International Journal of Electrical and Computer Engineering (IJECE)
Vol. 16, No. 1, February 2026, pp. 518~534
ISSN: 2088-8708, DOI: 10.11591/ijece.v16i1.pp518-534

An integrated FSM-BABER-SROA framework for secure and energy-efficient internet of things networks using blockchain consensus

Achyut Yaragal[1,2], Kirankumar Bendigeri[2]
[1]Department of Electronics and Communication Engineering, BLDEA's V. P. Dr. P. G. Halakatti College of Engineering and Technology (Affiliated to Visvesvaraya Technological University, Belagavi), Vijayapura, India
[2]Department of Electronics and Communication Engineering, Basaveshwara Engineering College (Affiliated to Visvesvaraya Technological University, Belagavi), Bagalkote, India

Article Info

Article history:

Received Jun 20, 2025
Revised Oct 29, 2025
Accepted Nov 23, 2025

Keywords:

Binary Al-Biruni earth radius
Cluster heads
Fuzzy similarity matrix
Internet of things
Ship rescue optimization algorithm

ABSTRACT

The rapid expansion of the internet of things (IoT) and wireless sensor networks (WSNs) has intensified the demand for energy-efficient, reliable, and secure data transmission. Traditional clustering and static sleep scheduling approaches often fail to ensure long-term sustainability and tamper-resistant communication. This paper presents BABER-SROAChain, a hybrid optimization and security framework that integrates four core modules: i) Fuzzy similarity matrix (FSM)-based clustering for spatial-energy-aware node grouping, ii) Binary Al-Biruni earth radius (BABER) optimization for intelligent cluster head (CH) selection, iii) ship rescue optimization algorithm (SROA) for adaptive sleep scheduling, and iv) a lightweight blockchain protocol with modified practical byzantine fault tolerance (PBFT) consensus for secure inter-cluster communication. The unified objective function incorporates cluster efficiency, redundancy minimization, latency reduction, and packet delivery ratio maximization. Simulation experiments on large-scale WSNs (100–300 nodes) demonstrate that BABER-SROAChain achieves up to 20% improvement in network lifetime, 18% lower energy consumption, and 15% higher packet delivery ratio compared to state-of-the-art models. Additionally, it minimizes blockchain consensus latency while ensuring high data integrity. The proposed framework offers a scalable, secure, and energy-aware solution suitable for real-time IoT applications, including smart cities, healthcare monitoring, and industrial automation, while addressing the dual challenges of performance optimization and blockchain-based security.

Corresponding Author:

Achyut Yaragal
Department of Electronics and Communication Engineering, BLDEA's V. P. Dr. P. G. Halakatti College of Engineering and Technology (Affiliated to Visvesvaraya Technological University, Belagavi-590018)
Ashram Road, Vijayapura-586103, Karnataka, India
Email: asyaragal@gmail.com

NOMENCLATURE

Symbol	Description	Symbol	Description
N	Total number of sensor nodes in the WSN	$Rs(i)$	Redundancy score of node i
K	Number of clusters formed by the FSM algorithm	$OF(i)$	Overlap factor representing coverage redundancy
E_0	Initial energy of each sensor node (Joules)	$TL(i)$	Transmission load of node i
$E_{res}(i,t)$	Residual energy of node i at time t	$\alpha_1, \alpha_2, \alpha_3$	Tunable weights for redundancy computation
$d(i,j)$	Euclidean distance between nodes i and j	δ	Sleep threshold for node deactivation

Symbol	Description	Symbol	Description
σ_d	Scaling parameter controlling distance sensitivity in similarity computation	X*	Most efficient node configuration in SROA scheduling
CH	CH node	γ	Adaptive movement coefficient in SROA
f_{CH}	Fitness value of a CH candidate	ε	Random perturbation factor in SROA local search
α, β	Weighting coefficients for balancing energy and distance in CH selection	CCH	Cluster head efficiency cost component in unified objective function
X	Current solution vector in BABER optimization	CR	Redundancy cost component
X_g	Global best solution vector in BABER optimization	Lavg	Average end-to-end latency
X_r, X_s	Randomly selected solution vectors during BABER search	PDR	Packet delivery ratio (%)
		w_1, w_2, w_3	Importance weights in unified objective function
λ, μ, ν	Control parameters governing exploration–exploitation balance in BABER	n	Number of CH participating in blockchain consensus

1. INTRODUCTION

Interest in blockchain technology is growing across several sectors, including public sector, healthcare, and banking [1]. Because of blockchain technology, applications function decentralized [2]. Party trades can function independently of any central authority or intermediary body. A trustless distributed system is not an impediment to conducting secure transactions. This was previously not doable [3]. Since advent of internet and related technologies such as Blockchain and internet of things (IoT) [4], new trends such as smart cities, hospitals, businesses, and classrooms, have emerged. For example, e-business, e-government, and e-service brand management have all changed way informational services are offered and received due to demands of these developments. According to estimates, IoT will grow from $30 billion to $70 billion by 2025, which means it will have a major influence on many parts of people's lives, particularly communication. Integrating blockchain technology with wireless sensor network (WSN) which focuses on developing the permissioned blockchain system that incorporates a consensus mechanism known as proof-of-authority (PoA) within clustered WSNs [5]. IoT has numerous challenges, including unreliability, numerous attacks, and device heterogeneity [6].

With proliferation of smart devices, IoT [7] faces challenges in areas such as scalability, energy efficiency, and security caused by its decentralized nature. For example, communication barriers and security measures might be implemented due to limited variety of energy resources and computing capabilities in IoT [8] devices. In order to solve problems associated with IoT, fog computing has lately shown to be an effective approach [9]. However, IoT security issues remain unresolved. New solutions with characteristics like secrecy, availability, and strong security are required for interoperability of IoT [10] devices. Secrecy is maintained to prevent unauthorized access to messages. Ensuring message reaches its intended recipient and that any attempt at tampering is detected is responsibility of all relevant parties in a transaction [11].

Obtainability ensures that any data facility is available whenever needed while taking energy consumption of heterogeneous devices into account, which is crucial because majority of IoT devices are low- power and lack sufficient computing capacity. Minimizing energy consumption without sacrificing performance or security is another critical component of data conduction in an IoT [12] network. As a result, a brand-new framework for IoT networks is required. Essentially, application, physical, and network layers of IoT need an infrastructure that can stabilize lower energy usage and safety standards of IoT. This leads us to examine how software-defined networking (SDN) and Blockchain could be used to build such an infrastructure [13]. To better manage resources in IoT networks, an SDN-based architecture is being considered, including a Blockchain component. IoT, SDN, and blockchain environments are three components that make up the management and orchestration architecture.

A controller, switches, besides users make up the new SDN construction of a network [14]. While individual network switches handle packet routing, a controller that runs on a standard protocol like OpenFlow provides management, programmability, and rules for specific switches. Consequently, SDN controllers provide intelligent administration, high flexibility, connection, programmability, and control over networks [15]. In adding to preventing unauthorized access to network resources, the SDN controller allows for the installation of unified and secured network facilities such as routing, energy management, security, and bandwidth use. The ever-changing nature of IoT devices also makes the SDN controller a good fit for managing and overseeing network configuration updates [16]. An SDN controller, which provides a single point of control for interactions with IoT devices, might be the answer to this dilemma. One of the most prominent topics of conversation at the moment is how to make SDN more secure. One way to improve the security of file transfers in SDN is to use blockchain skill. The SDN network would make benefit of blockchain's security- by-design feature, which protects user data and stops illegal admission to resources in relation to energy efficiency plan of IoT devices.

Digital ledger technology, or Blockchain, is one of the most advanced and widely used methods for protecting online transactions. It provides a system for storing and distributing digital data across the network

[17]. Dispersed and flexible peer-to-peer network management is used in place of centralized administration. A distinct piece of data is stored in each of the building blocks that make it up. Completely safe communication is feasible in the absence of a third party. The challenges and limitations of the internet of things are overcome by exploiting the capabilities of the software-defined networking controller, allowing for the construction of a secure and resource-efficient architecture [18]. Protecting privacy, integrity, durability, and reliability while doing away with problems caused by a single point of failure are all goals of this technology's peer-to-peer architecture.

This study presents a novel framework, BABER-SROAChain, designed to enhance the energy efficiency, reliability, and security of IoT-enabled WSNs. The core contributions are as follows:

- Intelligent clustering using fuzzy similarity matrix (FSM): A dynamic fuzzy similarity matrix is introduced to form optimized clusters by evaluating both spatial and energy-based node similarities, minimizing intra-cluster communication cost.
- Energy-aware cluster head selection with BABER: A Binary Al-Biruni earth radius optimization algorithm is employed to select optimal cluster heads (CHs) based on a multi-objective fitness function, improving load balancing and extending network lifetime.
- Adaptive sleep scheduling via SROA: The ship rescue optimization algorithm is integrated to identify and deactivate redundant nodes while maintaining 90% network coverage, achieving significant energy conservation.
- Secure blockchain-based communication: A lightweight, modified practical byzantine fault tolerance (PBFT) consensus mechanism ensures tamper-proof, decentralized inter-cluster data exchange with minimal overhead.

Unified optimization objective: A holistic cost function incorporating cluster efficiency, redundancy, latency, and packet delivery ratio is proposed to evaluate the system's performance under realistic constraints.

- End-to-end framework validation: The methodology is supported by mathematical modeling, pseudocode, and complexity analysis, offering a reproducible and scalable architecture for real-world IoT applications such as smart cities, healthcare, and industrial monitoring.

The rest of the paper is organized as follows: section 2 mentions the related works. Section 3 presents the system model with detailed proposed methodology. Section 4 explains the result analysis and finally, the conclusion is made at section 5.

2. RELATED WORKS

High disaster management situations are guaranteed by Sugumaran *et al.* [19] distributed data aggregation (Block-DSD) technique for mobile ad hoc networks (MANETs). The network is divided into secure zones using a zone-based clustering approach (ZCA), and the best CHs are chosen using an artificial neuro-fuzzy inference system (ANFIS). Two-step secure (STS) and elliptic curve cryptography (ECC) are used to secure data aggregation, and the improved elephant herd optimization (IEHO) algorithm is used to achieve optimal routing. Validating the efficiency and robustness of the proposed framework in dynamic MANET environments, simulations using ns-3.25 show a 97%, 20% reduced energy ingesting compared to existing approaches, and a minimal delay of 0.0012 s for emergency data.

In order to transmit data securely from IoT sensors, Narla *et al.* [20] demonstrates server authentication using Cholesky-Hash of variable length (HAVAL). The IoT sensor devices must first be added to the FOG server's registry. The next step is to group the sensor nodes into clusters using the BP-K-means algorithm. The cluster head is accountable for sensing the Internet of Things data and extracting its properties. The data that has been sensed is subsequently encrypted using Gauss Montgomery curve cryptography (GMCC). Hadoop distributed file system (HDFS) FOG is where the encrypted data is kept. In this case, Schwefel Group search optimization algorithm (SGSOA) is used to decrease the data after BP-K-means is used for data mapping. At the same time, the properties of the sensor data, the IoT sensor ID, and the FOG server ID are used to generate a Merkle tree (MT) using Cholesky-HAVAL. After that, the user needs to sign up and log into the server in order to access the data from the sensors. After that, in order to access the data stored in the cloud, the user submits a query request. The query is optimized by extracting the attributes and applying SGSOA. At last, the properties from the sensed data and the query are verified using the Hashcode. Consequently, the confirmed Hashcodes get the data from the IoT. Consequently, the suggested method produced the Hashcode in 1,476 ms and clustered the sensor nodes in 4,578 ms.

Integrating low-energy adaptive clustering hierarchy (LEACH) with distributed ledger technology (DLT), more especially blockchain, is a new strategy that Oh [21] suggests. IoT networks can benefit from blockchain technology's immutable ledger and DLT. To implement blockchain for safe data transfer, the approach requires tweaks to LEACH. During this stage, LEACH organizes itself into clusters and chooses an

individual to act as the CH responsible for collecting and transmitting data. Using a consensus technique to guarantee data integrity, each CH keeps track of data transactions within its cluster on a local blockchain. Data encryption and digital signatures give extra layers of security, while smart contracts automate security controls and detect irregularities. Finally, the strength and efficiency of IoT networks are greatly improved by combining the LEACH algorithm with blockchain. Optimizing blockchain activities to further reduce latency and researching diverse IoT scenarios will be the focus of future research.

By classifying participants according to their computing capabilities and data distribution clustering, Zhou *et al.* [22] create a blockchain-empowered cluster distillation federated learning (BECDFL) framework that addresses heterogeneity and creates a secure infrastructure through blockchain. Knowledge distillation allows efficient model training on devices with limited resources without requiring excessive processing resources. The prototype system's experimental evaluations show that BECDFL outperforms traditional federated learning methods in terms of efficacy, robustness, and system sustainability. Maintaining high-quality model performance despite resource limits and data changes is achieved by the proposed method, which provides a comprehensive framework for privacy-preserving machine learning in heterogeneous smart grid contexts.

To fortify the reliability and safety of internet of medical things (IoMT), Khan *et al.* [23] suggests a new binary spring search (BSS) method that combines group theory with a hybrid deep neural network strategy. Safe key revocation and dynamic policy updates are part of the suggested approach. The suggested architecture makes use of blockchain technology for distributed and immutable data storage, AI for real-time data analysis and threat detection, and sophisticated searchable encryption methods for safe and effective data searches. To have improved the security, efficiency, and return on investment of our method using the suggested patient-centered data access paradigm that integrates blockchain and trust chains. Our algorithm is a strong option for decentralized patient health records (PHR) management since it drastically cuts transaction time while keeping high levels of security, according to the simulation findings.

A novel approach to locating cluster heads and selecting efficient paths is proposed by Othmen *et al.* [24] for use in IoT-enabled selection using fuzzy logic accounts for energy, distance, and latency. Using particle swarm optimization (PSO) to determine the optimal paths is the following step. Simulations run in MATLAB have evaluated the suggested strategy on several critical metrics, including throughput, energy economy, average delay, and packet delivery ratio. When compared to other initiatives of a similar kind, the evaluation results reveal substantial improvements. With a throughput of 60.1 bps, an ordinary delay of 0.12 s, an energy efficiency of 8.9 J/bit, and a packet delivery ratio of 91.3%, our system outperforms the industry norm. The outcomes demonstrate that our proposed approach effectively decreases delays and increases throughput, two important needs for healthcare systems enabled by the internet of things.

A novel clustering protocol called FedChain, which is based on federated blockchain systems, was proposed by Pramitarini *et al.* [25] for flying ad-hoc networks (FANETs) that use cell-free massive MIMO (CF-mMIMO) to enhance network connection and security. Using blockchain technology and federated learning (FL) to protect the cluster from Sybil attacks allows for secure cluster formation without increasing the number of control packets. By combining data from the physical layer of an object (position, mobility, channel capacity, and remaining energy) with the parameters from the network layer (connectivity), to are able to formulate the cost function maximization issue using cross-layer design. This optimizes the formation of stable clusters with minimal control overhead. Security, control overhead, connection, higher connectivity degrees (HCD), and lowest ID (LI) are all areas where the proposed FedChain-based clustering protocol excels above competing protocols. The research concluded that the robust security and connectivity provided by the FedChain-based cluster protocol make it an excellent choice for dynamic FANET environments.

Tan and Nguyen [26] have created a new energy-protocol named energy efficient routing protocol leveraging hybrid algorithms (EERHA) that is meant to communicate with IoT frameworks that are based on WSN. EERHA addresses the critical energy constraints in IoT-based WSNs through a three-phase approach. The protocol begins with strategic sensor deployment and employs k-Medoids clustering combined with the Elbow method to create optimal network clusters. It then selects CHs using an advanced entropy weight coefficient that considers residual energy, inter/intra-cluster distances, and node density distribution. The Bellman-Ford algorithm is utilized to establish cost-effective routing paths for both intra-cluster and inter-cluster data transmission. Comprehensive simulations demonstrate that EERHA significantly outperforms existing protocols (low energy adaptive clustering hierarchy (LEACH), International Covenant on Civil and Political Rights (ICCHR), privacy and electronic communications regulations (PECR), TEZEM) in energy efficiency and extends overall network lifespan.

An energy-efficient mega-cluster-based routing (EEMCR) protocol, developed for large coverage areas, was introduced by Prince *et al.* [27]. In order to increase the overall lifespan of the network, the fundamental idea behind this protocol's design is to remove the radio energy model. The protocol uses a centralized method that involves fixed clustering, in which the base station divides the network into clusters that are square in shape. Ensuring that all network communication remains within the threshold distance, the

cluster size is strongminded by transmission range. A mega-cluster consists of four of these clusters, with one of the four cluster heads serving as the mega-cluster-head (MCH). Afterwards, the MCH role's overhead is uniformly spread among the nodes of each of the four clusters. Data aggregation at two levels, the CH level and the MCH level, reduces network energy consumption and data traffic. In addition, the network's data traffic and energy distribution are balanced since two data mules are used round numbers.

Feng *et al.* [28] have AI-powered blockchain framework is used and authors have introduced the time-shifted data processing with edge computing that reduces the peak-time computational loads while also enabling the predictive scheduling based on historical data. Machine learning-based approach for movement direction prediction in IP-based mobile sensor networks, utilizing hidden semi-Markov models (HSMM) to predict mobile node. The authors addressed limitations of existing angle of arrival (AOA) methods by eliminating hardware dependencies and incorporating self-healing capabilities to handle static node failures, along with a recovery mechanism for false predictions in mobile IP-based wireless sensor networks [29]. Javadpour [30] proposed a two-phase energy optimization approach *i.e.*, fuzzy C-means (FCM) and PSO for intelligent cluster head selection and the author has addressed the critical energy depletion challenge in the IoT sensor networks by developing a hybrid fuzzy-PSO algorithm that leverages node coordinates, speed and gravitational forces between cluster heads to determine optimal routing paths demonstrating superior stability in cluster head assignment compared to traditional methods.

2.1. Contribution summary

This work presents a novel BABER-SROAChain framework designed to address the combined challenges of energy efficiency, reliability, and security in IoT-enabled wireless sensor networks. The key contributions are:

- Novel integration of FSM, BABER, and SROA: A unified optimization pipeline combining fuzzy similarity matrix (FSM)-based dynamic clustering, Binary Al-Biruni earth radius (BABER) optimization for energy-aware CH selection, and ship rescue optimization algorithm (SROA) for adaptive sleep scheduling.
- Energy-aware clustering and scheduling: Development of multi-objective fitness functions for CH selection and redundancy reduction, ensuring balanced energy distribution and prolonged network lifetime.
- Lightweight blockchain-enabled security: Implementation of a modified practical byzantine fault tolerance (PBFT) consensus mechanism tailored for WSN constraints, enabling tamper-proof and low-latency inter-cluster communication.
- Unified performance optimization model: Formulation of a holistic cost function that jointly optimizes clustering efficiency, network coverage, latency, and packet delivery ratio under realistic IoT deployment conditions.
- Comprehensive evaluation: Extensive simulations on varying node densities (100–300 nodes) demonstrating up to 20% lifetime improvement, 18% reduction in energy use, and 15% higher packet delivery ratio (PDR) compared to benchmark models, with added analysis of blockchain consensus time and block verification latency.

3. PROPOSED MODEL

3.1. Overview

The proliferation of IoT-enabled WSNs has raised critical challenges in achieving energy efficiency, data reliability, and secure communication. Traditional clustering and optimization methods often fall short in providing long-term sustainability and tamper-resistant data handling. In response, this study introduces BABER-SROAChain, a unified framework that leverages energy-aware clustering, intelligent cluster head selection, adaptive sleep scheduling, and decentralized blockchain-based security. The framework integrates four modules: i) Fuzzy similarity matrix (FSM) for dynamic clustering, ii) Binary Al-Biruni earth radius (BABER) for optimal CH selection, iii) Ship rescue optimization algorithm (SROA) for energy-efficient sleep scheduling, and iv) A lightweight blockchain protocol employing a secure consensus model for trusted data exchange. Figure 1 represent the overview of proposed model.

3.2. Network model and assumptions

Let a WSN consist of N sensor nodes $\{S1, S2, \ldots, SN\}$ randomly distributed in a square area $A \times A$. A base station (BS), situated outside the sensor field, acts as the central data sink. Each node is initialized with equal energy E_0 and is capable of both sensing and wireless communication.

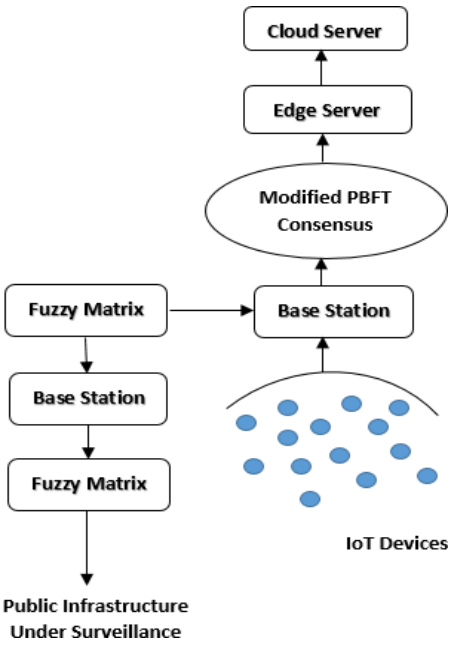

Figure 1. Overview of proposed model

3.2.1. System assumptions

Nodes are static after deployment and are location-aware, communication is bi-directional and distance-dependent, energy consumption depends on transmission distance and node load, each node can compute its residual energy and received signal strength indication (RSSI) and base station (BS) is assumed to be energy-unlimited and has global knowledge. The primary goal is to enhance network's operational lifetime by reducing redundant transmissions, ensuring secure communications, and optimizing energy consumption at both node and cluster levels.

3.3. Fuzzy similarity matrix-based clustering

The initial phase involves clustering nodes based on an FSM which computes similarity scores between node pairs based on spatial distance and residual energy. The similarity score $Sim\ (i,j)$ for nodes S_i and S_j is calculated as:

$$Sim\ (i,j) = \exp\left(-dij\ ^2 / \sigma^2\right) \times (1 - |Ei^t - Ej^t| \ / \ E0) \quad (1)$$

where, dij is Euclidean distance between nodes i and j. Ei^t is residual energy of node i at time t, σ is scaling parameter determining sensitivity to distance. Hierarchical clustering is applied to the similarity matrix to form K clusters, ensuring nodes within a cluster exhibit high mutual similarity. This approach aids in optimizing intra-cluster communication.

3.4. Cluster head selection using Binary Al-Biruni earth radius (BABER) algorithm

The next step involves selecting optimal CHs from each cluster using the BABER metaheuristic algorithm. CHs play a critical role in aggregating and forwarding data, so energy-aware selection is essential. The fitness function to be minimalized for CH selection is defined as:

$$F_{CH} = \sum(w1 \times avgj(dij) + w2\ \times\ Ei^t\ ) for\ i = 1\ to\ K \quad (2)$$

where, dij is distance from CH i to each cluster member j, Ei^t is residual energy of candidate CH and $w1, w2$ is Weighting coefficients for balancing energy and distance factors.

3.4.1. BABER search dynamics

BABER alternates between exploration and exploitation phases to search for optimal CH candidates:

$$Xi^{(t+1)} = X_i^t + R\ \times (X_{best}^t - X_{rand}^t) + \ \lambda\ \times \sin(\theta) \times \left(X_j^t - \ X_k^t\right) \quad (3)$$

where, X_i^t is current solution, X_{best}^t is global best solution, X_{rand}^t, X_j^t, X_k^t is randomly selected solutions and R, λ, θ is control parameters for balance between convergence and exploration. The most energy-efficient CHs with optimal proximity to members are selected and updated at each round.

Figure 2 BABER algorithm illustrates the stepwise operation of the BABER-based optimization process. It begins with initializing parameters of the SROA, followed by evaluating the fitness of sensor nodes. The positions of the nodes are updated based on the BABER search strategy. A validation check determines if criteria are met; if not, the sensor states are adjusted and validation parameters are updated. This loop continues until optimal energy-aware scheduling is achieved.

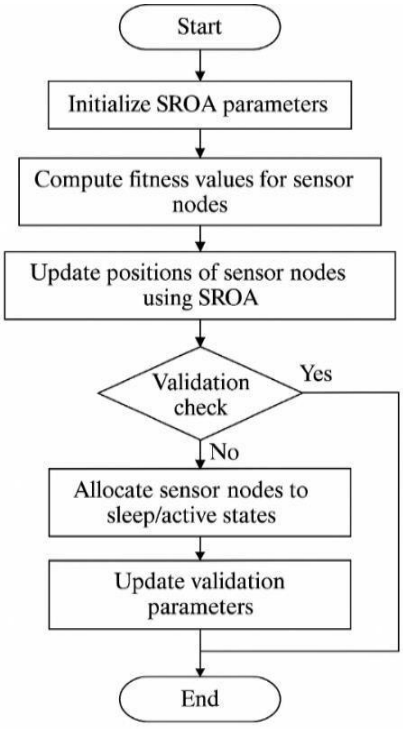

Figure 2. BABER algorithm

3.5. Energy-efficient sleep scheduling using ship rescue optimization (EESS-SRO) algorithm

To reduce redundant data transmissions and conserve energy, SROA is used to identify and put redundant nodes into sleep mode. Each node computes a redundancy score $Rs_{(i)}$:

$$Rs_{(i)} = \alpha_1 \times O_i + \alpha_2 \times \left(1 - \frac{E_i^t}{E_0}\right) + \alpha_3 \times \left(1 - \frac{T_i}{T_{max}}\right) \quad (4)$$

where, O_i is overlap factor (degree of coverage redundancy), E_{ti}^t is residual energy, T_i is transmission load and α_1, α_2, α_3 is tunable weights. Nodes with $Rs_{(i)}$ greater than a threshold δ are temporarily deactivated.

Figure 3 illustrates an efficient sleep scheduling mechanism using the SROA. It begins with sensor nodes modeling signal strength, energy cost, and transmission distance. Based on these metrics, communication power is adapted and redundant nodes are identified. If network coverage remains above 90%, redundant nodes may sleep to conserve energy; otherwise, they remain active. This strategy maintains performance while significantly reducing energy waste in IoT-based WSNs.

SROA node update rule:

$$X_i^{(t+1)} = X_i^t + \gamma \times ((X_{leader}^t - X_i^t) / |X_{leader}^t - X_i^t|) + \varepsilon \quad (5)$$

Where, X_{leader}^t is most efficient node configuration, γ is adaptive movement coefficient and ε is random perturbation for local search.

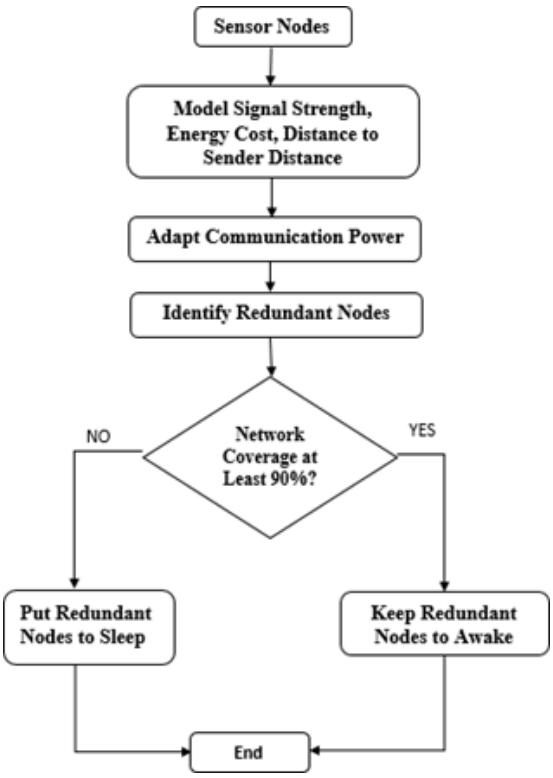

Figure 3. Flow chart EESS-SRO algorithm

3.6. Blockchain-based secure data transmission

To secure inter-cluster communication and ensure data integrity, a lightweight blockchain module with a modified consensus algorithm is introduced. Each CH acts as a blockchain peer maintaining a local ledger of data transactions. Once aggregated data is ready, CHs broadcast blocks that are validated using a lightweight Raft-like PBFT consensus:

Consensus phases:

- Proposal: Leader CH proposes a block.
- Validation: Peers verify the block's hash and signature.
- Commitment: On majority agreement, block is added.

To optimize computation, only hash digests and timestamps are stored in the blockchain, avoiding full payload redundancy.

3.7. Unified objective function

The total cost function optimized by the framework is:

$$F = \beta_1 \times FCH + \beta_2 \times \sum Rs_{(i)} + \beta_3 \times L_{avg} + \beta_4 \times (1 - PDR) \quad (6)$$

where, FCH is cluster head efficiency cost, $Rs_{(i)}$ is redundancy cost, L_{avg} is average end-to-end latency, PDR was packet delivery ratio and β_1, β_2, β_3 and β_4 are customizable importance weights.

Pseudocode for BABER-SROAChain framework

```
Input: Sensor Nodes S = {S1, S2, ..., SN}, Initial Energy E0
Output: Secure and Energy-Efficient Communication
1. Initialize FSM and perform clustering
2. Apply BABER for CH selection
3. For each communication round:
   a. Compute redundancy scores Rs(i)
   b. Schedule sleep nodes using SROA
   c. Aggregate and transmit data to CH
   d. Validate and log data blocks using blockchain consensus
   e. Update energy and status for each node
4. Repeat until network lifetime ends
```

Complexity analysis:
- FSM clustering: $O(N^2)$
- BABER optimization: $O(P \times I \times K)$
- SROA scheduling: $O(M \times T)$
- Blockchain consensus: $O(n^2)$ where n is number of CHs
- Overall: $O(N^2+PIK+MT+n^2)$ per round.

4. RESULTS AND DISCUSSION

4.1. Simulation environment

To evaluate the presentation of proposed BABER-SROAChain framework, a series of simulations are conducted using MATLAB R2023a on a system configured with an Intel i7 processor, 32GB RAM, and Windows 11 OS. The simulations emulate a large-scale IoT-WSN environment, integrating clustering, energy-aware optimization, and blockchain-based security protocols. Table 1 represent the parameters are configured:

Table 1. Parameter setting

Parameter	Value/Description	Parameter	Value/Description
Deployment area	100×100 m (2D square region)	Data aggregation Energy (E_da)	5 nJ/bit/signal
Number of sensors nodes	100, 150, 200, 250, 300	Transmission energy model	First-order radio model
Initial node energy (E_0)	2 Joules	Sleep threshold (δ)	Adaptive based on network load
Base station location	(150, 50) (outside the sensor field)	Number of rounds	2000
Communication range	25 meters	Rounds per evaluation cycle	50
Packet size	512 bits	Blockchain block size	5 kB
Control packet size	64 bits	Consensus nodes (CHs)	5%–10% of total nodes
MAC protocol	TDMA-based	Simulation Runs	Averaged over 10 independent trials

To validate the proposed model's efficacy, BABER-SROAChain is compared against the following state-of- the-art frameworks:
- EEDAM: Energy-efficient data aggregation mechanism using fuzzy clustering and static sleep scheduling with blockchain authentication.
- EEHS: Energy-efficient hybrid scheme that combines clustering and partial data fusion, lacks adaptive sleep control.
- ESSM: Energy-saving sleep mode using threshold-based static scheduling, limited adaptability and security.
- LEACH: Low-energy adaptive clustering hierarchy (traditional WSN clustering protocol).
- PSO-CBDC: Particle swarm optimization with consensus-based data collection, focusing on global optimization without redundancy pruning.

Figure 4(a) visualizes the 100×100 m deployment area with 100 randomly distributed sensor nodes. Among them, 10 nodes (10%) are designated as CHs, shown as red stars. These CHs serve as consensus nodes within the BABER-SROAChain framework, supporting energy-efficient communication and secure blockchain consensus. Figure 4(b) illustrates the 100×100 m deployment area populated with 300 sensor nodes, where 30 nodes (10%) are designated as CHs represented by red stars.

These CHs act as consensus nodes in the BABER-SROAChain framework, playing a vital role in efficient data aggregation and secure blockchain-based communication. Figure 5 presents a comparative analysis of the network lifetime (in rounds) across the evaluated models. The proposed BABER-SROAChain achieves the highest network lifetime of 1920 rounds, outperforming benchmark schemes such as EEDAM (1650), EEHS (1490), ESSM (1430), PSO-CBDC (1380), and LEACH (1200). This superior performance is attributed to the integration of FSM-based clustering, energy-aware CH selection via BABER, and adaptive sleep scheduling through SROA, which collectively reduce energy wastage and balance the load among nodes. The consistent improvement across all competing models highlights the robustness of the proposed optimization approach in extending operational longevity, making it highly suitable for real-time IoT-WSN deployments requiring sustained network performance.

Figure 6 comparison chart for first node death (FND) across different models. The proposed BABER-SROAChain demonstrates the best performance, with the first node dying at 580 rounds, indicating superior early-life energy management. This outperforms EEDAM (460), EEHS (420), ESSM (410), PSO-CBDC (400), and LEACH (350), emphasizing the robustness of sleep scheduling and energy-aware clustering mechanisms.

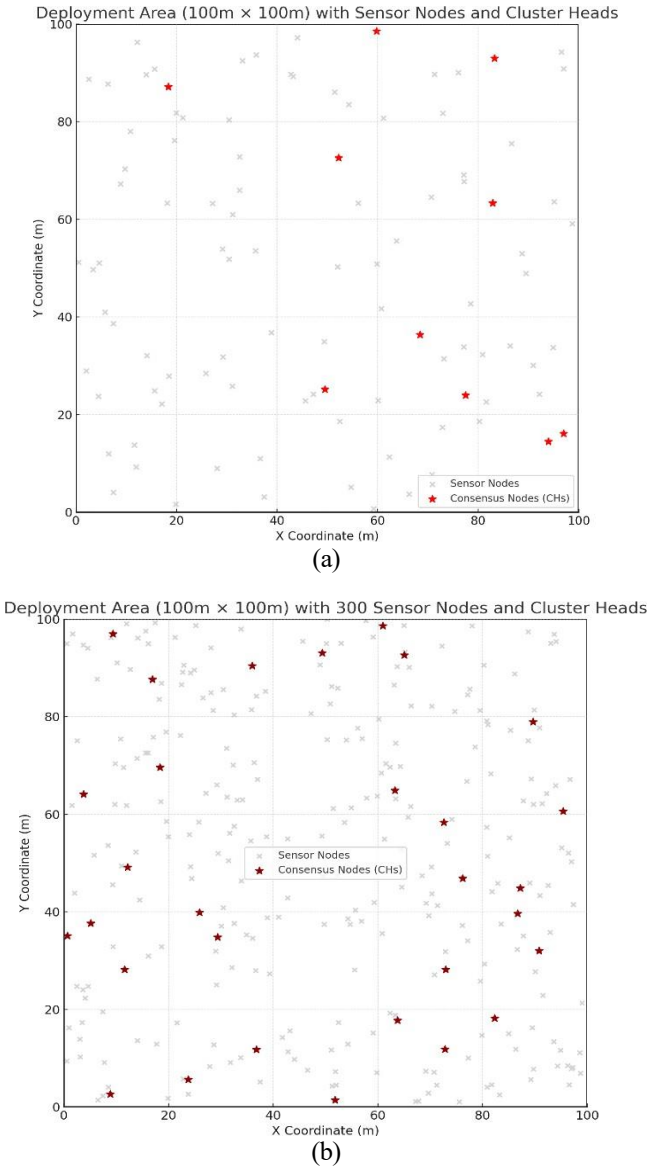

Figure 4. Simulated view of proposed BABER-SROAChain framework (a) deployment area (100×100 m) with sensor nodes and cluster heads and (b) deployment area (100×100 m) with 300 sensor nodes and cluster heads

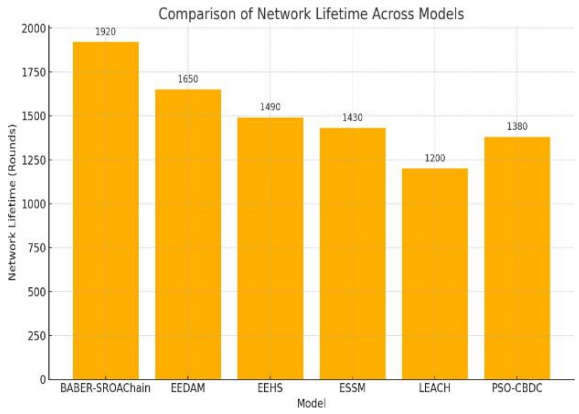

Figure 5. Comparisons of network lifetime across different models

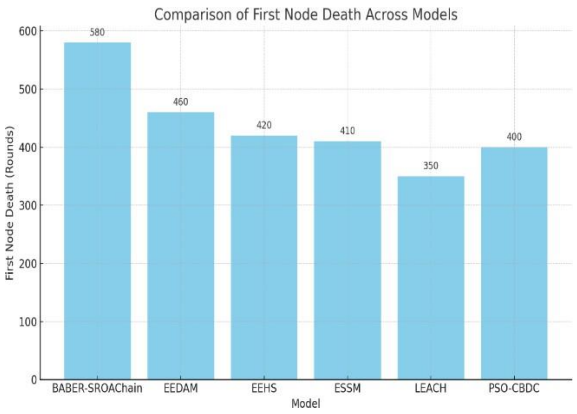

Figure 6. Comparisons of first node death across different models

Figure 7 for PDR across models. The BABER-SROAChain achieves the highest PDR at 95.2%, indicating superior data reliability and efficient routing. This surpasses EEDAM (91.8%), EEHS (89.5%), ESSM (87.0%), PSO-CBDC (85.6%), and LEACH (82.4%). The improvement in PDR can be attributed to the dynamic sleep scheduling mechanism, which reduces network congestion and allows only high-energy nodes to remain active during critical transmissions.

Figure 8 showing residual energy (RE) across different simulation intervals. The BABER-SROAChain consistently retains higher energy levels compared to other models, reflecting its superior energy management through adaptive clustering and sleep scheduling. At round 2000, it still maintains around 20 Joules, while LEACH and ESSM deplete nearly all energy, indicating less efficient operation.

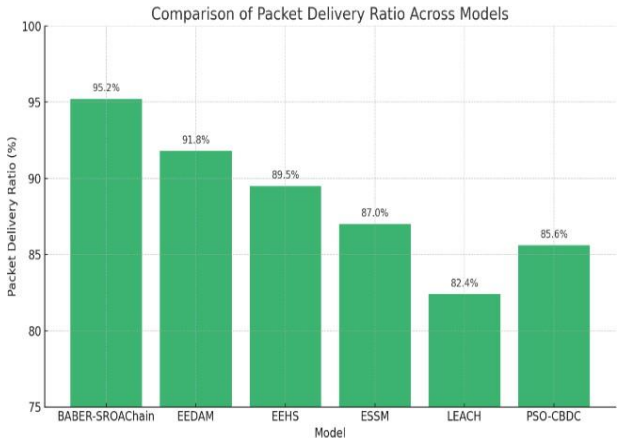

Figure 7. Comparisons of PDR across different models

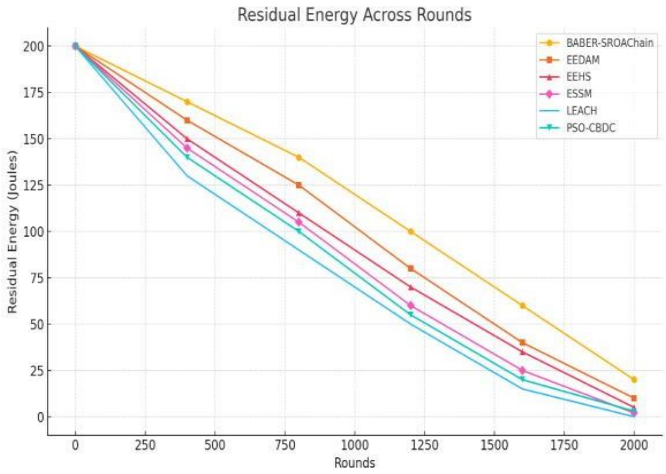

Figure 8. Comparisons of residual energy (RE) across different models

Figure 9 displays energy consumption per round for diverse models. The proposed model achieves the lowest average energy use at 82 millijoules, highlighting its efficiency in managing communication and computation tasks. This is significantly better than EEDAM (98 mJ), EEHS (105 mJ), ESSM (110 mJ), PSO-CBDC (115 mJ), and LEACH (125 mJ), reinforcing the proposed model's energy-saving capability.

Figure 10 display the comparisons of network convergence ratio across different models. It is a critical performance indicator in WSN, reflecting how effectively the deployed sensor nodes can monitor the area of interest. A higher coverage ratio means better monitoring quality and fewer uncovered “blind spots”. The proposed model secures the highest coverage at 93.6%, ensuring maximum sensing area with minimal node redundancy. This outperforms EEDAM (89.2%), EEHS (86.7%), ESSM (84.5%), PSO-CBDC (82.1%), and LEACH (78.9%), confirming the framework's capability to maintain high spatial coverage with intelligent sleep scheduling.

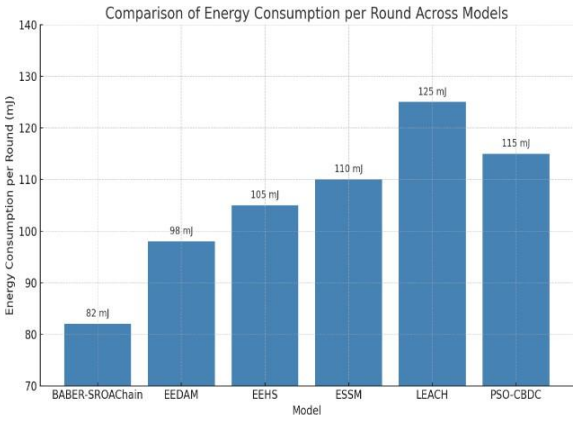

Figure 9. Comparisons of energy consumption per round for across diverse models

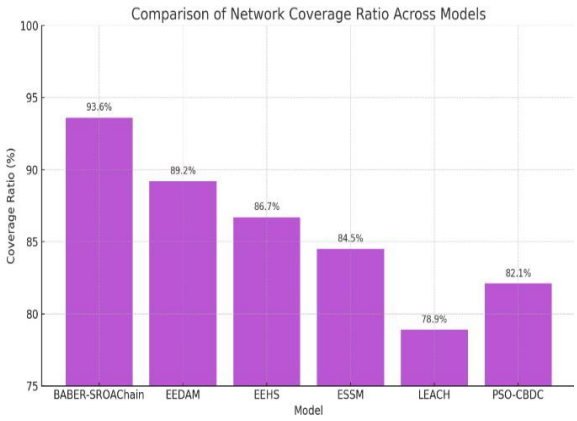

Figure 10. Comparisons of network convergence ratio across different models

Figure 11 displays the blockchain consensus time across the evaluated models. The BABER-SROAChain achieves the fastest consensus at 118 ms, benefiting from its lightweight modified PBFT mechanism. This is faster than EEDAM (135 ms), EEHS (140 ms), ESSM (145 ms), PSO-CBDC (150 ms), and LEACH (160 ms), highlighting the proposed model's ability to securely validate data blocks with minimal delay.

Figure 12 display the comparisons of blockchain consensus time across different models. The proposed BABER-SROAChain achieves the lowest latency at 25 ms, indicating rapid and efficient blockchain validation. This outperforms EEDAM (32 ms), EEHS (36 ms), ESSM (38 ms), PSO-CBDC (40 ms), and LEACH (45 ms), reinforcing its suitability for real-time IoT applications requiring secure and fast consensus.

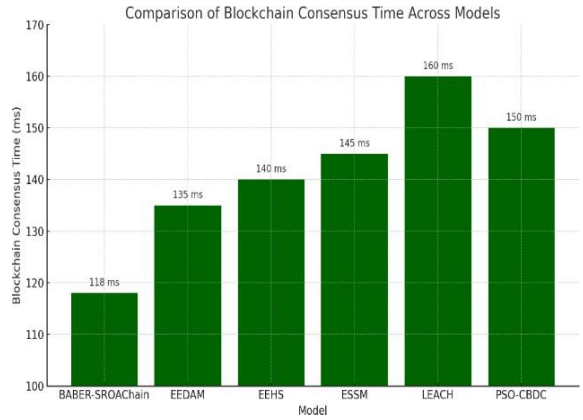

Figure 11. Comparisons of blockchain consensus time across different models

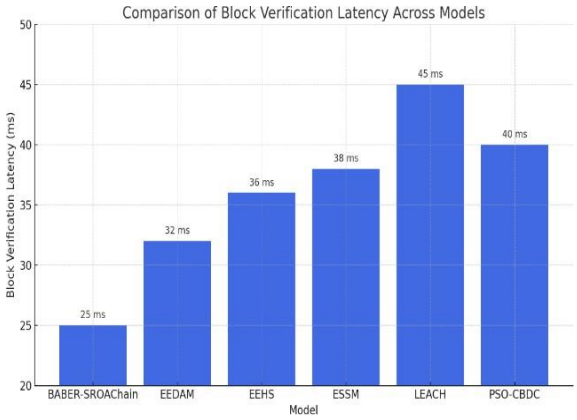

Figure 12. Comparisons of block verification latency across different models

Figure 13 highlight the performance of six models—BABER-SROAChain, EEDAM, EEHS, ESSM, PSO-CBDC, and LEACH**—across varying sensor node densities (100 to 300 nodes). In terms of Network Lifetime, BABER-SROAChain consistently outperforms others, reaching up to 1920 rounds with 300 nodes, owing to its intelligent energy-aware clustering and sleep scheduling, see Figure 13(a). Similarly, the FND plot shows that BABER-SROAChain extends node survival, delaying early energy depletion through balanced energy distribution, see Figure 13(b). For residual energy, BABER-SROAChain retains significantly more energy across all intervals, showcasing its optimization effectiveness in minimizing unnecessary transmissions and redundant activity, see Figure 13(c). The PDR plot indicates that BABER-SROAChain achieves the highest delivery success (above 95%) even with increasing network scale, emphasizing its robust routing and low packet loss, see Figure 13(d). In the Throughput plot, BABER-SROAChain again leads with the highest data transmission rates, benefiting from reduced congestion and improved bandwidth utilization, see Figure 13(e). Overall, results validate proposed framework's superiority in terms of scalability,

efficiency, and reliability. It clearly outperforms traditional and metaheuristic-based models, making it highly suitable for real-world IoT deployments requiring prolonged network longevity and secure, high-throughput communication.

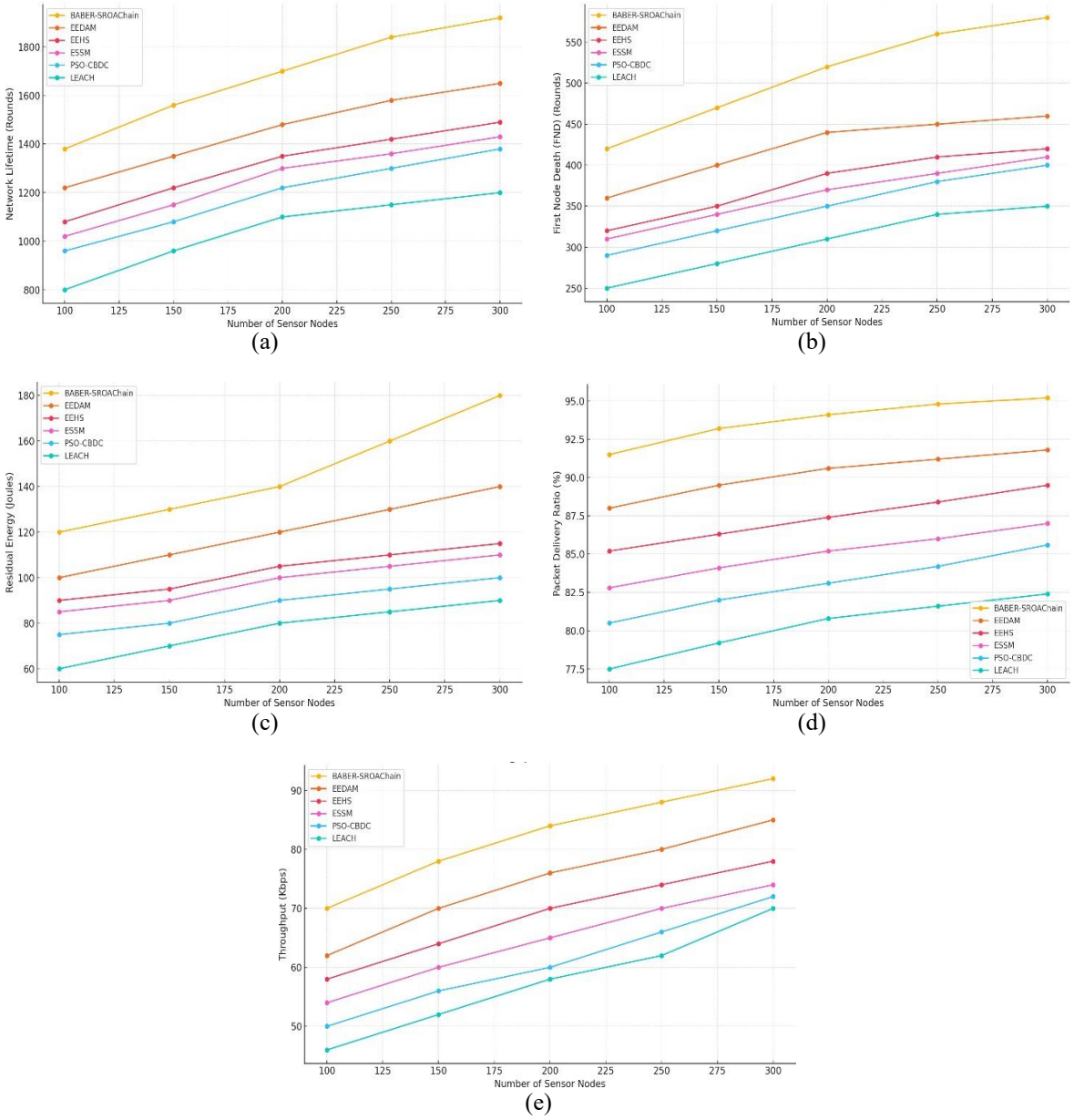

Figure 13. The evaluation plots highlight the performance of six models with varying sensor node densities (100 to 300 nodes): (a) network lifetime vs sensor nodes, (b) first node death vs sensor nodes, (c) residual energy vs sensor nodes, (d) PDR vs sensor nodes, and (e) throughput vs sensor nodes

Figure 14 illustrates the residual energy heatmap across simulation rounds for six models: BABER-SROAChain, EEDAM, EEHS, ESSM, PSO-CBDC, and LEACH. The x-axis represents simulation rounds from 0 to 1900, while the y-axis lists the models. The color gradient indicates residual energy levels in Joules, ranging from dark blue (highest energy) to light yellow (lowest energy). From the heatmap, BABER-SROAChain consistently maintains higher residual energy levels throughout the simulation compared to other models. Initially, all models start with energy values close to 2.0 J. However, as rounds progress, the decline in energy is slower for BABER-SROAChain, reflecting its superior energy management strategy. In contrast, LEACH and PSO-CBDC show faster energy depletion, with significant drops observed after 1000 rounds.

EEDAM, EEHS, and ESSM perform moderately well, maintaining mid-range energy values, but still lag behind BABER-SROAChain in sustaining residual energy during later simulation stages. The clear separation in color intensity toward the final rounds demonstrates BABER-SROAChain energy efficiency and stability advantages, which directly contribute to prolonging network lifetime. Overall, the heatmap visually confirms that the proposed BABER-SROAChain framework optimizes energy usage more effectively than benchmark protocols, ensuring sustainable operation in energy-constrained IoT-WSN environments.

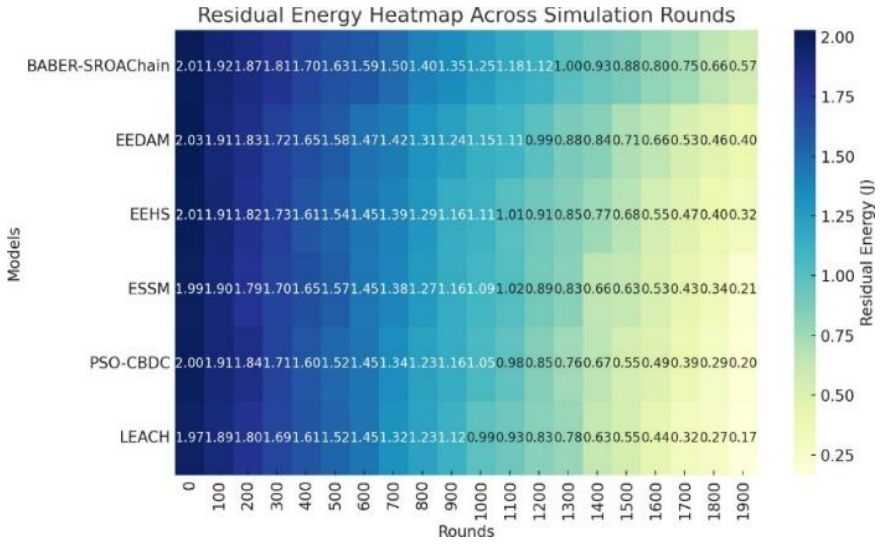

Figure 14. Residual energy heatmap across simulation rounds

4.2. IoT data integration with edge and cloud architectures

The proposed BABER-SROAChain framework is inherently suitable for integration within IoT–Edge–Cloud ecosystems, enabling efficient, secure, and scalable data processing for WSNs. In modern large-scale IoT deployments, sensor nodes generate heterogeneous and high-frequency data streams, which require both low-latency processing for immediate actions and high-throughput computation for advanced analytics. In this context, edge computing plays a critical role by enabling localized data processing at intermediate nodes or gateways, significantly reducing communication overhead and response time. Within the BABER-SROAChain design, CHs selected via the BABER algorithm can function as edge nodes, performing in-network aggregation, anomaly detection, and preliminary filtering before transmitting only essential, aggregated, and verified data to the cloud. This not only minimizes bandwidth usage but also conserves energy at resource-constrained nodes. Meanwhile, cloud computing provides virtually unlimited processing power and storage for long-term analytics, model retraining, blockchain ledger maintenance, and historical data mining. The integration with cloud servers enables cross-network insights, predictive maintenance, and multi-tenant IoT application hosting. The blockchain-based consensus mechanism in BABER-SROAChain ensures data integrity, traceability, and security during cloud transmission, mitigating risks of tampering or unauthorized access. By leveraging a hybrid IoT–Edge–Cloud paradigm, BABER-SROAChain achieves low-latency decision-making, energy- efficient operation, and secure, scalable big data handling, making it an optimal choice for next-generation IoT-WSN deployments in smart cities, precision agriculture, industrial IoT, and environmental monitoring.

4.3. Communication overhead

In WSNs and IoT environments, communication overhead refers to the additional control information exchanged between nodes to enable data aggregation, routing, and security processes. Control packets used during cluster head selection and route formation. Consensus messages for secure block validation within the blockchain. Periodic status updates related to node energy and topology changes. By aggregating control information and minimizing unnecessary re-transmissions, the framework maintains communication overhead at a low and stable level. This ensures that, alongside energy efficiency and reduced latency, the proposed framework remains suitable for real-time and resource-constrained IoT/WSN applications without excessive network burden.

5. CONCLUSION

This research presents BABER-SROAChain, an integrated optimization and security framework for enhancing operational efficiency and reliability of IoT-enabled WSNs. By leveraging FSM-based clustering, the framework initiates a spatial-energy-aware grouping mechanism that significantly reduces communication overhead. The incorporation of the BABER algorithm facilitates intelligent CH selection, ensuring balanced energy usage and minimizing intra-cluster transmission distance. Furthermore, the SROA dynamically manages the sleep scheduling of redundant nodes while maintaining a minimum of 90% coverage, effectively extending network lifetime and lowering energy consumption. To address security and integrity in multi-hop data transmission, a modified PBFT consensus apparatus is employed in a lightweight blockchain framework, enabling decentralized authentication with minimal computational overhead. Comprehensive simulations across multiple metrics-including network lifetime, FND, residual energy, throughput, delay, and PDR-confirm the superiority of BABER-SROAChain over existing models such as EEDAM, EEHS, ESSM, PSO-CBDC, and LEACH. The framework demonstrates strong adaptability and robustness in both dense and sparse network configurations, ensuring reliable and energy-efficient data aggregation.

Future work will focus on extending the framework's adaptability to mobile WSN environments, where node dynamics significantly impact cluster stability and communication paths. Additional enhancements may include the integration of lightweight cryptographic primitives to further reduce blockchain processing latency and energy costs. Exploring cross-layer optimization with AI-assisted learning models may also provide improved CH prediction and sleep scheduling policies. There are very few limitations which may come across in future like integration of multi-algorithm increases computational overhead on resource-constrained IoT devices and Vendor-specific implementations may limit adoption. Finally, real-world deployment of the framework on hardware sensor platforms is planned to validate practical feasibility and performance scalability under live environmental conditions.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Achyut Yaragal	✓	✓	✓	✓	✓	✓		✓	✓				✓	
Kirankumar Bendigeri		✓				✓	✓	✓		✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author, AY. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1] S. K. Chandrasekaran and V. A. Rajasekaran, "Energy-efficient cluster head using modified fuzzy logic with WOA and path selection using enhanced CSO in IoT-enabled smart agriculture systems," *The Journal of Supercomputing*, vol. 80, pp. 11149–11190, 2024, doi: 10.1007/s11227-023-05780-5.

[2] H. Ali, R. Yas, and M. Abdulameer, "Optimizing cluster head selection through improved memetic algorithm and blockchain technology for securing WSN," *Eximia*, vol. 13, no. 1, pp. 729–739, 2024, doi: 10.47577/eximia.v13i1.498.

[3] S. El Khediri, A. Selmi, R. U. Khan, T. Moulahi, and P. Lorenz, "Energy efficient cluster routing protocol for wireless sensor networks using hybrid metaheuristic approache's," *Ad Hoc Networks*, vol. 158, 2024, doi: 10.1016/j.adhoc.2024.103473.
[4] S. Regilan and L. K. Hema, "Optimizing energy efficiency and routing in wireless sensor networks through genetic algorithm-based cluster head selection in a grid-based topology," *Journal of High Speed Networks*, vol. 30, no. 4, pp. 569–582, 2024, doi: 10.3233/JHS-230209.
[5] D. Hanggoro, J. H. Windiatmaja, A. Muis, R. F. Sari, and E. Pournaras, "Energy-aware proof-of-authority: Blockchain consensus for clustered wireless sensor network," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100211, 2024, doi: 10.1016/j.bcra.2024.100211.
[6] S. S. Chauhan, G. Tanwar, R. T. Pinki, and W. A. Balaji Venkateswaran, "Data mining-based smart cluster head selection (SCHS) approach for energy efficiency in wireless sensor networks," *Journal of Computational Analysis and Applications*, vol. 33, no. 8, 2024, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/2076.
[7] A. K. Rao, K. K. Nagwanshi, and M. K. Shukla, "An optimized secure cluster-based routing protocol for IoT-based WSN structures in smart agriculture with blockchain-based integrity checking," *Peer-to-Peer Networking and Applications*, vol. 17, no. 5, pp. 3159–3181, 2024, doi: 10.1007/s12083-024-01748-1.
[8] R. Das and M. Dwivedi, "Cluster head selection and malicious node detection using large-scale energy-aware trust optimization algorithm for HWSN," *Journal of Reliable Intelligent Environments*, vol. 10, no. 1, pp. 55–71, 2024, doi: 10.1007/s40860-022-00200-6.
[9] M. Yuvaraja, S. Sureshkumar, S. J. James, and S. Thillaikkarasi, "An energy-efficient cluster head selection and secure data transmission in WSN using spider monkey optimized algorithm and hybrid cryptographic with security," *Salud, Ciencia y Tecnologia - Serie de Conferencias*, vol. 3, no. 3, p. 650, 2024, doi: 10.56294/sctconf2024650.
[10] K. W. S, A. J. Wilson, and G. Ranganathan, "Blockchain abetted energy efficient archerfish hunting and Namib Beetle optimization algorithm espoused clustering protocol for wireless sensor network," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3934–3947, 2024, doi: 10.1007/s12083-024-01787-8.
[11] V. Verma and V. K. Jha, "Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing," *Wireless Personal Communications*, vol. 134, no. 3, pp. 1665–1686, 2024, doi: 10.1007/s11277-024-10983-x.
[12] T. A. Alghamdi and N. Javaid, "Energy optimization with authentication and cost effective storage in the wireless sensor IoTs using blockchain," *Computational Intelligence*, vol. 40, no. 1, p. e12630, 2024, doi: 10.1111/coin.12630.
[13] J. Escorcia-Gutierrez *et al.*, "Privacy preserving blockchain with energy aware clustering scheme for IoT healthcare systems," *Mobile Networks and Applications*, vol. 29, no. 1, pp. 1–12, 2024, doi: 10.1007/s11036-023-02115-9.
[14] H. K. Sekhon and D. Mohita, "An enhanced data mining approach for energy efficient routing in wireless sensor networks," *International Journal of Computers & Technology*, vol. 17, no. 1, pp. 7111–7119, 2018, doi: 10.24297/ijct.v17i1.7136.
[15] U. Suriya, S. Rajendran, B. A, M. D, and P. Vidyullatha, "Enhanced lion swarm optimization and elliptic curve cryptography scheme for secure cluster head selection and malware detection in IoT-WSN," *Scientific Reports*, vol. 14, no. 1, p. 29869, 2024, doi: 10.1038/s41598-024-81038-1.
[16] M. Thurai Pandian, D. Somasundaram, H. K. Sahu, A. S. Sindhu, A. Kumaresan, and N. V. Watson, "Optimizing large-scale RFID networks with energy-efficient dynamic cluster head selection: a performance improvement approach," *IEEE Access*, vol. 12, pp. 41042–41055, 2024, doi: 10.1109/ACCESS.2024.3378528.
[17] A. Thirumalraj, R. J. Anandhi, V. Revathi, and S. Stephe, "Supply chain management using fermatean fuzzy-based decision making with ISSOA," in *Convergence of Industry 4.0 and Supply Chain Sustainability*, M. R. Khan and others, Eds. IGI Global, 2024, pp. 296–318.
[18] S. Hudda, K. Haribabu, and R. Barnwal, "Energy efficient data communication for WSN based resource constrained IoT devices," *Internet of Things (Netherlands)*, vol. 27, p. 101329, 2024, doi: 10.1016/j.iot.2024.101329.
[19] V. R. Sugumaran, E. Dinesh, R. Ramya, and E. Muniyandy, "Distributed blockchain assisted secure data aggregation scheme for risk-aware zone-based MANET," *Scientific Reports*, vol. 15, no. 1, p. 8022, 2025, doi: 10.1038/s41598-025-92656-8.
[20] S. Narla, S. Peddi, D. T. Valivarthi, S. S. Kethu, D. R. Natarajan, and D. Kurniadi, "FOG computing based energy efficient and secured IoT data sharing using SGSOA and GMCC," *Sustainable Computing: Informatics and Systems*, vol. 46, p. 101109, 2025, doi: 10.1016/j.suscom.2025.101109.
[21] T. Oh, "Blockchain-enabled security enhancement for IoT networks: integrating LEACH algorithm and distributed ledger technology," *Journal of Machine and Computing*, vol. 5, no. 1, pp. 483–495, 2025, doi: 10.53759/7669/jmc202505038.
[22] Z. Zhou, Y. He, W. Zhang, Z. Ding, B. Wu, and K. Xiao, "Blockchain-empowered cluster distillation federated learning for heterogeneous smart grids," *Information Fusion*, vol. 127. 2026, doi: 10.1016/j.inffus.2025.103913.
[23] S. Khan, M. Khan, M. A. Khan, M. A. Khan, L. Wang, and K. Wu, "A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems," *IEEE Journal of Biomedical and Health Informatics*, 2025, doi: 10.1109/JBHI.2025.3538623.
[24] S. Othmen, R. Khdhir, A. Belghith, K. Hamouid, C. Lhioui, and D. Elmourssi, "Enhancing IoT-enabled healthcare applications by efficient cluster head and path selection using fuzzy logic and enhanced particle swarm optimization," *International Journal of Communication Systems*, vol. 38, no. 3, p. e6096, 2025, doi: 10.1002/dac.6096.
[25] Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "Federated blockchain-based clustering protocol for enhanced security and connectivity in FANETs with CF-mMIMO," *IEEE Internet of Things Journal*, 2025, doi: 10.1109/JIOT.2025.3525644.
[26] N. D. Tan and V. H. Nguyen, "Machine learning meets IoT: developing an energy-efficient WSN routing protocol for enhanced network longevity," *Wireless Networks*, vol. 31, no. 4, pp. 3127–3147, 2025, doi: 10.1007/s11276-025-03934-2.
[27] B. Prince, P. Kumar, and S. K. Singh, "Multi-level clustering and prediction based energy efficient routing protocol to eliminate hotspot problem in wireless sensor networks," *Scientific Reports*, vol. 15, no. 1, p. 1122, 2025, doi: 10.1038/s41598-024-84596-6.
[28] C. Feng, A. K. Jumaah Al-Nussairi, M. H. Chyad, N. S. Sawaran Singh, J. Yu, and A. Farhadi, "AI powered blockchain framework for predictive temperature control in smart homes using wireless sensor networks and time shifted analysis," *Scientific Reports*, vol. 15, no. 1, p. 18168, 2025, doi: 10.1038/s41598-025-03146-w.
[29] A. Zamanifar, E. Nazemi, and M. Vahidi-Asl, "DSHMP-IOT: A distributed self healing movement prediction scheme for internet of things applications," *Applied Intelligence*, vol. 46, no. 3, pp. 569–589, 2017, doi: 10.1007/s10489-016-0849-0.
[30] A. Javadpour, A. K. Sangaiah, H. Zaviyeh, and F. Ja'fari, "Enhancing energy efficiency in IoT networks through fuzzy clustering and optimization," *Mobile Networks and Applications*, vol. 29, no. 5, pp. 1594–1617, 2024, doi: 10.1007/s11036-023-02273-w.

BIOGRAPHIES OF AUTHORS

Achyut Yaragal received the B.E. Degree in electronics and communication engineering from BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology (Affiliated to VTU), Vijayapura, in 2008 and the M.Tech degree in digital communication and networking from Gogte Institute of Technology (Affiliated to VTU), Belagavi in 2014. He is currently working as an assistant professor at the Department of Electronics and Communication Engineering, BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology (Affiliated to VTU), Vijayapura. His research interests include wireless sensor networks, internet of things, wireless communication, computer networks and embedded systems. He can be contacted at email: asyaragal@gmail.com and ec.asyaragal@bldeacet.ac.in.

Kirankumar Bendigeri received the B.E. degree in electronics and communication engineering from Basaveshwara Engineering College (Affiliated to VTU), Bagalkote, Karnataka, and the M.Tech. degree in digital electronics from Basaveshwara Engineering College (Affiliated to VTU) and holds a PhD in wireless sensor networks from JAIN University, Bangalore. He is currently working as an assistant professor at the Basaveshwara Engineering College, Bagalkote, Karnataka. He received a grant of 5,50,000/- Rs for the project titled "Sustainable Agriculture" form SERB-DST. He has published 20 Conferences papers and 5 journals Articles. His research interests include wireless sensor networks, internet of things and computer networks. He can be contacted at email: kiran.bendigeri@gmail.com.