequence of authentication cannot be directly witnessed, it is assessed and established based on network throughput, energy consumption, and longevity. The smart contract was also created using Solidity. With the custom of both PoW and PoA consensus approaches, the network as an entire is proved.

Simulation Setup

The Intel(R) Core(TM) i5-5200U CPU @ 3.5GHz, 6 GB RAM, and a 64-bit operating system are the stipulations for the simulation setup. SNs are immovable during the simulations. The model evaluation simulation configuration is provided in Table 4.

System Performance Metrics

Numerous monitoring and tracking applications are produced by the exponential rise of research in low-power electronics, pervasive smart sensors, and WSNs. Different standards for quality are essential to be met by these technologies.

The delay, a packet experiences while traveling from the basis to the receiving node is known as latency. A public block chain model called Ethereum was applied by several writers, generating a lag of 15,000 milliseconds, yet their IoT systems were able to hold it. With private block chain schemes, they had a latency of only 8000 ms.

The relationship between scheduling delays is displayed in Fig. 4. The delay grows as the effective communication distance increases under the same network node density. Consequently, more nodes are vying for the identical interval slot, increasing competition. Given that the delay time of EQSHC is

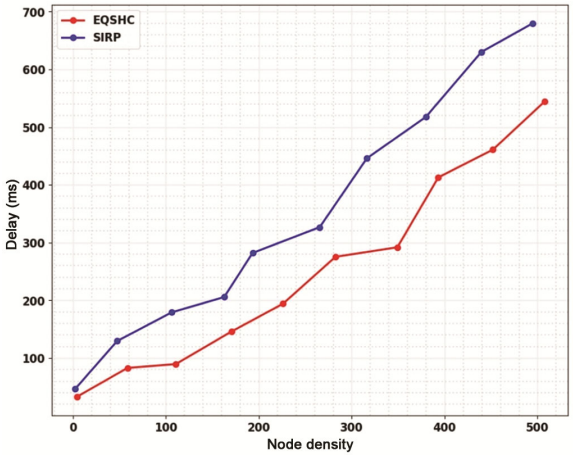

Fig. 4 — Performance analysis of delay with node density

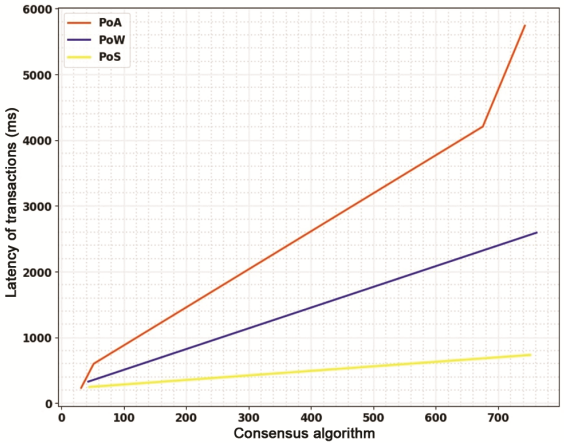

Fig. 5 — Latency transactions on different block chain

700 ms and SIRP is 550 ms, EQSHC has a higher delay than SIRP. The scheduling delay also increases when node density rises and the communication distance remains constant. Efficiency should also be considered alongside delay to assess the overall effectiveness of EQSHC and SIRP in different node density scenarios.

The experiment's results showing latency transactions on various block chain platforms as shown in Fig. 5 can vary depending on the consensus algorithm used. Proof of Authority (PoA) offers generally lower latency for transactions compared to Proof of Work (PoW) and Proof of Stake (PoS) systems. This is because PoA relies on a fixed set of trusted validators, leading to faster communication and validation processes lower compared to PoW and Proof of Stake (PoS) systems. PoA block chain systems rely on a predefined set of trusted validators who are accountable for verifying transactions. Similarly, in PoS systems, token holders (validators)

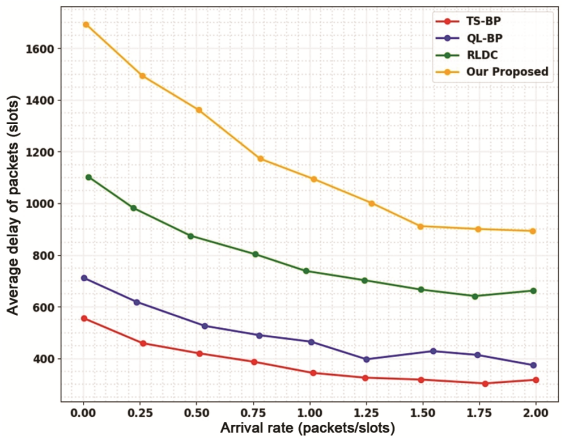

Fig. 6 — Average delay packets/slot

are designated to authorize transactions based on the number of tokens they have and the extent of time they have been holding them. In terms of routing data, PoA block chain solutions can be an effective and practical way to gather and handle route scheduling data. Overall, PoA block chain systems offer lower latency for token transactions compared to PoW and PoS systems.

The average packet latency for each algorithm is displayed in Fig. 6. The comparison studies were put into practice in a routing system with 50% hostile routing nodes. Both of the system's algorithms performed well even when a lot of malicious nodes MN were present. The suggested algorithm outperformed the (Q-Learning Backpressure Routing Algorithm) QL-BP algorithm, which it reduced by only about 32% while the QL-BP algorithm only decreased by about 37%, reducing average packet latency by about 81% compared to the RLDC algorithm's reduction of about 55%. This was because the QL-BP algorithm does not trust the queue length material released between routing nodes. The MNs can raise the parameter by sending out a falsely reduced queue length, considerably boosting the likelihood that the data packet will be routed to the malicious node and interfering with the normal routing scheduling function.

The nodes' lifetimes in the network are shown in Fig. 7. In terms of network longevity, the suggested block chain solution is contrasted with the options already available. The nodes perish at an early stage; for example, the initial node perishes in the 4500th round. However, at the 750th round, the 10th node perishes. Because these nodes use more energy and there is no mechanism for effective Cluster Head (CH) selection, the nodes in the (Particle Swarm

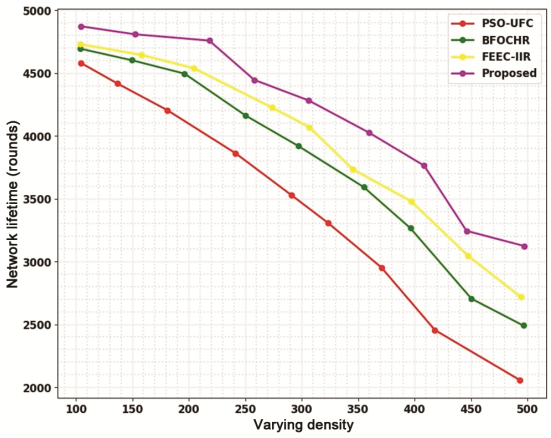

Fig. 7 — Network lifetime

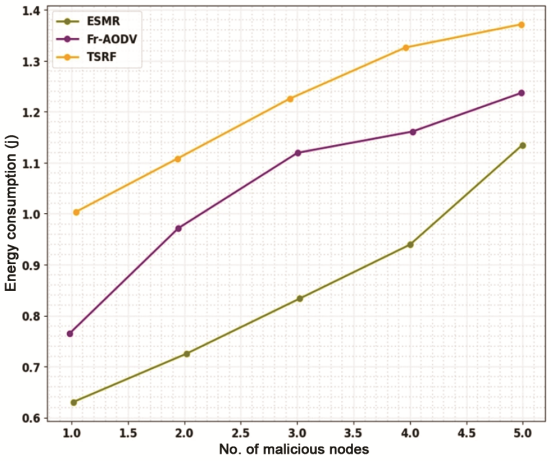

Fig. 8 — Energy consumption

Optimization-based Unequal and Fault Tolerant Clustering nodes in the Protocol) PSO-UFC fail early. As an outcome, random CH selection reduces network performance and renders the network inefficient. In the MF-WWO comparison, there are 5000 total rounds in the network nodes function. Early on, the first node's energy starts to run out. The 10^{th} node, however, expires after 3000 rounds.

Plenty of energy is applied as an importance of the attackers sending malicious packets to the aim location and Fig. 8 reaches its greatest when there are attackers on the network. Energy-Saving Multipath Routing (ESMR), Fault-Tolerant Ad hoc On-Demand Distance Vector Routing (FR-AODV), and Threshold Sensitive Routing Function (TSRF) are compared with the energy consumption with the value of No. of nodes. TSRF has a high value of number in malicious nodes with high energy consumption of 0.8–1.4 (*j*). The authorized nodes intersect the network after nodes have registered and been authenticated. This means that they utilize less energy than they would if

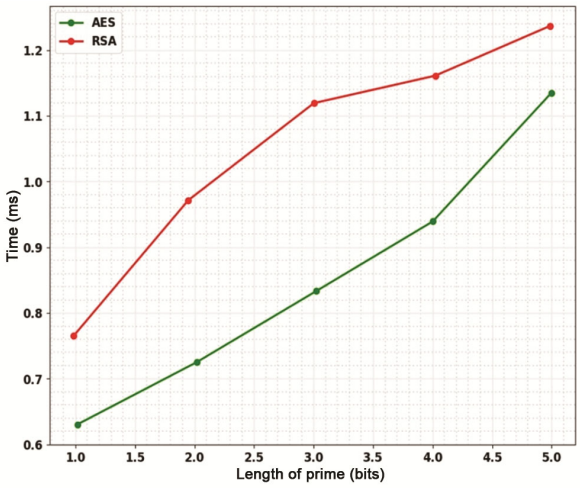

Fig. 9 — Encryption time comparison

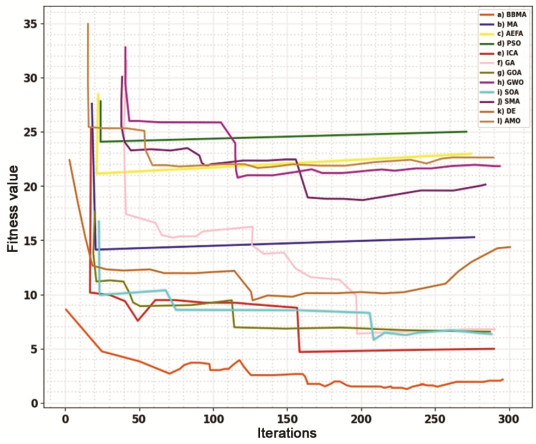

Fig. 10 — Convergence curves of the average fitness value

there were attackers around.

The encryption times of the proposed Modified RSA (MRSA) method versus RSA are compared in Fig. 9. Illustrations show the connection between the size (length) of the RSA key and the time it takes to compute the RSA algorithm. As the key size increases, the time vital for the algorithm also increases rapidly indicating that RSA is computationally intensive and time-consuming for larger key sizes.

These values indicate the effectiveness and accuracy of the solution in achieving the desired objectives. In Fig. 10, the intersection curves of Fitness values in fitness optimization algorithms are illustrated. Similarly, the (Artificial Ecosystem-Based Firefly Algorithm) AEFA algorithm has a fitness value of 92%, indicating the highest level of efficiency in optimizing fitness. The (Biogeography-Based Optimization with Migration) BBMA (89%), (Grey Wolf Optimizer) GW0 (90%), and (Sine Cosine Method) SMA (92%) algorithms also perform

Table 5 — Comparison of value in algorithm

Authors	Technique	Fitness values in%
Yang *et al.* 2024[26]	BBMA	89
Zhu *et al.* 2024[27]	MA	91
Karthikeyan *et al.* 2024[28]	AEFA	92
Luo *et al.* 2024[29]	PSO	97
Nguyen *et al.* 2024[30]	ICA	79
Babu *et al.* 2024[31]	GA	85
Wang *et al.* 2024[32]	GW0	90
Hien *et al.* 2024[33]	SOA	89
Cao *et al.* 2024[34]	SMA	92
Gu *et al.* 2024[35]	DE	82
Shwetha *et al.* 2024[36]	AMO	90
Okafor *et al.* 2024[37]	GSA	87

quite well, demonstrating their ability to generate solutions with high fitness values. The findings illustrated that the PSO algorithm has the highest fitness value of 97%. The PSO algorithm proves to be highly effective in optimizing fitness.

State of Art

Further comparing the given algorithms, PSO outperforms the other algorithm with an accuracy of fitness value 97%. It is illustrated in given table below

Fitness values in percentage for various optimization techniques are presented in Table 5. These include Bacterial Foraging Optimization (BBMA), Memetic Algorithm (MA), Adaptive Enriched Firefly Algorithm (AEFA), Imperialist Competitive Algorithm (ICA), Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Grey Wolf Optimizer (GWO), Sine Cosine Algorithm (SOA), Social Spider Algorithm (SMA), Differential Evolution (DE), Antlion Optimizer (AMO), and Gravitational Search Algorithm (GSA). These fitness values represent the effectiveness of each optimization technique in achieving optimal solutions for the given problem. Notably, PSO demonstrates the highest fitness value at 97%, indicating its superior performance compared to other optimization methods.

Conclusions

This study successfully implemented a blockchain-based node recognition system for Wireless Sensor Networks (WSNs). The proposed system leverages a modified blockchain transaction ledger to securely store sensor data, addressing the vulnerability of conventional WSNs to data alteration and fake identities. The findings demonstrate the effectiveness of the Particle Swarm Optimization (PSO) algorithm in cluster head selection, achieving a high fitness value of 97%. Additionally, the integration of the Rivest-Shamir Adleman (RSA) cryptosystem safeguards data transmission. However, current blockchain technologies can be resource-intensive. Future research should explore lightweight and energy-efficient blockchain protocols specifically designed for WSNs. Furthermore, integrating this approach with emerging technologies like the Internet of Things (IoT) and artificial intelligence (AI) has the potential to significantly enhance security and communication efficiency in future WSN deployments. Future research should explore lightweight and energy-efficient block chain protocols tailored for WSNs, considering potential integration with emerging technologies like IoT and artificial intelligence for enhanced security and communication efficiency.

References

1 Pradhan N R & Singh A P, Research issues of information security using block chain technique in multiple media WSNs: A communication technique perceptive, in *Smart Sensor Networks Using AI for Industry 4.0*, (2021) 65–76, CRC Press, https://doi.org/10.1201/9781003145028-4.

2 Goyat R, Kumar G, Alazab M, Saha R, Thomas R & Rai M K, A secure localization scheme based on trust assessment for WSNs using block chain technology, *Future Gener Comput Syst*, **125** (2021) 221–231, https://doi.org/ 10.1016/j.future. 2021.06.039.

3 Almaiah M A, A new scheme for detecting malicious attacks in wireless sensor networks based on block chain technology, In *Artificial Intelligence and Block chain for Future Cybersecurity Applications*, (Springer), (2021) 217–234, https://doi.org/10.1007/978-3-030-74575-2 12.

4 Khalaf O I & Abdulsahib G M, Optimized dynamic storage of data (odsd) in iot based on block chain for wireless sensor networks, *Peer Peer Netw Appl*, **14(5)** (2021) 2858–2873, https://doi.org/10.1007/s12083-021-01115-4.

5 Lazrag H, Chehri A, Saadane R & Rahmani M D, Efficient and secure routing protocol based on block chain approach for wireless sensor networks, *Concurr Comput: Pract Exp*, **33(22)** (2021) e6144, https://doi.org/10.1002/cpe.6144.

6 Fu M H, Integrated technologies of block chain and biometrics based on wireless sensor network for library management, *Inf Technol Libr*, **39(3)** (2020) https://doi.org/ 10.6017/ital.v39i3.11883.

7 Nguyen G N, Le Viet N H, Devaraj A F S, Gobi R & Shankar K, Block chain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks, *Sustain Comput*: *Sci J Inform*, **28** (2020) 100464, https://doi.org/10.1016/j.suscom.2020.100464.

8 Chanana R, Singh A K, Killa R, Agarwal S and Mehra P S, Block chain based secure model for sensor data in wireless sensor network, In 2020 6th International Conference on Signal Processing and Communication (ICSC) *IEEE*, (2020, March) 288–293, https://doi.org/10.1109/ICSC48311.2020. 9182776.

9 Yang J, He S, Xu Y, Chen L & Ren J, A trusted routing scheme using block chain and reinforcement learning for wireless sensor networks, *Sensors*, **19(4)** (2019) 970, https://doi.org/10.3390/s19040970.

10 Cui Z, Fei X U E, Zhang S, Cai X, Cao Y, Zhang W & Chen J, A hybrid block chain-based identity authentication scheme

for multi-wsn, *IEEE Trans Serv Comput*, **13(2)** (2020). 241–251, https://doi.org/10.1109/TSC.2020.2964537.

11 Guerrero-Sanchez A E, Rivas-Araiza E A, Gonzalez-Cordoba J L, Toledano-Ayala M & Takacs A, Block chain mechanism and symmetric encryption in a wireless sensor network, *Sensors*, **20(10)** (2020) 2798, https://doi.org/10.3390/s20102798.

12 Goyat R, Kumar G, Rai M K, Saha R, Thomas R & Kim T H, Block chain powered secure range-free localization in wireless sensor networks, *Arab J Sci Eng*, **45(8)** (2020) 6139–6155, https://doi.org/10.31127/tuje.1094375.

13 Tariq F, Anwar M, Janjua A R, Khan M H, Khan A U & Javaid N, Block chain in wsns, vanets, iots and healthcare: A survey, In workshops of the international conference on advanced information networking and applications, *Springer, Cham*, (2020, April) 267–279, https://doi.org/10.1007/978-3-030-44038-1_25.

14 Hong S, p2p networking based internet of things (iot) sensor node authentication by block chain, *Peer Peer Netw Appl*, **13(2)** (2020) 579–589, https://doi.org/10.1007/s12083-019-00739-x.

15 Manjula V & Thalapathi R R, Security vulnerabilities in traditional wireless sensor networks by an intern in iot, block chain technology for data sharing in iot, in principles of internet of things (iot) ecosystem: Insight paradigm, *Springer, Cham*, (2020) 579–597, https://doi.org/1007/978-3-030-33596-0 23.

16 Revanesh M & Sridhar V, A trusted distributed routing scheme for wireless sensor networks using block chain and meta-heuristics-based deep learning technique, *Trans Emerg Telecommun Technol*, **32(9)** (2021) e 4259, https://doi.org/10.1002/ett.4259.

17 Ramasamy L K, Khan K P F, Imoize A L, Ogbebor J O, Kadry S & Rho S, Block chain- for malicious node detection: A survey, *IEEE Access*, **9 (**2021) 128765–128785, https://doi.org/1109/ACCESS.2021.3111923.

18 Mubarakali A, An efficient authentication scheme using block chain technology for wireless sensor networks, *Wirel Pers Commun*, (2021) 1–15, https://doi.org/10.1007/s11277-021-08212-w.

19 Awan S, Javaid N, Ullah S, Khan A U, Qamar A M & Choi J G, Block chain based secure routing and trust management in wireless sensor networks, *Sensors*, **22(2)** (2021) 411, https://doi.org/10.3390/s22020411.

20 Chen Y, Yang X, Li T, Ren Y & Long Y, A block chain-empowered authentication scheme for worm detection in wireless sensor network, *Digit Commun Netw*, (2021) 04–007, https://doi.org/10.1016/j.dcan.

21 Javaid N & Mateen A, Corrections to a secure and efficient trust model for wireless sensor iots using block chain, *IEEE Access*, **10** (2021) 55888, https://doi.org/10.1109/ACCESS20213177085.

22 Ahmed A, Abdullah S, Bukhsh M, Ahmad I & Mushtaq Z, An energy-efficient data aggregation mechanism for iot secured by block chain, *IEEE Access*, **10** (2021) 11404–11419, https://doi.org/1109/ACCESS.2022.3146295.

23 Hrovatin N, Tošić A, Mrissa M & Kavšek B, Privacy-preserving data mining on block chain-based wsns, *Appl Sci*, **12(11)** (2021) 5646, https://doi.org/10.3390/ app12115646.

24 Rajhi M & Hakami A, A cryptographic iterative hash function scheme for wireless sensor network (WSNs) security enhancement for sensor data transmission in block chain, (2021) https://doi.org/10.36227/techrxiv.19323308.v2.

25 Sangeetha S B & Prasad K K, Validation of block chain transactions in wireless sensor networks using dense neural networks, **13(01)** (2022) https://doi.org/10.21917/ijct.(2021)0391.

26 Yang J, Shen Y & Tan Y, Parameter compensation for the predictive control system of a permanent magnet synchronous motor based on bacterial foraging optimization algorithm, *World Electr Veh J*, **15(1)** (2024) 23, https://doi.org/10.3390/wevj15010023.

27 Zhu N, Gong G, Lu D, Huang D, Peng N & Qi H, An effective reformative memetic algorithm for distributed flexible job-shop scheduling problem with order cancellation, *Expert Syst Appl*, **237** (2024) 121205, https://doi.org/10.1016/j.eswa.2020.113721.

28 Karthikeyan M, Manimegalai D & Raja Gopal K, Firefly algorithm based WSN-iot security enhancement with machine learning for intrusion detection, *Sci Rep*, **14(1)** (2024) 231, https://doi.org/10.1038/s41598-023-50554-x.

29 Luo X, Chen J, Yuan Y & Wang Z, Pseudo gradient-adjusted particle swarm optimization for accurate adaptive latent factor analysis, *IEEE Trans Syst Man Cybern*, **99**(2024) 1–14, https://doi.org/10.1109/TSMC.2023.3340919.

30 Nguyen H, Bui X N, Choi Y & Topal E, Application of artificial intelligence in predicting slope stability in open-pit mines: A case study with a novel imperialist competitive algorithm-based radial basis function neural network In *Applications of Artificial Intelligence in Mining*, *J Geotech Eng*, (2024) 97–111, https://doi.org/10.1016/B978-0-443-18764-3.00001-1.

31 Babu R M, Satamraju K P, Gangothri B N, Malarkodi B & Suresh C V, A hybrid model using genetic algorithm for energy optimization in heterogeneous internet of block chain things, *Telecom Rav Eng*, **83** (2024) 1, https://doi.org/1615/TelecomRadEng.2023050237.

32 Wang Y, Ran S & Wang G G, Role-oriented binary grey wolf optimizer using foraging-following and levy flight for feature selection, *Appl Math Model*, **126**, (2024) 310–326, https://doi.org/10.1016/j.apm.2023.08.043.

33 Hien C T, Duong M P & Pham L H, Skill optimization algorithm for solving optimal power flow problem, *Bull Electr Eng*, **13(1)** (2024) 12–19, https://doi.org/ 10.11591/eei.v13i1.5280.

34 Cao F, Feng Y, Wang S, Zhang G & Xing K, Deadlock control and hybrid social spider scheduling algorithm for two-stage assembly permutation flowshop with limited buffers, *Expert Syst Appl*, **245** (2024) 122744, https://doi.org/10.1016/j.eswa.2023.122744.

35 Gu Q, Li S & Liao Z, Solving nonlinear equation systems based on evolutionary multitasking with neighborhood-based speciation differential evolution, *Expert Syst Appl*, **238** (2024) 122025, https://doi.org/10.1016/j.eswa.2023.122025.

36 Shwetha G R & Murthy S V N, A combined approach based on antlion optimizer with particle swarm optimization for enhanced localization performance in wireless sensor networks, *J Adv Inf Technol*, **15(1)** (2024) https://doi.org/10.12720/jait.

37 Okafor K C, Adebisi B, Akande A O & Anoh K, Agile gravitational search algorithm for cyber-physical path-loss modelling in 5G connected autonomous vehicular network, *Veh Commun*, **45** (2024) 100685, https://doi.org/10.1016/j.vehcom.2023.100685.