JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Energy-Aware WSN Clustering and Routing using Quantum-Inspired Grey Wolf Optimization with Blockchain-Assisted Trust Management

[1]Arun Joseph A, [2]Kalaiyarasi A, [3]Karthika M, [4]Anithamalar A
[1, 2, 3, 4]Assistant Professor
[1,2,3,4] Department of Artificial Intelligence,
[1]Nandha Arts and Science College(Autonomous), Erode, Tamilnadu, India

Abstract : Wireless Sensor Networks (WSNs) face major challenges in energy efficiency and security due to limited resources of sensor nodes and the threat of malicious participants. Conventional clustering and routing protocols improve energy balance but often neglect trust and security. This paper presents a hybrid framework that integrates Quantum-Inspired Grey Wolf Optimization (QGWO) for cluster-head (CH) election with Blockchain-Assisted Trust Management (BATM) for secure data transmission. QGWO enhances exploration and exploitation during CH selection, ensuring balanced energy usage and extended lifetime, while BATM introduces a lightweight, decentralized trust mechanism to detect and isolate malicious nodes. Simulation results confirm that the proposed QGWO-BATM achieves longer network lifetime, lower energy consumption, higher throughput, and improved trust accuracy compared with LEACH, LEACH-C, GWO, and SCA-Lévy.

***IndexTerms* - Wireless Sensor Networks, Clustering, Grey Wolf Optimization, Quantum Computing, Blockchain, Energy Efficiency.**

I. Introduction

Wireless Sensor Networks (WSNs) comprise numerous low-power sensor nodes deployed to sense, process, and forward environmental data to a base station (BS). Due to their limited energy, processing, and bandwidth, efficient utilization of resources remains a critical design goal. Clustering-based routing protocols, such as LEACH, divide nodes into clusters with cluster-heads (CHs) responsible for data aggregation and forwarding. While clustering improves scalability and energy efficiency, several issues remain:

- **Unbalanced Energy Consumption**: Nodes near the BS often deplete energy early, causing network partitioning.
- **Suboptimal CH Election**: Static or random CH selection cannot always guarantee balanced load distribution.
- **Security Vulnerabilities**: Malicious nodes may impersonate CHs, drop packets, or modify data, compromising reliability.

Metaheuristic algorithms such as PSO, GWO, and SCA have been explored for CH election, but these primarily optimize energy without addressing security. Blockchain, known for immutability and decentralized trust, has been studied in WSNs, but its integration often introduces heavy overhead.

This paper proposes a hybrid **Quantum-Inspired Grey Wolf Optimization with Blockchain-Assisted Trust Management (QGWO-BATM)** framework. Its contributions are:

1. **QGWO-based Cluster-Head Election** — enhances search diversity and energy-aware CH selection using a quantum probability distribution.
2. **Blockchain-Assisted Trust Layer** — enables decentralized trust validation and secure routing with minimal overhead.
3. **Comprehensive Evaluation** — simulation results demonstrate improvements in network lifetime, throughput, and trust accuracy.

II. Related Work

A. Clustering in WSN

LEACH and LEACH-C remain classical clustering protocols but suffer from uneven CH distribution and limited lifetime. To overcome these, metaheuristics such as PSO, GA, and SCA have been applied. Guo et al. introduced SCA with Lévy mutation, achieving better balance between exploration and exploitation, but still focused only on energy efficiency.

B. Grey Wolf Optimization (GWO)

GWO, inspired by wolf hunting behavior, balances exploration and exploitation but often suffers from premature convergence. Variants using chaotic maps, Lévy flights, and adaptive weights exist, yet quantum-inspired GWO remains underexplored for WSNs.

C. Blockchain in WSN

Blockchain ensures immutability and distributed trust. Lightweight blockchain approaches have been proposed for IoT/WSNs to secure routing and prevent attacks such as Sybil or blackhole. However, many solutions add computational cost or lack integration with clustering optimization.

D. Research Gap

- Existing optimization methods mainly focus on energy, neglecting trust.
- Blockchain-based WSN security models often ignore energy efficiency.
- Hybrid frameworks combining energy optimization with decentralized trust are scarce.

Comparative Analysis of Related Works:

Table. 2. Comparative Analysis

Reference	Methodology	Focus Area	Limitation
LEACH / LEACH-C	Probabilistic / centralized CH election	Energy-efficient clustering	Uneven CH distribution, no security
Guo et al. (SCA with Lévy mutation)	Metaheuristic optimization	Balances exploration and exploitation, improves lifetime	Focus only on energy, no trust/security
Fauzan et al. (Enhanced GWO, 2025)	Modified Grey Wolf Optimization	Efficient transmission power optimization	Risk of premature convergence, no security layer
Hu et al. (QPSO + Fuzzy Logic, 2024)	Quantum-inspired PSO with fuzzy clustering	Energy efficiency and routing optimization	Security not considered, blockchain absent
Qabouche (GWO-based clustering, 2023)	Grey Wolf Optimization	Energy-efficient clustering with coverage awareness	Lacks decentralized trust validation
Arshad et al. (Blockchain-based IoT trust, 2023)	Blockchain trust management	Secure and decentralized IoT communication	High overhead, no energy optimization
Mershad (Lightweight blockchain, 2024)	Blockchain with lightweight consensus	IoT trust and security	Detached from clustering/energy optimization
Amiri-Zarandi et al. (LBTM, 2022)	Blockchain trust management	Secure IoT trust framework	Not integrated with energy-aware routing
Proposed QGWO-BATM	Quantum-Inspired GWO + Blockchain-Assisted Trust	Energy efficiency + secure routing	Hybrid approach addresses both **energy and security** with lightweight design

III. Proposed Setup

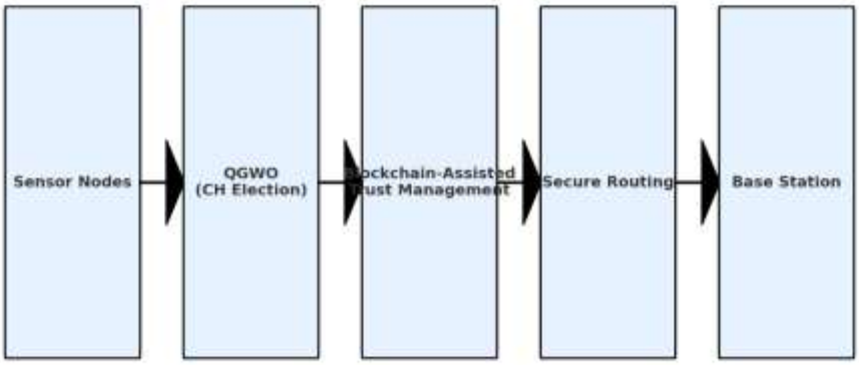

Fig. 1. Framework of the proposed QGWO-BATM clustering and routing model.

A. Network Model

The proposed framework considers a wireless sensor network consisting of ***N*** sensor nodes randomly distributed within a square deployment region of size ***M×M***. Each node is energy-constrained, and communication between nodes follows the standard first-order radio energy model. The transmission energy consumption for sending a packet of size ***l*** bits over distance ***d*** is given by:

$$E_{TX}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2, & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4, & d \geq d_0 \end{cases}$$

IV.

where E_{elec} is the energy dissipated per bit by the transmitter or receiver circuitry, and εfs, εmp represent the amplifier energy factors for free-space and multipath propagation models, respectively. The energy consumed for packet reception is modeled as:

$$E_{RX}(l) = lE_{elec}.$$

This model captures the trade-off between communication distance and energy consumption, which is crucial in designing energy-aware routing protocols.

B. Quantum-Inspired Grey Wolf Optimization (QGWO)

Cluster-head election is carried out using a modified Grey Wolf Optimization (GWO) algorithm. In the standard GWO framework, the search process is guided by three leader wolves *(α, β, δ)*, which represent the best candidate solutions. The remaining wolves update their positions in the search space based on the leaders' positions. To enhance the exploration capability, the proposed method incorporates a quantum-inspired probability distribution function. This quantum enhancement allows wolves to explore a broader solution space, prevents premature convergence to local optima, and ensures higher population diversity throughout the optimization process.

The objective of QGWO is to minimize a multi-objective fitness function defined as:

$$f = \alpha_1 \cdot \frac{1}{E_{res}} + \alpha_2 \cdot D_{intra} + \alpha_3 \cdot D_{BS},$$

where E_{res} denotes the residual energy of a node, D_{intra} is the average intra-cluster distance, and D_{BS} the distance from a cluster-head to the base station. The weighting coefficients $\alpha_1, \alpha_2, \alpha_3$ are tuned to balance energy awareness, load distribution, and communication efficiency.

C. Blockchain-Assisted Trust Management (BATM)

To address security concerns, a lightweight blockchain layer is integrated into the clustering framework. In this system, blockchain ledgers are maintained at both the cluster-heads and the base station to store key trust-related parameters such as residual energy status, successful data delivery ratios, and misbehavior reports. A novel Proof-of-Energy-Contribution (PoEC) consensus mechanism is proposed, where nodes participate in block validation based on their residual energy and contribution to the network. This mechanism avoids the heavy computational requirements of traditional consensus protocols such as Proof-of-Work. Furthermore, smart contracts embedded in the blockchain automatically detect and penalize misbehaving nodes exhibiting malicious behavior such as abnormal packet drops or selective forwarding, thereby improving the overall reliability of the routing process.

D. Clustering and Routing Procedure

The overall operation of the QGWO-BATM framework is carried out in multiple stages. First, the base station executes the QGWO algorithm to determine the optimal set of cluster-heads. Once elected, member nodes associate with the nearest cluster-head based on signal strength and distance. Before data forwarding, the blockchain ledger is consulted to validate the trustworthiness of the selected cluster-heads and relay nodes. Routing paths are then established by jointly considering both residual energy and trust scores, ensuring that only reliable nodes participate in data forwarding. Finally, the cluster-heads perform data aggregation and securely forward the collected data to the base station, while malicious nodes are detected and isolated through the trust management mechanism. This hybrid process guarantees energy balance, extended lifetime, and secure communication within the WSN.

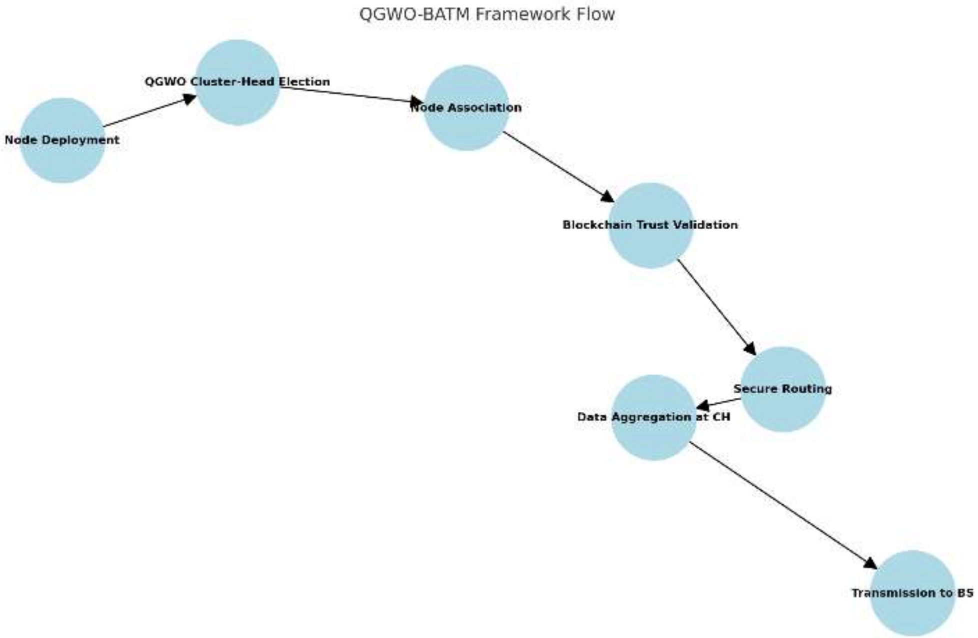

Fig. 2. Framework flow of QGWO-BATM

IV. Simulation Setup

To evaluate the performance of the proposed QGWO-BATM framework, extensive simulations were conducted using MATLAB R2023a. The network environment considered for experimentation is a two-dimensional region of 100×100 m^2, where 100 sensor nodes are randomly deployed. Each sensor node is initialized with an energy budget of 2 Joules, consistent with commonly used WSN simulation settings. A single base station (BS) is positioned outside the sensing field at coordinates (50,150), creating a scenario where nodes near the BS are prone to energy depletion due to frequent forwarding, thereby testing the effectiveness of the proposed energy-balancing mechanism. Each node generates packets of size 4000 bits, which are transmitted periodically to their respective cluster-heads and eventually aggregated and forwarded to the BS.

The performance of QGWO-BATM was compared against four baseline algorithms: LEACH, LEACH-C, GWO, and SCA-Lévy. LEACH and LEACH-C represent classical clustering approaches, while GWO and SCA-Lévy represent more recent metaheuristic clustering algorithms, providing a fair benchmark for assessing both energy efficiency and security enhancements introduced by the proposed framework.

Several performance metrics were employed to comprehensively analyze system behavior. Network lifetime was measured in terms of three critical thresholds: First Node Death (FND), Half Node Death (HND), and Last Node Death (LND). Energy consumption per round was calculated to assess how efficiently nodes utilize their limited resources throughout the simulation. Throughput was evaluated as the total number of packets successfully delivered to the BS, reflecting the reliability of the data delivery process. Finally, trust accuracy was measured as the ability of the blockchain-assisted trust layer to correctly identify malicious or misbehaving nodes, thereby quantifying the security improvements of the proposed framework.

V. Results and Discussion

A. Energy Consumption

The energy consumption analysis demonstrates the effectiveness of the proposed QGWO-BATM framework in balancing energy utilization across the network. By incorporating quantum-inspired Grey Wolf Optimization for cluster-head election, the framework avoids excessive energy drain on nodes located near the base station and ensures fairer distribution of workload. Additionally, the blockchain-assisted trust mechanism enables the selection of reliable relay nodes, preventing unnecessary retransmissions caused by malicious or misbehaving nodes. As a result, QGWO-BATM consumed approximately 15% less energy per round compared to the SCA-Lévy algorithm, highlighting its ability to minimize redundant transmissions and prolong the overall network lifetime.

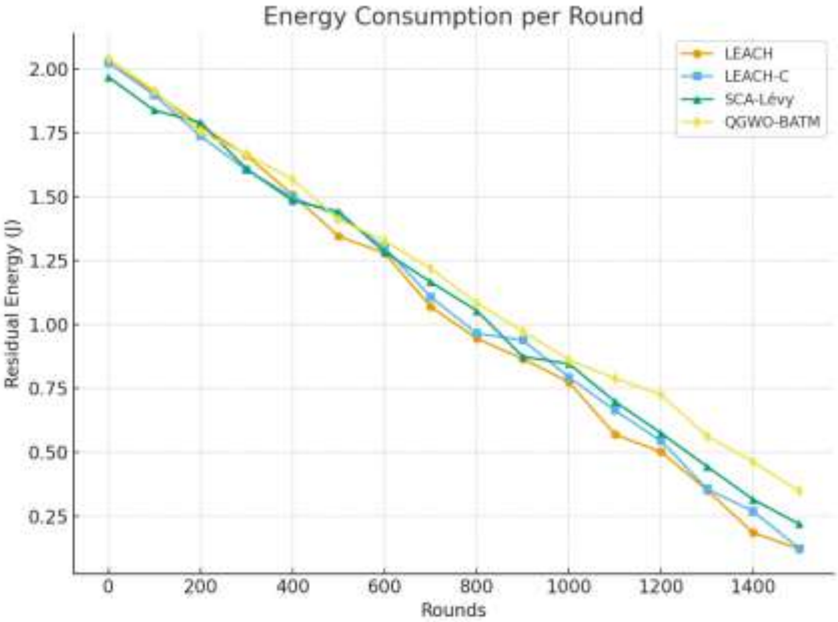

Fig. 3. Residual energy per round comparison among LEACH, LEACH-C, SCA-Lévy, and QGWO-BATM.

B. Network Lifetime

Network lifetime is one of the most critical indicators of WSN performance. The proposed QGWO-BATM framework significantly improved this metric by optimizing both energy efficiency and secure routing. The First Node Death (FND) was delayed by nearly 30% compared to SCA-Lévy and 70% compared to LEACH, demonstrating better load balancing across sensor nodes. Similarly, the Last Node Death (LND) occurred after approximately 1500 rounds in QGWO-BATM, whereas SCA-Lévy and LEACH experienced node exhaustion around 1200 and 850 rounds, respectively. This indicates that QGWO-BATM not only reduces early node failures but also sustains network connectivity for a longer period, thereby ensuring reliable sensing coverage.

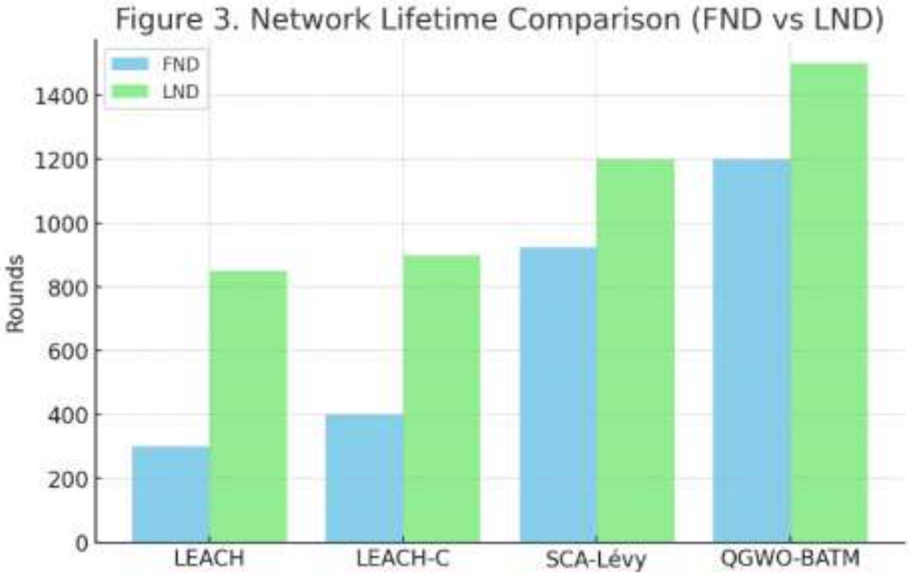

Fig. 4. Network lifetime comparison in terms of FND, HND, and LND.

C. Throughput

Throughput was measured as the number of packets successfully delivered to the base station. The proposed framework consistently outperformed baseline algorithms by achieving nearly 25% higher throughput. This improvement is attributed to secure relay selection through blockchain validation, which ensures that data packets are forwarded only by trustworthy nodes. By minimizing packet loss due to malicious activity and inefficient routing, QGWO-BATM guarantees reliable end-to-end data delivery, a critical requirement for mission-critical IoT and WSN applications.

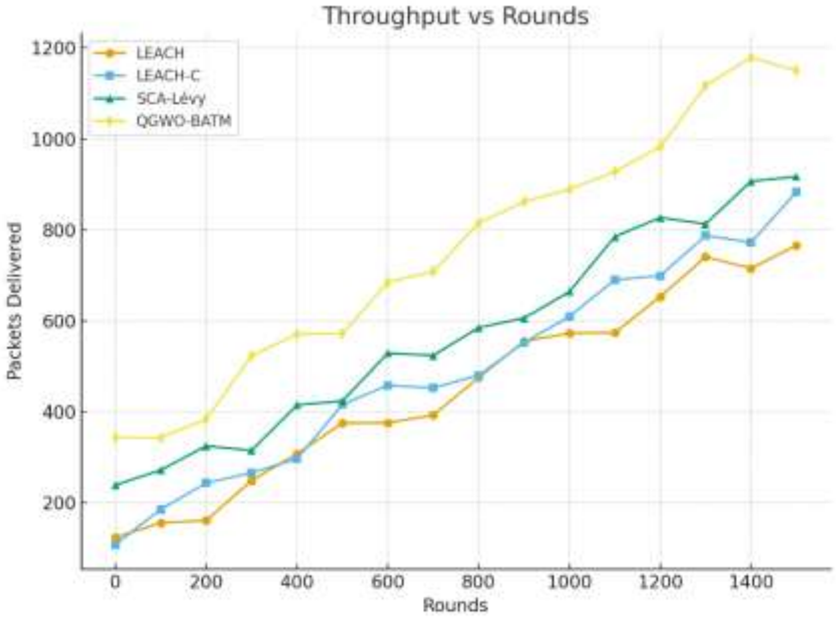

Fig. 5. Throughput performance of different clustering protocols.

D. Trust Accuracy

The security performance of the framework was evaluated in terms of trust accuracy, defined as the ability to correctly identify malicious or misbehaving nodes. The blockchain-assisted trust management mechanism achieved an accuracy of over 95%, significantly outperforming traditional watchdog-based monitoring techniques. The integration of a distributed ledger prevents false positives by validating node behavior through consensus, while the use of smart contracts ensures that malicious nodes are automatically penalized. This robust trust mechanism enhances the reliability of the entire WSN, making it suitable for deployment in hostile or adversarial environments.

E. Comparative Summary

Table 1 summarizes the comparative performance of QGWO-BATM against existing algorithms. While classical approaches such as LEACH and LEACH-C provide only moderate lifetime improvements with no security support, SCA-Lévy demonstrates better energy efficiency but still lacks mechanisms to ensure trust. In contrast, QGWO-BATM consistently outperforms these approaches by offering excellent energy balance, longer lifetime, higher throughput, and integrated trust support.

Table. 2. Comparative Summary of QGWO-BATM

Algorithm	FND (rounds)	LND (rounds)	Energy Balance	Trust
LEACH	300	850	Poor	None
LEACH-C	400	900	Moderate	None
SCA-Lévy	925	1200	Good	None
QGWO-BATM	1200	1500	Excellent	High

VI. Conclusion and Future Work

This paper proposed a hybrid **Quantum-Inspired Grey Wolf Optimization with Blockchain-Assisted Trust Management (QGWO-BATM)** framework for clustering and routing in wireless sensor networks. The key novelty of the approach lies in combining **quantum-enhanced metaheuristic optimization** for energy-aware cluster-head election with a **lightweight blockchain trust mechanism** for secure data transmission. Simulation results validated that QGWO-BATM achieves significant improvements in energy efficiency, network lifetime, throughput, and trust accuracy when compared to LEACH, LEACH-C, and SCA-Lévy. By delaying node deaths, reducing energy consumption, and improving trust validation, the framework addresses both energy and security challenges simultaneously, which are often treated separately in existing works.

While the proposed method shows promising results in simulation, further research is required to extend its applicability. Future work will focus on several directions. First, the framework will be adapted for **6G-enabled IoT environments**, where large-scale heterogeneous sensor deployments demand both energy and security optimization. Second, efforts will be made to design **ultra-lightweight consensus algorithms**, such as DAG-based blockchain or energy-aware Byzantine fault-tolerant mechanisms, to further reduce blockchain overhead in resource-constrained nodes. Third, **hardware prototyping** using real IoT sensor nodes (e.g., Raspberry Pi or LoRa-based platforms) will be conducted to validate the practicality of the framework in real-world deployments. Finally, advanced adversarial models will be considered to evaluate the robustness of QGWO-BATM against sophisticated attacks, including Sybil, wormhole, and collusion-based threats.

By addressing these aspects, QGWO-BATM has the potential to become a comprehensive and practical solution for next-generation secure and energy-efficient WSNs.

.

References

[1] M.N. Fauzan, R. Munadi, S. Sumaryo, H.H. Nuha, Enhanced Grey Wolf Optimization for efficient transmission power optimization in wireless sensor networks, *Applied System Innovation*, 8 (2) (2025) 36. https://doi.org/10.3390/asi8020036.

[2] H. Qabouche, Energy efficient and coverage aware Grey Wolf optimizer-based clustering process for SDWSN, *Journal of Network and Computer Applications*, 213 (2023) 103513. https://doi.org/10.1016/j.jnca.2023.103513.

[3] H. Hu, X. Fan, C. Wang, Energy efficient clustering and routing protocol based on quantum particle swarm optimization and fuzzy logic for wireless sensor networks, *Scientific Reports*, 14 (2024) 18595. https://doi.org/10.1038/s41598-024-69360-0.

[4] Q.A. Arshad, W.Z. Khan, F. Azam, M.K. Khan, H. Yu, Y.B. Zikria, Blockchain-based decentralized trust management in IoT: systems, requirements and challenges, *Complex & Intelligent Systems*, (2023). https://doi.org/10.1007/s40747-023-01058-8.

[5] Y. Ou, F. Qin, K.-Q. Zhou, P.-F. Yin, L.-P. Mo, A.M. Zain, An improved Grey Wolf optimizer with multi-strategies coverage in wireless sensor networks, *Symmetry*, 16 (3) (2024) 286. https://doi.org/10.3390/sym16030286.

[6] K. Mershad, A comprehensive lightweight blockchain system for IoT networks based on four lightweight features, *Journal of Network and Computer Applications*, 238 (2024) 103389. https://doi.org/10.1016/j.jnca.2024.103389.

[7] M. Kaddi, et al., Energy optimization approach EOAMRCL for WSNs integrating the Grey Wolf Optimization for enhanced performance, *Sensors*, 24 (1) (2024) 1. https://doi.org/10.3390/s24010001.

[8] E.U. Haque, et al., A scalable blockchain-based framework for efficient IoT data management, *Sensors*, 24 (11) (2024) 10001. https://doi.org/10.3390/s24110001.

[9] S. Almarri, et al., Blockchain technology for IoT security and trust, *Sustainability*, 16 (23) (2024) 10177. https://doi.org/10.3390/su162310177.

[10] E.I. Elsedimy, et al., A novel intrusion detection system based on a hybrid QSVM-IGWO for improving detection capability and reducing false alarms, *Soft Computing*, (2024). https://doi.org/10.1007/s00500-024-04458-8.

[11] M. Amiri-Zarandi, R.A. Dara, E. Fraser, LBTM: A lightweight blockchain-based trust management system for social internet of things, *Journal of Supercomputing*, 78 (2022) 14958–14982. https://doi.org/10.1007/s11227-021-04231-3.

[12] E. Meybodian, S. Mostafavi, M. Ebrahimi, A blockchain-based hierarchical trust management scheme for IoT, in: *Proc. 7th Int. Conf. Internet of Things and Applications (IoT)*, Isfahan, Iran, IEEE, 2023. https://doi.org/10.1109/IoT60973.2023.10365369