RESEARCH PAPER

Design of an Incremental Graph-Based Routing Model for Enhancing QoS of Dense IoMT Networks, using Truncated Side Chains

Prof. Radhika P. Fuke[1], Dr. Rekha Ranawat[2]

[1]Assistant Professor, Department of Information Technology, PRMIT&R Badnera. (Corresponding Author) Email: radhika.fuke@gmail.com

[2]Associate Professor, Department of IAC, SAGE University Indore. Email: rekharathore23@gmail.com

***Corresponding author: Prof. Radhika P. Fuke, Assistant Professor, Department of Information Technology, PRMIT&R Badnera**

Email: radhika.fuke@gmail.com

Received: 25th May, 2026; **Revised:** 6th June, 2026; **Accepted:** 8th June, 2026; **Available Online:** 09th June, 2026

ABSTRACT

The expansion of the IoMT domain is fast-paced, resulting in the development of a pressing demand for intelligent routing techniques capable of effectively addressing network congestion issues by providing high levels of QoS and safeguarding sensitive healthcare data transmission processes. Modern health facilities employ multiple medical devices that constantly produce and transfer important medical data, making communication between these devices indispensable in practice. Nevertheless, the currently available routing strategies frequently do not sufficiently account for the spatio-temporal characteristics of network nodes and ensure data routing security. Therefore, this study aims to design an incrementally improved graph-based routing scheme that improves the quality of service in densely populated IoMT environments based on the truncated sidechain technique. This scheme accounts for the spatial and temporal properties of network nodes and employs a hybrid optimization algorithm comprising a combination of the Teacher–Learner-based Firefly Optimization Algorithm and Graph-based Q-Learning for calculating optimal routes. Furthermore, the truncated sidechain technique is utilized to improve the security of transmitted medical data, and the Grey Wolf–Whale Optimization algorithm is used to find the best length of the sidechain by a Fuzzy Analytic Hierarchy Process approach. The results of experimentation are showing clearly that the suggested model gives better efficiency due to five different aspects which are reducing the communication time delay by 10.5%, enhancing the energy efficiency by 8.5%, improving the throughput by 3.9% and increasing the packet delivery rate by 1.5% and decreasing the jitter rate by 8.3%. The system has been proved to properly function to make the IoT routing process secure and efficient by enhancing the performance of blockchain through three distinctive reductions in energy consumption which include 5.9% reduction in the mining energy consumption, 4.9% reduction in the storage energy consumption, and 12.5% reduction in the mining time.

Keywords: IoT Networks, Graph Based Q Learning, Elk Kernel with Truncated Sidechains, Teacher Learner Based Firefly Optimization, Grey Wolf Whale Optimization.

How to cite this article: Fuke RP, Ranawat R. Design of an Incremental Graph-Based Routing Model for Enhancing QoS of Dense IoMT Networks, using Truncated Side Chains. Int J Drug Deliv Technol. 2026;16(57s): 1492-1511. DOI: 10.25258/ijddt.16.57s.152

Source of support: Nil.

Conflict of interest: None.

Introduction

(IoMT) has introduced a paradigm shift in the modern health care systems through the provision of real time continuous monitoring of patients with medical devices that can interact and process intelligent data that aids clinicians in making better decision-making processes. IoT technology in the form of IoMT uses connected medical sensors, wearable medical sensors and advanced medical equipment that enable collection and transmission and processing of relevant medical data which helps clinicians improve their diagnostic, treatment, and preventative medical practices. The increasing number of connected devices and their fluctuating operational patterns in IoMT environments create substantial difficulties for network administrators because they must sustain Quality of Service (QoS) standards while processing substantial amounts of sensitive medical information which requires immediate attention. The existing routing methods fall short of meeting the demands of complex network environments because they cannot properly identify and use both spatial links and temporal patterns that exist between network elements which causes suboptimal path selection and longer processing times and decreased network efficiency. The Trust and Reputation System (TRS) routing methods provide improved routing reliability but they struggle to adapt to fast changing healthcare environments while failing to meet the demands

of strong routing systems that need to scale and operate with advanced intelligence. The traditional routing methods create problems for data security together with patient privacy protection because standard security methods fail to safeguard IoMT systems against developing cyber threats and unauthorized access and data manipulation dangers.

The study presents a new routing system named the IGRMQITS to solve essential problems which occur in crowded Internet of Medical Things networks. The suggested framework employs an integrated strategy that integrates spatial and temporal information about network nodes to optimize routing efficiency and decision-making procedures. The framework applies Graph-based Q-Learning (GQL), which is the fundamental component of the intelligent framework that enables it to develop an adaptive intelligent framework to automatically discover new pathways based on the changing states of the network. The system applies an optimized hybrid approach, which employs Teacher-Learner Firefly Optimizer (TLFFO) to explore the network space in discovering the best communication pathways while ensuring equilibrium between exploration and exploitation operations. The framework uses Blockchain-Driven Deep Traffic Pattern Analysis (BDDTPA) to track network traffic trends, which is essential in traffic control and system performance improvement in IoMT frameworks.

The security enhancement strategy in the proposed framework provides the main novelty of the system through the application of the truncated sidechain structure that makes it possible to process routing and healthcare information in a secure manner. The strategy provides for the protection of data integrity in a way that shields the system from malicious attacks but does not affect the efficiency of communication in the network. The GWWO method is used to determine the optimal sidechain length since it offers a way to build a secure system with sufficient effectiveness. The FAHP technique ensures the timely modification of sidechain parameters in the light of new conditions for health care privacy and performance. The multi-tiered security system provides for the safety of IoMT networks through efficient system performance. The experiment on the proposed IGRMQITS model shows significant improvements in various performance metrics. The results show that the system reduces the communication delay by 10.5%, increases the energy efficiency by 8.5%, increases throughput by 3.9%, 1.5%, and reduces network jitter by 8.3%, which indicates better network stability and responsiveness. Incorporation of blockchain-based security protection improves the system's operational efficiency by decreasing mining duration by 12.5%, energy needs by 5.9% and storage demands by 4.9%, thereby successfully reducing computing and resource expenses. The proposed framework demonstrates the improvement of the security and system performance in several enhancements throughout IoMT networks

Motivation

Introduction

The IoMT technology is one of the innovative technologies that have been embraced by the modern healthcare sector. This technology enables patient monitoring through real-time data transmission from wearable health devices. Wearable medical devices transmit data through networks of connected monitoring systems. The interconnected monitoring systems allow vast amounts of data sharing between different medical devices. The existing system needs to improve its data management performance while ensuring safe communication and fulfilling two requirements which involve maintaining high Quality of Service (QoS) and established performance standards. The current situation becomes more difficult because high-density IoMT environments contain multiple devices that operate together. The existing routing methods do not use spatial and temporal node information properly which leads to incorrect path selection and network congestion issues that reduce operational efficiency. Today's security systems lack adequate strength to protect medical data from modern cyber threats and data breaches and privacy violations. The current situation requires development of an advanced routing system which will improve network performance while keeping communication secure. The goal of the research work is to propose a novel IoMT routing algorithm integrating machine learning routing approaches, advanced optimization techniques, and blockchain security features to enable safe and effective information transfer in healthcare settings

.

Contributions

Some of the key contributions from this research work towards improving the IoMT network security and routing efficiency include:

Design of IGRMQITS Framework:

The research paper presents a unique routing framework referred to as IGRM for QoS Improvement in Dense IoMT Networks with Truncated Sidechains. The technique intends to solve various routing issues that occur within

the IoMT network comprising multiple medical devices.

Using Spatial–Temporal Node Features:

The proposed model implements a Graph-based Q-Learning (GQL) method to analyze the spatial and temporal node characteristics of its nodes. The routing system uses this information to create optimal data transmission methods which improve network performance.

Using TLFFO to improve routes:

The model implements Teacher–Learner based Firefly Optimisation (TLFFO) as its routing optimization method. The optimization method improves route selection because it uses the entire network search area to conduct its searching activities which leads to enhanced communication results. • Safe Data Transmission with Truncated Sidechains:

The framework employs a secure truncated sidechain system to protect both routing data and medical information. The Grey Wolf Whale Optimiser (GWWO) determines the optimal length of sidechains while the Fuzzy Analytic Hierarchy Process (FAHP) dynamically adjusts sidechains to fulfill security and privacy requirements.

Better Network Performance:

The testing process demonstrated that network performance metrics experienced significant improvements. The proposed system achieves a 10.5% reduction in communication delays which results in an8.5% improvement in energy efficiency and a3.9% throughput increase and a 1.5% packet delivery ratio enhancement and an 8.3% network jitter reduction. The framework improves blockchain operations by decreasing mining time by12.5% and reducing mining energy expenses by5.9% and lowering mining storage needs by4.9%.

The proposed framework provides a successful method to enhance routing efficiency throughout the network. Improve QoS, and keep data safe in dense IoMT networks. The study establishes a foundation for developing advanced smart healthcare networking systems which will promote secure medical networking operations in the future.

Literature Review

The IoMT has expanded rapidly during the past several years to become a critical component of contemporary healthcare systems. IoMT enables continuous data collection together with real-time patient monitoring through its integration of medical sensors with wearable devices and monitoring systems and healthcare management platforms. Healthcare organizations are increasingly adopting Internet of Medical Things networks to support diagnostic processes and develop treatment strategies and perform patient care management as medical devices gain connectivity. Organizations that handle rapid technological expansion face challenges because they need to maintain efficient data routing and network reliability while protecting medical data. Researchers have dedicated their efforts to developing advanced routing solutions and secure communication systems which can manage the extensive data generated by Internet of Medical Things environments.

The proper operation of IoMT systems depends on the optimal routing of medical sensors, monitoring devices, gateways, and healthcare servers to ensure active communication between their components. The routing mechanism decides how medical data moves across the network and has a direct effect on the overall Quality of Service (QoS).Different routing methods exist which researchers have proposed to enhance network performance based on their research findings. The energy consumption of network nodes determined which communication paths early routing methods would select. The methods were designed to extend the operational life of IoMT devices through their power-saving communication capabilities. The strategies succeeded in reducing power consumption, but their implementation led to extended communication delays which caused a decline in service quality. The increased delays which occur during healthcare operations which need immediate data transfer will disrupt both patient monitoring systems and emergency response systems.. Researchers investigated the application of machine learning-based routing methodologies because they needed to solve their existing limitations. The intelligent routing systems examined current network conditions to determine optimal data transmission paths. The application of machine learning methods improved routing efficiency but most methods failed to consider both temporal dynamics and spatial characteristics. Devices in IoMT networks demonstrate high dynamicity because they switch between various operational states. The factors must be included in the routing process because their absence will create routing decisions that lead to inefficient network operation. The research that was conducted recently studied two methods which included graph-based network modeling and deep reinforcement learning to develop better methods for representing IoMT network systems. Graph-based approaches model the network through nodes which connect to each

other via links. The system provides users with successful results when they search for optimal routing paths. Deep reinforcement learning techniques enhance the routing process through their ability to adjust routing decisions based on current network conditions. The advanced models used for routing work better than their predecessors but their ability to optimize large IoMT networks which experience rapid changes remains insufficient.

The IoMT networks within the healthcare industry face two main challenges which need to be solved because they handle highly confidential medical data. Secure transmission methods should protect medical records and patient monitoring data and diagnostic results from unauthorized access and data alterations. Researchers have studied blockchain solution for securing IoMT communication systems since it effectively addresses their security problems. The decentralized system of blockchain technology delivers its benefits by generating permanent data records which may be verified through simple procedures. Blockchain technology functions as an efficient security measure which safeguards healthcare data in distributed network environments.

The implementation of Internet of Medical Things environments together with standard blockchain systems creates various technical problems. Standard blockchain systems require basic operational needs which IoMT networks cannot meet because their operations need high computational power and large storage space. Network communication delays result from additional tasks which need to be performed thus decreasing the total efficiency of the network. Researchers have developed truncated blockchain models which reduce their storage and processing requirements by maintaining only essential blockchain blocks to address existing challenges. Truncated blockchain frameworks can help lower costs but they often don't have good ways to figure out the best truncation length to use to balance performance and security.

Optimisation algorithms were introduced in subsequent research to determine optimal truncation settings which improved blockchain performance. The methods used for blockchain performance enhancement did not satisfy essential prerequisites needed in healthcare settings which required secure handling of confidential medical data. Healthcare organizations require different privacy measures for various health data categories which blockchain systems must adapt to deliver privacy protection at different levels.

Research in this area explores the integration of graph-based routing techniques and blockchain-based security systems. Researchers developed hybrid frameworks that generated solutions to enhance routing efficiency while ensuring data security. The developed methods increased network reliability and user protection but required more processing resources due to their dependence on blockchain operations. Next research studies applied graph-based routing techniques with blockchain systems that work with reduced capacity to achieve better performance results. The new solutions provided significant improvements over the previous methods, but did not have enough mechanisms to select the best truncation settings under the user privacy requirements.

Researchers have introduced a new framework called the IGRM for QoS Enhancement in Dense Internet of Medical Things Networks. The system employs smart routing along with a secure blockchain system that the developers built for dense Internet of Medical Things environments. The model employs the Graph-based Q-learning algorithm which controls the routing process to establish communication routes between the nodes of the network based on their spatial and temporal locations. The approach helps the system to identify the most efficient ways of communication which reduces the delay and improves the overall performance of the network. The optimization approach in the framework uses Teacher-Learner based Firefly Optimization (TLFFO) algorithm that makes the routing process more efficient.. The system can manage high-volume network traffic that enters and exits the system. The proposed model not only enhances the routing performance but also guarantees data security with improved security measures. The researchers suggest a truncated sidechain architecture that allows blockchain systems to run efficiently with lower unnecessary processing needs. The GWWO enables us to discover the optimal sidechain lengths needed to meet the security requirements, while simultaneously reducing operational costs. This paper presents the application of a AHP to evaluate various levels of data privacy and to identify suitable security measures for sensitive health data.

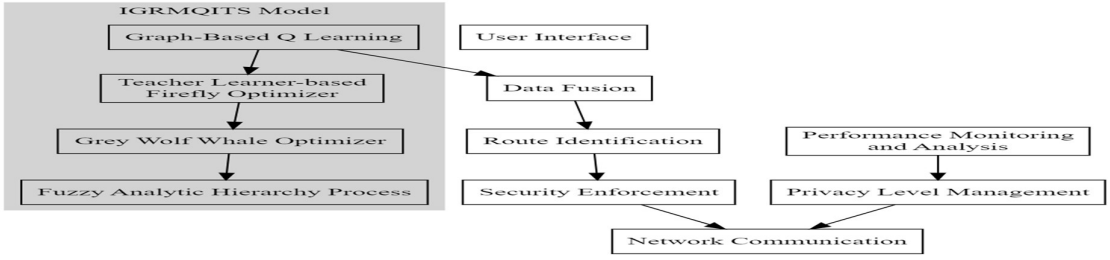
Previous works have made great progress in two fields which are routing of IoMT and security of blockchain. The researchers have to solve multiple challenges which prevent them to develop efficient networks that can handle increased traffic while maintaining user privacy. We propose the IGRMQITS framework that overcomes the challenges by implementing advanced routing algorithms, optimization methods, and blockchain based security measures. The framework enhances

routing efficiency by providing better network performance and service delivery and protecting data security in busy IoMT environments. The proposed model provides a strong basis to develop secure intelligent healthcare communication systems using IoMT.

2. Proposed Design of an IGMR for improving QoS using truncated sidechains

The present IoMT network routing models reveal that there are several research methodologies that involve the need for sophisticated computing resources to provide real-time performance while their present condition is not ideal for practical healthcare scenarios. The clinical IoMT system requires consistent communication along with speedy data transfer capabilities that hospitals and other medical organizations demand to monitor patients and make healthcare decisions. This section provides a solution for the above issues by proposing an Incremental Graph-based Routing Model with Truncated Sidechains. The proposed model generates QoS improvements that improve the IoMT network systems operating in highly populated regions. The Incremental Graph-based Routing Model makes use of the TLFFO algorithm to optimize the route, which can be seen in Figures 1 and 2 below.The optimisation method uses Graph-based Q-Learning (GQL) to identify optimum communication routes through efficient spatial and temporal network node utilization. The framework uses routing optimisation together with a truncated sidechain security mechanism to ensure secure data transmission. The Grey Wolf Whale Optimiser (GWWO) algorithm determines the optimal length of sidechain which maintains security requirements while supporting network operations. The Fuzzy Analytic Hierarchy Process (FAHP) transforms the sidechain structure according to specific privacy requirements. The security framework for IoMT applications operating in real-time environments receives enhanced protection through this development. The proposed model begins with the calculation of an iterative spatial-temporal trust value which Equation (1) describes. The Teacher-Learner based Firefly Optimisation (TLFFO) process uses this value to discover optimal routes.

$$\backslash ISTT(i) = \frac{e(i)}{NC}\sum_{j=1}^{NC}\frac{THR(j)*PDR(j)}{D(j)*E(j)} \ldots (1)$$



Time-based Metric Estimation

Let i be the index of a node and e be residual energy of a node. THR, PDR, D and E are the parameters of temporal throughput, packet delivery ratio, communication delay and energy consumption respectively. The values of these temporal parameters are determined by the following calculation method.

$$THR = \frac{P_{Rx}}{D} \quad (2)$$

$$PDR = \frac{P_{Rx}}{P_{Tx}} \quad (3)$$

$$D = ts(Rx) - ts(Tx) \quad (4)$$

$$E = e(Tx) - e(Rx) \quad (5)$$

TLFFO-based Route Generation

After computing the temporal metrics, the TLFFO generates a population of NP particles, where each particle represents a potential routing path consisting of N stochastic nodes between the source and destination.

$$N = STOCH(1, N_{(s,d)}) \quad (6)$$

where $N_{(s,d)}$represents the total number of nodes between the source and destination nodes.

The node selection condition is ensured using:

Particle Fitness Evaluation

The TLFFO algorithm calculates the fitness of each particle as:

$$f_p = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{ISTT(i)+ISTT(j)}{d(i,j)} \quad (8)$$

After generating NP particles, the fitness threshold is computed as:

$$f_{th} = \frac{1}{NP}\sum_{i=1}^{NP} f_p\,(i) \times LP \quad (9)$$

where **LP** denotes the learning parameter.
Particles are categorized as follows:
$f_p > 2f_{th}$→ **Teacher particles**
$f_p > f_{th}$→ **Student particles**
$f_p \leq f_{th}$→ **Fireflies with low brightness**
Student particles update their routing paths using teacher particles as:
$N_{new} = N_{student} \cup N_i where i = STOCH(1, N_{teacher})$ (10)

Low-fitness particles are regenerated using Equations (6)–(8). This process continues for **NI iterations**, and finally the routing paths with $f_p \geq 2f_{th}$ are selected as optimal candidate routes.

Graph-based Q-Learning Model

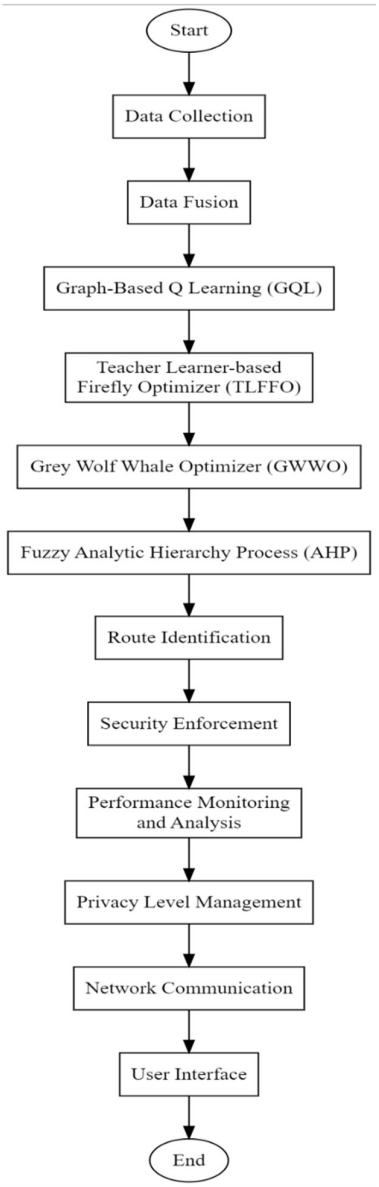
The selected routes are then processed by the Graph-based Q-Learning (GQL) model to determine the final optimal routing path.
The IoMT network is represented as a graph:
.

$$G = (V, E) \quad (11)$$

where
V represents the set of nodes
E represents communication links between nodes.
Each edge $e \in E$ is assigned a transmission cost calculated as:

$$w_e = \alpha_1 L_e + \alpha_2 \frac{1}{B_e} + \alpha_3 E_e \quad (12)$$

where
L_e= latency of the link
B_e= bandwidth of the link
E_e= error rate
$\alpha_1, \alpha_2, \alpha_3$= weighting coefficients
These coefficients are determined empirically based on the QoS requirements of the IoMT network



The model uses Q learning with the Q value function, Q(s,a), where s is the current state of the network and an is actions that include selecting paths between the current and subsequent nodes. The importance of the Q value function in this case is that it helps to determine action an at state s. The update rule of the Q value function is written as equation 13,

The learning process depends on two factors since the learning rate α controls how much new data will replace existing knowledge and the immediate reward r in state s and the discount factor γ determines how much current rewards will be discounted against future rewards and s represents the new state which results from taking action a while a prime denotes all possible actions that can be done after reaching state s prime through different paths.

The immediate reward r should be based on the most prominent network priorities since it is the primary reward for the sets of the IoMT network. The value of measurement w should decrease with the increase of the edge weight because paths should provide higher rewards.

In IoMT scenario, state representation needs to consider the current network load distribution, existing path QoS metrics and the operational status of its nodes. The actions allow moving from one node to another by using the graph edges. Graph exploration is needed for the learning process and the Q Values are updated based on state transitions and rewards acquired from experiences. The policy π for every state defines the action that has to be taken among the

possible actions using the Q Values. 14. pi(s)=argmaxaQ(s,a)…(14) The policy is written in the form of the equation.

The evaluation process is of utmost importance as it determines the best path to obtain the highest Q Value in all states, resulting in optimal network performance and resource distribution for IoMT systems. The model adapts its α and γ values dynamically which shows its ability to adapt to different network conditions and transmission requirements which are essential for medical usage. The model outputs its final output through the paths indicated by π with the highest Q Values required by the current network state, ensuring that data routing through the selected paths will be most effective under the current network conditions.

In this paper, we propose a new truncated sidechaining model which uses GWWO to select optimal sidechain lengths to achieve data security on selected routes with higher QoS. First the Wolves, Each Wolf Corresponds to Length of Sidechains. These Wolves are constructed as in Equation 15.

$$fw = \frac{1}{ND}\sum_{i=1}^{ND}\frac{TM(i)}{dm(i) * em(i)} \dots (16)$$

The model then repeats this process for NW Wolves and calculates an Iterative Fitness Threshold using equation 17,

$$if(th) = \frac{\sum_{i=1}^{NW} fw(i) * LW}{NW} \dots (17)$$

$$L(SC, Beta) = \frac{L(SC, Beta) + \sum_{i=1}^{N(Alpha)} L(SC, i)}{N(Alpha) + 1} \dots (18)$$

Where N(Alpha) = Number of Alpha Wolves in this process. Similarly, Wolves having fw>2*if(th) are Marked as 'Gamma' Wolves and their configuration is updated by equation 19,

$$L(SC, Gamma) = \frac{L(SC, Gamma) + \sum_{i=1}^{N(Beta)} L(SC, i)}{N(Beta) + 1} \dots (19)$$

Wolves with fw>if(th) are Marked as 'Delta' Wolves and their configuration is updated as per equation 20,

$$L(SC, Delta) = \frac{L(SC, Delta) + \sum_{i=1}^{N(Gamma)} L(SC, i)}{N(Gamma) + 1} \dots (20)$$

The Wolves receive the designation of 'Whales' and their regeneration occurs through equations 15 and 16 which belong to the Next Iteration Sets that facilitate the integration of stochastic updates into this system. The process executes for NI Iterations and GWWO selects the Wolf Configuration with highest fitness after the final iteration to use it for segregating the current blockchain into sidechains. The system resumes its operations whenever the condition described in equation 21 gets fulfilled.

$$\frac{dm(i+1) * em(i+1)}{dm(i) * em(i)} > fth(s) \dots (21)$$

The fitness threshold of sidechaining fth(s) lies between two conditions since scientists concluded that fth(s) was equal to 2 in solving the issue of mining delay and power consumption that leads to unexpected jumps. These chosen sidechains are subsequently truncated by employing the fuzzy Analytic Hierarchy Process (AHP), which focuses on various degrees of privacy, thus, providing a secure system for real-time networks. In the presented model of FAHP, there is a systematic truncation of sidechains generated from the main blockchain network according to the predetermined process of privacy criteria. This security mechanism is achieved by privacy level prioritization systems that safeguard real-time networks from any possible threats.

Firstly, the process begins with choosing sidechains S = {s1, s2,… sn} that have certain parameters Pi = {pi1, pi2, pi3, others. These parameters are estimated through the formula number 22.

$$pim = \alpha + \sum\theta j \cdot g(vj) + \sum\sum\beta jl \cdot g(vj) \cdot g(vl) + \epsilon \dots (22)$$

The equation starts with the constant termα which is followed by the interaction term coefficients βjl and the error term ϵ which describes both model errors and measurement errors while g(vj) normalizes parameter states to a standard range that typically extends from 0 to 1 for exact comparison and summation purposes. After this the FAHP model applies fuzzy logic to manage decision-making uncertainties through its fuzzy logic system. The FAHP model starts with the first step of establishing a criteria through equation 23.

$$A = [aij]^{m \times m} \dots (23)$$

The scale used in this study shows that aij defines the weight of criterion i as compared to criterion j because the scale extends from 1 to 9 which shows that 1 denotes equal weight and 9 denotes total weight difference between two criteria. The experts supplied their comparison data through their specialized knowledge and through their research results. The FAHP method develops three triangular fuzzy numbers a~ij=(lij,mij,uij) from this matrix because it needs to address the uncertain aspects of human decision-making.

$$Si = \frac{1}{m}\sum a(i, j) \dots (24)$$

Silicon shows its relevance through the ability to capture all the evaluation data, which shows the level of relevance of each of the criteria. This procedure provides a benchmark, which

allows one to identify the relevance of the truncation work.

To verify the consistency of the pairwise comparisons it is required to calculate a Consistency Ratio (CR). CR is obtained by equation 25.

$$CR = \frac{CI}{RI} \dots (24)$$

The process determines the normalized weight vector W, which represents criterion assignment based on weight W={w1,w2,...,wm} after the consistency ratio achieves an acceptable level. The normalization is performed via equation 25, which provides the calculation method.

$$wi = \frac{Si}{\sum Sk} \dots (25)$$

The normalized weight vector W determines the weight of each criterion according to its normalized value which sums up to one required for later calculations. The FAHP model determines the final truncation process by calculating the truncated value TV(si) through equation 26 for each sidechain si.

$$TV(si) = \sum wj \cdot f(pij) \dots (26)$$

The function f defines many criteria to standardize different measurement techniques but still allows the system to measure the influence of other variables on results and non-linear progress within the process. These criteria suggest to use sigmoid functions to map parameters to privacy scores. The privacy score function of the parameter pij can be derived from equation 27.

$$f(pij) = \frac{1}{1 + e^{-k(pij-c\ )}} \dots (27)$$

The equation states that e represents the base value of natural logarithms while k serves as a positive constant which provides control over the function's slope steepness according to privacy score sensitivity needs for parameter pij changes and cj defines the function's inflection point which depends on parameter j. The sigmoid function provides multiple benefits for privacy score mapping because it delivers two main advantages. The system establishes output limits between 0 and 1 which creates an automatic process for normalizing results. The constant k allows users to modify how sensitive the privacy score reacts to different parameter value changes. The point cj serves as an inflection point which can be adjusted to match the required target value for parameter j, with data above cj producing scores higher than 0.5 and data below cj resulting in scores lower than 0.5 for real-time scenarios. The system needs to use original equation 28 because it combines all required parameters to create complete functioning model for f.

$$f(pi1, pi2, \dots, pim) = \sum wj \cdot \frac{1}{1 + e^{-kj(pij-\ )}} \dots (28)$$

The FAHP method provides weight values which assess how important each parameter is for determining privacy protection through empirical impact analysis.The model produces output in the form of truncated sidechains S' which contain elements s'1 through s'n and each truncated sidechain s'i represents a portion of original sidechain si which results from applying thresholding to truncated valueTV(si) sets.The final evaluation provides a concrete method to truncate sidechains by using fuzzy-evaluated priorities which achieves the main objective of the FAHP model through selecting essential parameters which protect privacy at required levels. Thus, enhancing efficiency of the sidechaining process. The following section of this text contains performance metrics which were used to estimate efficiency and which were compared to existing models.

Result Analysis and Comparison

The researchers investigate the IGRM for Improving Quality of Service for Densely Connected Internet of Medical Things Using Truncated Sidechains. The approach uses GQLTL for improving routing in congested Internet of Medical Things. The routing model selects the optimal routes for data transmission based on the analysis of the time and spatial properties of the IoMT nodes. The model employs a truncated sidechain mechanism to establish secure connections with its optimized routes. The Grey Wolf Whale Optimiser (GWWO) optimises the sidechains to optimal lengths. The fuzzy AHP is used for precise chain cutting according to different levels of privacy requirement. To evaluate their proposed system, the authors built a full-fledged testing environment simulating real-world IoMT healthcare scenarios.

Network Topology

The network setup demonstrates how the IoMT devices function in a simulated healthcare environment. The design of the system was based on actual medical monitoring equipment which had the following specific components.

The total number of IoMT devices is 100.

There are 5 IoMT gateways in the system.

The area covered by the deployment of the devices is 100 meters by 100 meters.

NS-3 network simulator was utilized to conduct experiments. It allows users to build complex network communication protocol models and demonstrates their operations. The following are the main parameters of the experiment.

The simulation lasts for 30 minutes or 1800 seconds.

The communication range of IoMT devices is 10 meters.

Each device sends one data packet once per minute.

The mobility model of the experiment is Random Waypoint Mobility Model.

Network Performance Metrics

The researchers used important metrics related to network performance to evaluate the proposed routing model.

Communication delay point.

Energy efficiency is the amount of energy spent for each packet transmission.

The PDR measures the successful delivery rate of packets from total sent packets.

Jitter measures the variation in transmission times for network packets which occur during active data transfers.

The experimental conditions required two distinct communication systems which scientists used to test their model under various network load conditions.

Low Traffic Situation • Rate of data generation: 0.5 packets per minute for each device

A lot of traffic • Rate of data generation: 2 packets per minute for each device

Security and Privacy Settings

The IGRMQITS framework security and privacy features were evaluated through these configuration settings: • Length of the cryptographic key: 256 bits • Privacy levels: Low, Medium, and High • The sidechain width can extend between 10 to 50 blocks.

Execution of Experiments

The scientists conducted multiple testing rounds under various network conditions to achieve both reliable outcomes and valid statistical results. The researchers introduced random elements which included node movement and packet generation events to create different communication patterns used by IoMT devices. The performance testing required multiple network communication instances (NC) to be created which included 10,000 to 500,000 transmissions in each instance.

The researchers used this equation to determine routing delay (D) for every communication instance.

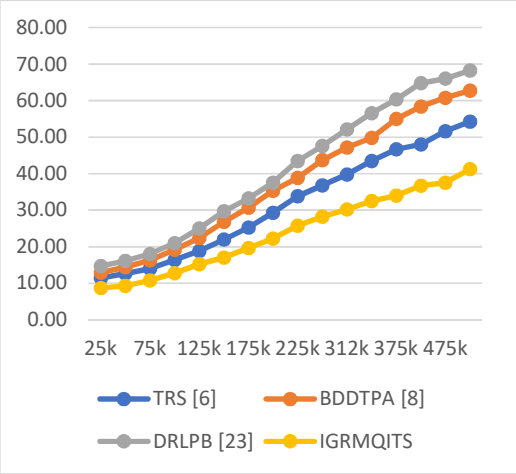
$$\boldsymbol{D = \frac{1}{NC}\sum_{i=1}^{NC}(t_{s\_reach} - t_{s\_start})} \quad (23)$$

where

t_{s_reach} denotes the time at which the packet arrives at the destination node

• t_{s_start} represents the time when the packet transmission begins at the source node

The delay was compared with several existing routing approaches, including TRS, BDDTPA, and DRLPB. The comparative analysis, presented in Figure 2, demonstrates the improvements achieved by the proposed routing and security model in dense IoMT network environments.

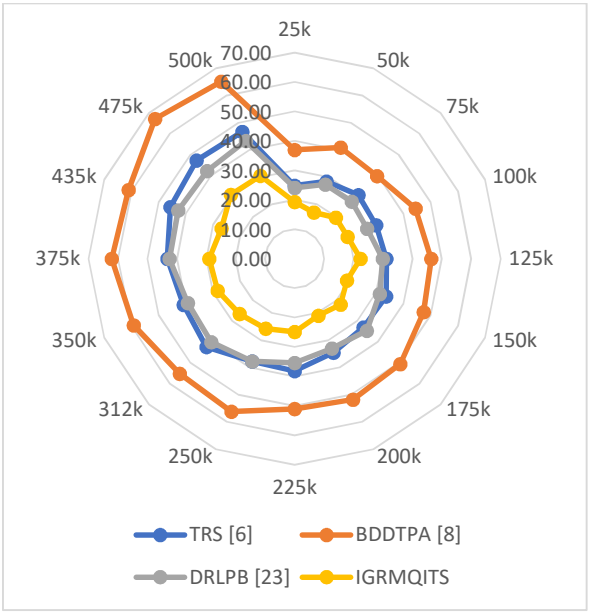


Routing delay (D) becomes a significant parameter in IoMT that influences the entire Quality of Service (QoS) of the data transmission in these networks. The research conducts delay analysis between IGRMQITS framework and some traditional approaches such as TRS BDDTPA and DRLPB in relation to various amounts of communication within the system. The findings prove that the proposed approach has smaller delay values than the rest of the approaches. For instance, IGRMQITS obtained a delay value of 8.71 seconds when the amount of messages (NM) is 25,000 whereas the same number was observed with 11.38 seconds, 12.90 seconds, and 14.72 seconds from TRS BDDTPA and DRLPB respectively. There are two main factors that contribute to smaller values of delay which are the GQL algorithm and TLFFO technique. Together these two techniques provide the best routes in terms of spatial and temporal aspects of nodes in networks that allows for faster and reliable communication in IoMT applications such as patient monitoring and healthcare data services.

We also used Equation (29) to look at the energy consumption (E) involved in routing operations, in addition to looking at delays. Figure 3 shows the results.

$$E = \frac{1}{NC}\sum_{i=1}^{NC}\left(E_{src(start)_i} - E_{src(complete)_i}\right) \quad (29)$$

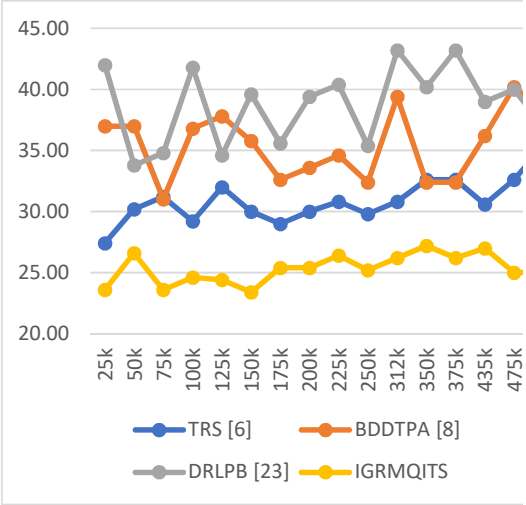
where $E_{src(start)}$and $E_{src(complete)}$denote the energy levels of the source node at the beginning and at the completion of the routing process, respectively. This metric helps in assessing the energy efficiency of the routing framework during communication operations.



The energy consumption (E) of routing operations in IoMT networks, where network measure their energy consumption in milliwatts (mW), establishes a significant relationship between device operation performance and device operational lifetime. The study measures energy efficiency of IGRMQITS framework by performance comparison of TRS BDDTPA DRLPB routing methods with different NM routing communication volumes. The experimental results show that the proposed model consumes less energy than all other methods under all test conditions. The IGRMQITS model consumes 19.26 mW energy at NM 25,000 while TRS BDDTPA and DRLPB consume 24.81 mW 36.96 mW and 24.11 mW respectively.

In IoMT environments, medical devices consume considerable battery power for

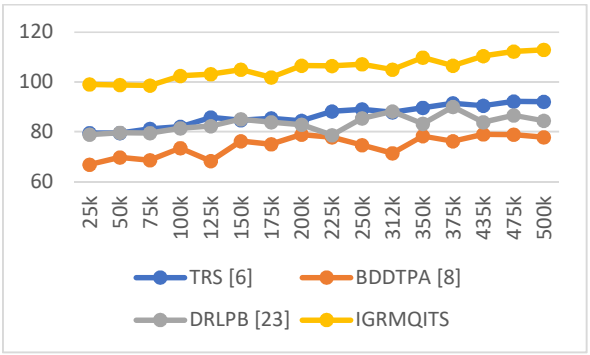
operational needs, which makes energy conservation a critical advantage. Energy efficiency extends the life of devices, reducing the need for regular maintenance and battery replacement. The required system performance needs continuous system operation which has special significance in healthcare monitoring systems. The proposed model enhances the energy efficiency by employing the TLFFO and GWWO optimization techniques to find the optimal routing pathways and sidechain configuration solutions. The model minimizes unnecessary processing requirements and the energy consumption for data transmission by selecting the best communication routes. The proposed framework enhances the dependability and sustainability of IoMT networks by the implementation of energy-saving routing operations. Figure 4 demonstrates the improved jitter test results which the model achieves with energy savings. The communication system between networks achieves improved stability for reliable performance



The measurement of energy consumption (E) in Internet of Medical Things (IoMT) network routing operations occurs through the assessment of power usage which is expressed in milliwatts (mW). The study investigates how efficiently the IGRMQITS framework operates when compared to existing routing techniques which include TRS, BDDTPA, and DRLPB at different routing communication levels (NM) The experimental analysis shows that the proposed method requires less energy for operations than all other tested models. When NM equals 25,000 the IGRMQITS model consumes 19.26 mW while TRS BDDTPA and DRLPB consume 24.81 mW 36.96 mW and 24.11 mW respectively.

Lower energy consumption provides great benefits in IoMT due to the fact that medical equipment uses a battery to power up. Thus, low energy consumption makes it possible to extend the life of devices by minimizing maintenance costs and battery replacements. In addition, the need to run medical equipment continuously without a break becomes very important due to the fact that the system depends on it to monitor patients continuously. This is made possible by combining Teacher-Learner Firefly Optimization and GWWO algorithms, making data transfer more efficient.

In short, the IGRMQITS framework makes IoMT networks more stable, reliable, and energy-efficient by using less energy when routing. The framework also shows better jitter stability, as shown in Figure 4, which supports consistent and reliable communication in IoMT-based healthcare systems.



THR in IoMT networks is the speed of data transfer in the network, measured in kbps. Measurement of throughput through Quality of Service (QoS) is important as it depicts the capability of the network to process and transmit actual communication traffic. The study tests the performance of IGRMQITS frameworks. The performance is tested based on the throughput of IGRMQITS with TRS BDDTPA DRLPB network communication techniques with different routing communication volumes. The experimental results indicate that IGRMQITS always has a higher throughput than the other compared models. When NM is 25,000, the proposed framework transmits data at a rate of 99 kbps. The TRS BDDTPA and DRLPB data rates are 79.4 kbps and 66.8 kbps 78.8 kbps, respectively. The proposed approach keeps the performance of data transmission at a stable level, which is improved with the increase of the communication volume. Healthcare systems that use IoMT technology require the fast and reliable transmission of large amounts of medical data, sensor readings and patient

monitoring information. The ability to transmit more data means medical professionals can share information more quickly, leading to better real-time monitoring and diagnosis of patients and better medical decision making.

The proposed model has better throughput performance because it uses both the GQL routing strategy and the TLFFO algorithm together. The system uses these methods to select optimal routes which enable it to manage increased data traffic by improving network resource allocation. The IGRMQITS framework improves data transmission speed and reliability through dense IoMT networks which leads to enhanced network performance. Figure 7 shows that the Packet Delivery Ratio (PDR) performance is also getting better in a similar way

.

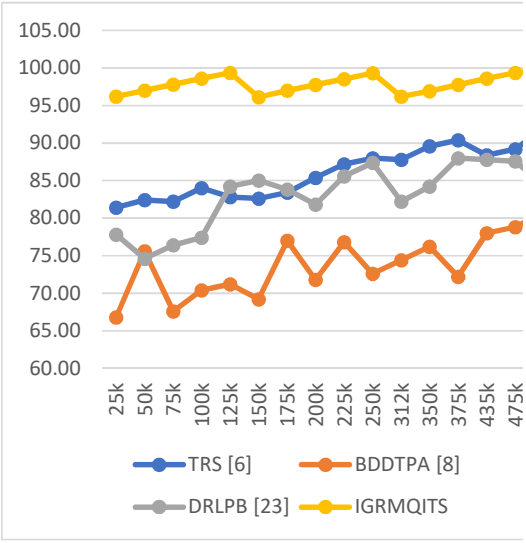


Figure 7. Total PDR for routing in IoMT Networks

The PDR is successfully delivered to their destinations to the total number of data packets transmitted in an IoMT network. Network reliability test is an important performance metric to evaluate the ability of the network to maintain stable communication links. The study examines the performance of the proposed Incremental Graph-based Routing Model in providing Packet Delivery Ratio (PDR) results for Quality of Service enhancement in dense Internet of Medical Things (IoMT) networks through its utilization of Truncated Sidechains (IGRMQITS). The results of this work are compared with existing routing methods including TRS and BDDTPA and DRLPB at different levels of NM routing activities.

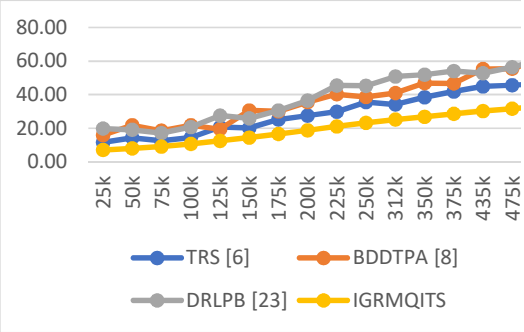
The IGRMQITS framework achieves better PDR results than all other tested methods across every communication level according to experimental results. The proposed model achieves a PDR of 96.18% when NM equals 25,000 while TRS BDDTPA and DRLPB achieve PDR values of 81.40% 66.80% and 77.80% respectively. The proposed framework shows improved packet delivery rates when more routing communications occur. The system demonstrates its ability to maintain dependable communication through dense IoMT networks use medical devices and their data flow to operate. Hospitals need satisfactory patient data delivery rates to transmit patient vital signs and monitoring results and medical diagnosis files because these records contain vital medical information. Healthcare workers receive all necessary information to their work because reliable packet delivery lets them receive information on time which is essential for patient monitoring and clinical decision making. The network achieves better performance through decreased packet loss because it becomes more stable which diminishes retransmission needs.

The improved PDR results of IGRMQITS achieve their highest performance through advanced routing optimization methods which use the GPL algorithm and the Teacher-Learner Firefly Optimization algorithm. The methods use network conditions to determine suitable routing paths which operate under both spatial and temporal conditions. The system increases its likelihood to successfully transmit packages because all components work together as one unit.

The increase in the proposed system's PDR indicates its ability to offer efficient data communication in a dense IoMT environment. The proposed solution is essential to the healthcare industry since hospitals rely on efficient data transmission to offer quality services to their patients. In addition to evaluating the efficiency of routing operations in the proposed framework, the authors tested the proposed framework concerning blockchain processes.

Storage Analysis

In Figure 8, the authors compare the amount of space required by the blockchain process, including the time taken to add new blocks to the blockchain, using the proposed system against traditional systems such as TRS, BDDTPA, and DRLPB.

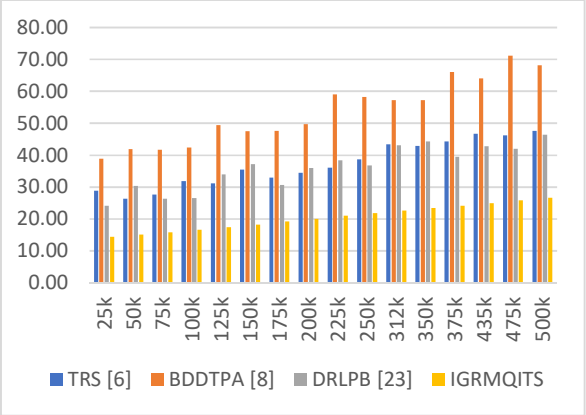


The main measure for assessing blockchain security in the protection of medical data is the need for further network block development in the IoMT systems. The research evaluates the IGRM based on Truncated Sidechains for QoS improvements in dense IoMT networks compared to three existing routing approaches including TRS, BDDTPA and DRLPB at different levels of routing communication. From the experimental results, it can be observed that IGRMQITS framework always has shorter mining delay in comparison with other methods. When NM=25000, the mining and insertion time of blocks in the proposed model is 7.11 seconds. The TRS system takes 11.55 seconds to perform its functions and BDDTPA and DRLPB take 15.77 and 19.84 seconds to perform their functions respectively. Proposed framework shows the improved performance results with the increase of number of routing communications. The system is capable of performing blockchain operations in dense operation conditions of Internet of Medical Things

.Healthcare IoMT systems achieve better operational efficiency through decreased mining times because their systems allow for protected medical data documentation and verification activities that need no extra time. The blockchain system provides faster data storage capabilities through its quick block generation system which enables immediate recording of essential health information about patients and their medical observations. The system provides users with faster response times which protect all their information. The applications require these elements because they depend on fast data verification for their essential functions.

The IGRMQITS model works better because it uses better optimisation methods. The GWWO uses its method to determine the ideal sidechain lengths while FAHP evaluates various privacy degrees which occur during sidechain truncation. The systems work together to diminish unnecessary blockchain resource consumption while they improve mining operation efficiency.

The proposed framework's shorter mining delay shows that IGRMQITS makes it possible to manage blockchain-based data more quickly and efficiently in IoMT networks. This solution improves the security and reliability of healthcare data storage systems while maintaining their accessibility. Our team conducted a delay analysis while we examined the energy consumption required to create a block which we then compared to existing models. The results are shown in Figure 9.

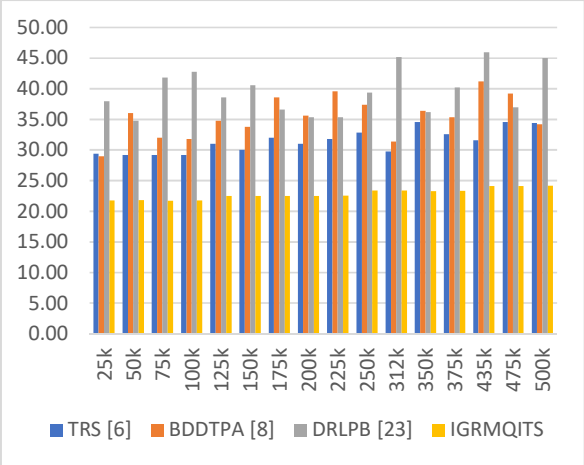


IoMT network's energy consumption (E) for mining and creating blocks that researchers quantify in milliwatts (mW) emerges as an important parameter that helps in analysing whether the blockchain architecture is able to protect data related to the health industry or not. As the energy consumption within IoMT networks has to be efficient because the medical devices work on batteries having small battery life, their working hours get decreased up to 50% due to the continuous process of blockchain architecture. This paper measures the energy efficiency of IGRMQITS model based on Incremental graph for improving quality of services in dense IoMT networks with Truncated side chains (IGRMQITS) when compared with TRS-BDDTPA and DRLPB using various amounts of routing communications (NM).The proposed model needs about 14.42 mW of power when NM = 25,000 for operation. TRS, BDDTPA, and DRLPB, on the other hand, use 28.81 mW, 38.96 mW, and 24.11 mW, respectively. The proposed framework continues to show similar improvements as the communication load grows, showing that it can support energy-efficient blockchain operations even when the network is busy.

The healthcare facilities which adopt IoMT systems achieve energy savings through their blockchain operations because their multiple sensors and medical devices keep sending patient data. The energy-saving practices extend device longevity while they also minimize maintenance needs and decrease operational costs. Energy-efficient blockchain processing ensures that sensitive healthcare data can be securely stored and authenticated without causing excessive network device usage.

The advanced optimisation techniques which drive better energy efficiency for the proposed model serve as its primary energy-efficient mechanism. The Grey Wolf Whale Optimiser (GWWO) helps find the best sidechain lengths which cuts down on extra work that needs to be done when making blocks. The Fuzzy Analytic Hierarchy Process (FAHP) establishes different privacy levels which control the process that disconnects the sidechain. The mechanisms work together to reduce unnecessary blockchain activities which improve the efficiency of the mining operation.

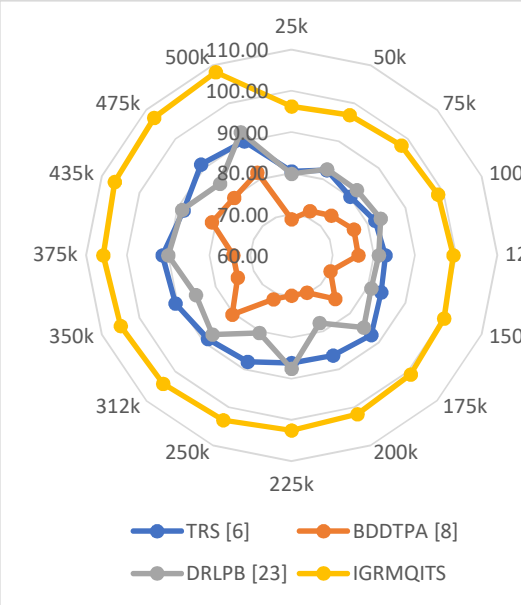
The IGRMQITS framework demonstrates superior performance over all other frameworks because it consumes lessenergy when executing block creation and verification processes. The improvement enables blockchain data management systems used by IoMT networks to achieve better sustainability and operational efficiency. Systems that consume less energy result in improved operational reliability while IoMT healthcare devices function correctly during extended real-world usage. The framework protects secure data through its security measures while enabling the network to run at maximum efficiency. We performed our analysis of energy consumption together with system performance assessments during jitter testing which took place at the time of block insertion. The results shown in Figure 10 prove that the new models outperform existing models which possess the same characteristics.



The IoMT networks are plagued with jitter (J) which is the time difference between the completion of blockchain operations that take to finish their tasks. The blockchain system is capable of providing stable processing operations in the network structure. The system shows increased intervals of block creation and testing as jitter decreases, which helps to preserve the accuracy of data management in the system in IoMT networks. This research evaluates the jitter performance of IGRMQITS, which is an Incremental Graph-based Routing Model for QoS enhancement in dense IoMT networks that uses Truncated Sidechains as its routing system. It compares IGRMQITS with TRS BDDTPA and DRLPB as the number of tests increases It tests different routing communication levels including NM.
The experimental results show that the IGRMQITS framework always produces smaller jitter values in comparison to the other models. The model output indicates that at NM 25,000 the system jitter performance is 21.75 microsecond. TRS system shows 29.40 microseconds jitter. BDDTPA produces 29.00 microseconds and DRLPB shows 38.00 microseconds. The proposed framework keeps stable jitter levels during its operation with increasing routing communication activities. The system shows its ability to continuously perform blockchain tasks in busy Internet of Medical Things environments.

The Internet of Medical Things demands healthcare systems to safeguard sensitive medical information with robust validation methods to secure data storage. The blockchain network guarantees consistent operation providing timely documentation of patient records and monitoring information and healthcare activities. The system produces precise validation outcomes that improve

healthcare delivery through better monitoring systems and remote patient treatment solutions. The proposed model has better jitter stability because of more advanced optimization techniques. The Grey Wolf Whale Optimiser (GWWO) determines the best sidechain configurations, and Fuzzy Analytic Hierarchy Process (FAHP) evaluates the sidechain privacy specifications in the truncation phase. The mechanisms facilitate the more efficient operation of the blockchain within the network by reducing unwarranted variations in processing that take place during the creation of blocks. The proposed system with the blockchain implementation has lower jitter values in the IGRMQITS framework for IoMT data management, thus achieving more consistent outcomes. The enhancements in system stability make the system more reliable, allow better understanding of data processing and create more security measures against unauthorized access to confidential health records. Figure 11 shows the throughput performance test from the blockchain operations, which it conducted by performing jitter analysis.



The research established an Incremental Graph-based Routing Model to improve Quality of Service delivery in IoMT networks which operate with Truncated Sidechains. The increasing adoption of IoMT technologies in healthcare systems requires networks to process vast amounts of medical information while maintaining dependable communication and safeguarding patient privacy and operational security. The proposed framework establishes intelligent routing together with blockchain security elements to fulfill these requirements. It allows for fast transfer of information, while simultaneously providing a safe environment for controlling the data in densely populated IoMT ecosystems.

For the routing process in the proposed architecture, Graph-Based Q-Learning (GQL) is used to select the best path between different devices within the network. TLFFO optimizes the routing system by selecting the route based on the current location and motion trajectory of IoMT devices. In addition to optimizing the routing process, the proposed architecture introduces a truncated sidechain design scheme, which increases data security. GWWO is used for determining optimal sidechain length, while FAHP fine-tunes this value depending on the varying privacy levels, ensuring the safe storage and transmission of confidential healthcare data.

As evidenced from the tests, the proposed framework provides significant improvements in multiple performance metrics related to communication networks. It was found that the communication delay dropped by 10.5%, while energy efficiency improved by 8.5%. The increase in throughput was 3.9%, the packet delivery rate increased by 1.5%, and network jitter decreased by 8.3%. Mining efficiency is enhanced with the inclusion of the blockchain component, decreasing mining time by 12.

The designed system offers an increased reliability of communication among IoMT-based health care systems. The better quality of services facilitates more reliable and rapid transmission of patient data, which is important for both real-time monitoring and effective medical decision-making processes. The decrease of energy consumption along with improved performance of blockchains allows for operating devices for a prolonged time and makes IoMT-based systems sustainable.

The IGRMQITS architecture can be considered a complete solution, providing optimization of intelligent routing together with safety measures regarding the storage of sensitive information using blockchain technology. The offered solution facilitates the improvement of network performance and safety of sensitive data in a dense IoMT environment. It seems that this area will be promising for future research related to IoMT applications.

Conclusion & Future Scope

We have proposed an IGRM for QoS improvement in congested IoT networks with truncated sidechains (IGRMQITS). There are specific requirements in relation to the modern healthcare services as such environments

require IoMT devices that in turn require communication technologies capable of conveying huge amounts of medical data ensuring patient privacy and security. Hence, the framework utilizes intelligent routing techniques and blockchain-based security strategies to address these requirements, ensuring reliable and efficient data transmission in IoMT networks.

The proposed framework is based on a GQL technique to assist the system to identify a proper routing strategy. GQL is used to find the best communication routes in the network. Furthermore, the application of the Teacher–Learner based Firefly Optimisation (TLFFO) algorithm contributes to the advancement of the system by choosing network paths based on the physical and temporal characteristics of IoMT devices. The proposed solution has another benefit, the truncated sidechain approach, that provides enhanced security features when transmitting critical medical data. Grey Wolf Whale Optimiser (GWWO) is employed to determine appropriate sidechain lengths and Fuzzy Analytic Hierarchy Process (FAHP) is used to make decision for selecting specific values based on privacy requirements.

The experimental results show the efficiency of the proposed structure in improving several network performance metrics. The results indicate 10.5% reduction in communication delays, 8.5% improvement in energy efficiency, improvement in network jitter. Integration of the blockchain technology in the structure helps to improve mining operations by reducing mining delay by 12.5% and energy use in mining activities by 5.9% and cuts storage needs by 4.9%.

The improvements show that the proposed structure allows the IoMT-based health care networks to keep their communication functionalities with reliable performance and high-quality results. Higher quality of services allows doctors to access patient information with higher speeds, which guarantees accuracy of monitoring results necessary for patient monitoring. The IoMTs are sustainable because it uses energy-efficient blockchain technology to optimize the operational capabilities of the devices.

The IGRMQITS framework suggests a complete methodology that combines routing optimization and blockchain data management. The proposed method helps the developers to build scalable secure energy-efficient healthcare communication systems through IoMT technologies by enhancing the network performance and protecting the information in busy IoMT environments.

Possibilities for future research

The successful development and validation of the IGRMQITS framework provides many opportunities for further research and development of new technologies in IoMT-based healthcare systems. In future, the work will be done on developing solutions to improve security, intelligence, and scalability for the IoMT systems that will be bigger and more complex. • Future work will include the integration of 5G networks and edge computing and advanced blockchain architectures for new communication technologies development. These technologies will allow the IoMT healthcare systems to transfer data faster, reducing latency, and improving the reliability and scalability of the system. • AI and machine learning help healthcare analysts by predictive analytics and enable more efficient routing operations. Intelligent models could identify rare patterns of patient data that would help and improve their clinical decision making. • Making devices work better together

The main challenge with IoMT environments is that devices from different manufacturers have to be compatible with each other. Future research will examine standardized protocols and an interoperable framework to enable seamless data sharing between medical devices and health care systems and cloud applications. • Greater use of devices by health care facilities to deliver medical care puts patient data at risk and there is a need to improve security within networks. Future research will focus on the development of new encryption methods and zero trust and intelligent threat detection security frameworks.

IoMT Deployments: • Lightweight routing algorithms enable scientists to evaluate blockchain solutions that can support large scale IoMT networks with less computation requirements, as shown in the study. • Analysis of Private Medical Data: Future work will focus on privacy etc. Medical information is very sensitive and needs to be protected. • Real-Time Analytics for Health Services : Health care response systems need a platform that allows simultaneous analysis of data streams from IoMT devices to improve functionality. The remote health monitoring system will apply real-time data analytics to improve predictive diagnostics and emergency medical services. • Regulatory compliance: As IoMT applications become more common around the world, organizations will need to ensure that they comply with health regulations such as HIPAA, GDPR and others. The future research project will develop frameworks for secure and efficient management of health data from the IoMT devices. • Humans and Machines

Interaction in Health Care Systems: Scientists working in the field of improving healthcare systems for the purpose of effective interaction between employees and IoMT solutions have the prospects in their research activities. The application of IoMT solutions in clinical practice allows medical workers to work with their patients in a much more efficient way. • Implementation of IoMT technologies into practice will bring health care services to all corners of the world, due to which poor people will get access to quality health care. In the future, scientific research will be dedicated to the development of IoMT solutions that would enable the provision of remote health care services in rural communities. IoMT solutions would transform healthcare services, giving users two big benefits: more effective treatment and greater security of medical information. Currently, research in this area will lead to the development of new systems that will operate at high speed and will be available to everyone.

References

L. Yin, J. Xu and Q. Tang, "Sidechains With Fast Cross-Chain Transfers," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 3925-3940, 1 Nov.-Dec. 2022, doi: 10.1109/TDSC.2021.3114151.

J. Li, T. Liu, D. Niyato, J. Li and Z. Han, "On Sidechain-Assisted Transaction Service Management for Internet of Things: A Random Contract Approach," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 5, pp. 3437-3453, 1 Sept.-Oct. 2022, doi: 10.1109/TNSE.2022.3181114.

S. Khan, M. B. Amin, A. T. Azar and S. Aslam, "Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability," in IEEE Access, vol. 9, pp. 116672-116691, 2021, doi: 10.1109/ACCESS.2021.3106384.

M. Westerkamp and A. Küpper, "Instant Function Calls Using Synchronized Cross-Blockchain Smart Contracts," in IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2136-2150, Sept. 2023, doi: 10.1109/TNSM.2023.3236437.

C. T. Nguyen et al., "FedChain: Secure Proof-of-Stake-Based Framework for Federated-Blockchain Systems," in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2642-2656, 1 July-Aug. 2023, doi: 10.1109/TSC.2023.3240235.

G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak and A. Ignjatovic, "Trust-Based Blockchain Authorization for IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1646-1658, June 2021, doi: 10.1109/TNSM.2021.3077276.

L. Besançon, C. F. Da Silva, P. Ghodous and J. -P. Gelas, "A Blockchain Ontology for DApps Development," in IEEE Access, vol. 10, pp. 49905-49933, 2022, doi: 10.1109/ACCESS.2022.3173313.

D. Dansana et al., "BDDTPA: Blockchain-Driven Deep Traffic Pattern Analysis for Enhanced Security in Cognitive Radio Ad-Hoc Networks," in IEEE Access, vol. 11, pp. 98202-98216, 2023, doi: 10.1109/ACCESS.2023.3312291.

J. Liu et al., "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2231-2242, May 2023, doi: 10.1109/JBHI.2022.3183397.

E. Zhou et al., "MSTDB: A Hybrid Storage-Empowered Scalable Semantic Blockchain Database," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 8, pp. 8228-8244, 1 Aug. 2023, doi: 10.1109/TKDE.2022.3220522.

M. Yuan et al., "TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Control in Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 3, pp. 3489-3500, March 2023, doi: 10.1109/TITS.2022.3226500.

N. Afraz, F. Wilhelmi, H. Ahmadi and M. Ruffini, "Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis," in IEEE Access, vol. 11, pp. 95653-95666, 2023, doi: 10.1109/ACCESS.2023.3309423.

A. Hafid, A. S. Hafid and M. Samih, "A Tractable Probabilistic Approach to Analyze Sybil Attacks in Sharding-Based Blockchain Protocols," in IEEE Transactions on Emerging Topics in Computing, vol. 11, no. 1, pp. 126-136, 1 Jan.-March 2023, doi: 10.1109/TETC.2022.3179638.

B. van Haaren Van Duijn, J. Bonnin Roca, A. G. L. Romme and M. Weggeman, "The Seven Capital Sins in the Governance of Blockchain Ecosystems," in IEEE Engineering Management Review, vol. 51, no. 3, pp. 13-17, 1 thirdquarter,Sept. 2023, doi: 10.1109/EMR.2023.3280130.

W. Wang and Y. Zhao, "Blockchain-Based Spectrum Management Architecture and Trading Mechanism Design for Space-Air-Ground Integrated Network," in IEEE Communications Letters, vol. 27, no. 10, pp. 2692-2696, Oct. 2023, doi: 10.1109/LCOMM.2023.3308097.

X. Hao, W. Ren, Y. Fei, T. Zhu and K. -K. R. Choo, "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things," in IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 773-786, 1 March-April 2023, doi: 10.1109/TSC.2022.3179727.

Y. Lu, X. Tang, L. Liu, F. R. Yu and S. Dustdar, "Speeding at the Edge: An Efficient and Secure Redactable Blockchain for IoT-Based Smart Grid Systems," in IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12886-12897, 15 July15, 2023, doi: 10.1109/JIOT.2023.3253601.

H. M. Buttar, W. Aman, M. M. U. Rahman and Q. H. Abbasi, "Countering Active Attacks on RAFT-Based IoT Blockchain Networks," in IEEE Sensors Journal, vol. 23, no. 13, pp. 14691-14699, 1 July1, 2023, doi: 10.1109/JSEN.2023.3274687.

X. Feng, J. Ma, H. Wang, S. Wen, Y. Xiang and Y. Miao, "Space-Efficient Storage Structure of Blockchain Transactions Supporting Secure Verification," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2631-2645, 1 July-Sept. 2023, doi: 10.1109/TCC.2022.3220664.

Y. Liu et al., "A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things," in IEEE Transactions on Computers, vol. 72, no. 2, pp. 501-512, 1 Feb. 2023, doi: 10.1109/TC.2022.3157996.

Z. Wang, Q. Chen and L. Liu, "Permissioned Blockchain-Based Secure and Privacy-Preserving Data Sharing Protocol," in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10698-10707, 15 June15, 2023, doi: 10.1109/JIOT.2023.3242959.

X. Li, J. Xu, L. Yin, Y. Lu, Q. Tang and Z. Zhang, "Escaping From Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 3699-3715, 1 Sept.-Oct. 2023, doi: 10.1109/TDSC.2022.3212601.

D. S. Gadiraju, V. Lalitha and V. Aggarwal, "An Optimization Framework Based on Deep Reinforcement Learning Approaches for Prism Blockchain," in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2451-2461, 1 July-Aug. 2023, doi: 10.1109/TSC.2023.3242606.

G. Tian, J. Wei, M. Kutyłowski, W. Susilo, X. Huang and X. Chen, "VRBC: A Verifiable Redactable Blockchain With Efficient Query and Integrity Auditing," in IEEE Transactions on Computers, vol. 72, no. 7, pp. 1928-1942, 1 July 2023, doi: 10.1109/TC.2022.3230900.

B. Cao et al., "Blockchain Systems, Technologies, and Applications: A Methodology Perspective," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 353-385, Firstquarter 2023, doi: 10.1109/COMST.2022.3204702.

K. Saadat, N. Wang and R. Tafazolli, "AI-Enabled Blockchain Consensus Node Selection in Cluster-Based Vehicular Networks," in IEEE Networking Letters, vol. 5, no. 2, pp. 115-119, June 2023, doi: 10.1109/LNET.2023.3238964.

L. Cui, Z. Xiao, F. Chen, H. Dai and J. Li, "Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme," in IEEE Transactions on Cybernetics, vol. 53, no. 6, pp. 3588-3598, June 2023, doi: 10.1109/TCYB.2022.3163743.

Y. Liu et al., "A Flexible Sharding Blockchain Protocol Based on Cross-Shard Byzantine Fault Tolerance," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2276-2291, 2023, doi: 10.1109/TIFS.2023.3266628.

W. Shang and Z. Yu, "A new media content trusted dissemination architecture based on AV-blockchain and ChinaDRM," in Intelligent and Converged Networks, vol. 4, no. 2, pp. 142-157, June 2023, doi: 10.23919/ICN.2023.0015.

K. Qian, Y. Liu, C. Shu, Y. Sun and K. Wang, "Fine-Grained Benchmarking and Targeted Optimization: Enabling Green IoT-Oriented Blockchain in the 6G Era," in IEEE Transactions on Green Communications and Networking, vol. 7, no. 2, pp. 1036-1051, June 2023, doi: 10.1109/TGCN.2022.3185610.

Z. Wu, J. Liu, J. Wu, Z. Zheng and T. Chen, "TRacer: Scalable Graph-Based Transaction Tracing for Account-Based Blockchain Trading Systems," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2609-2621, 2023, doi: 10.1109/TIFS.2023.3266162.

C. Zhang et al., "A Blockchain-Based Model Migration Approach for Secure and Sustainable Federated Learning in IoT Systems," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6574-6585, 15 April15, 2023, doi: 10.1109/JIOT.2022.3171926.

F. Yu, J. Peng, X. Li, C. Li and B. Qu, "A Copyright-Preserving and Fair Image Trading Scheme Based on Blockchain," in Tsinghua Science and Technology, vol. 28, no. 5, pp. 849-861, October 2023, doi: 10.26599/TST.2022.9010066.

K. Almi'Ani, Y. C. Lee, T. Alrawashdeh and A. Pasdar, "Graph-Based Profiling of Blockchain

Oracles," in IEEE Access, vol. 11, pp. 24995-25007, 2023, doi: 10.1109/ACCESS.2023.3254535.

M. Li, W. Wang and J. Zhang, "LB-Chain: Load-Balanced and Low-Latency Blockchain Sharding via Account Migration," in IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 10, pp. 2797-2810, Oct. 2023, doi: 10.1109/TPDS.2023.3238343.

N. K. Akrasi-Mensah et al., "Adaptive Storage Optimization Scheme for Blockchain-IIoT Applications Using Deep Reinforcement Learning," in IEEE Access, vol. 11, pp. 1372-1385, 2023, doi: 10.1109/ACCESS.2022.3233474.

M. Rehman, I. T. Javed, K. N. Qureshi, T. Margaria and G. Jeon, "A Cyber Secure Medical Management System by Using Blockchain," in IEEE Transactions on Computational Social Systems, vol. 10, no. 4, pp. 2123-2136, Aug. 2023, doi: 10.1109/TCSS.2022.3215455.

A. Lakhan et al., "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 664-672, Feb. 2023, doi: 10.1109/JBHI.2022.3165945.

L. Li, D. Jin, T. Zhang and N. Li, "A Secure, Reliable and Low-Cost Distributed Storage Scheme Based on Blockchain and IPFS for Firefighting IoT Data," in IEEE Access, vol. 11, pp. 97318-97330, 2023, doi: 10.1109/ACCESS.2023.3311712.

Y. Xu, E. Yu, Y. Song, F. Tong, Q. Xiang and L. He, "$\mathcal {R}$-Tracing: Consortium Blockchain-Based Vehicle Reputation Management for Resistance to Malicious Attacks and Selfish Behaviors," in IEEE Transactions on Vehicular Technology, vol. 72, no. 6, pp. 7095-7110, June 2023, doi: 10.1109/TVT.2023.3238507.

X. Jia, Z. Yu, J. Shao, R. Lu, G. Wei and Z. Liu, "Cross-Chain Virtual Payment Channels," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3401-3413, 2023, doi: 10.1109/TIFS.2023.3281064.

Z. Zhou, Y. Tian, J. Xiong, J. Ma and C. Peng, "Blockchain-Enabled Secure and Trusted Federated Data Sharing in IIoT," in IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 6669-6681, May 2023, doi: 10.1109/TII.2022.3215192.

Y. Guo, Z. Wan, H. Cui, X. Cheng and F. Dressler, "Vehicloak: A Blockchain-Enabled Privacy-Preserving Payment Scheme for Location-Based Vehicular Services," in IEEE Transactions on Mobile Computing, vol. 22, no. 11, pp. 6830-6842, 1 Nov. 2023, doi: 10.1109/TMC.2022.3193165.

I. Aviv, A. Barger, A. Kofman and R. Weisfeld, "Reference Architecture for Blockchain-Native Distributed Information System," in IEEE Access, vol. 11, pp. 4838-4851, 2023, doi: 10.1109/ACCESS.2023.3235838.

K. Hao, J. Xin, Z. Wang, Z. Yao and G. Wang, "Efficient and Secure Data Sharing Scheme on Interoperable Blockchain Database," in IEEE Transactions on Big Data, vol. 9, no. 4, pp. 1171-1185, 1 Aug. 2023, doi: 10.1109/TBDATA.2023.3265178.

J. Li, J. Wu, L. Chen, J. Li and S. -K. Lam, "Blockchain-Based Secure Key Management for Mobile Edge Computing," in IEEE Transactions on Mobile Computing, vol. 22, no. 1, pp. 100-114, 1 Jan. 2023, doi: 10.1109/TMC.2021.3068717.

W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin and A. Miranskyy, "Immutable Log Storage as a Service on Private and Public Blockchains," in IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 356-369, 1 Jan.-Feb. 2023, doi: 10.1109/TSC.2021.3120690.

L. Wang, Z. Guan, Z. Chen and M. Hu, "sChain: An Efficient and Secure Solution for Improving Blockchain Storage," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3662-3676, 2023, doi: 10.1109/TIFS.2023.3285489.

S. Häselbarth, O. Winkels and K. Strunz, "Blockchain-Based Market Procurement of Reactive Power," in IEEE Access, vol. 11, pp. 36106-36119, 2023, doi: 10.1109/ACCESS.2023.3263669.

P. Bagchi et al., "Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications," in IEEE Transactions on Vehicular Technology, vol. 72, no. 8, pp. 10393-10408, Aug. 2023, doi: 10.1109/TVT.2023.3260579.