International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

Quality of Service-Aware Privacy Preservation in Fog Computing: A Blockchain, Attribute-Based Encryption and Machine Learning-Based Approach

Roshan Gunwantrao Belsare
Department of Computer Science and Engineering
Government College of Engineering
Amravati, India

Dr. P. B. Ambhore
Department of Computer Science and Engineering
Government College of Engineering
Amravati, India

Dr. P. N. Chatur
Prof. A. V. Deorankar
Department of Computer Science and Engineering
Government College of Engineering
Amravati, India

Abstract: Blockchain technology has become a fundamental enabler for secure and decentralized data management in fog computing and the Internet of Things (IoT). However, conventional consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) suffer from limitations including high energy consumption, centralization risks, and limited scalability, making them inefficient for dynamic, resource-constrained fog environments.

To address these challenges, this research proposes a Quality of Service (QoS)-aware privacy preservation framework that integrates blockchain, Attribute-Based Encryption (ABE), and machine learning. A Grey Wolf Optimization (GWO)-enhanced hybrid consensus model is introduced, combining PoW-based computational security with PoS-driven energy efficiency, dynamically balancing workload and trust-based miner selection. The proposed GWO-powered trust evaluation optimizes node selection based on trust score, mining efficiency, and energy consumption, ensuring enhanced security against Sybil attacks and other adversarial threats.

Furthermore, a Modified Attribute-Based Encryption (ABE) scheme is incorporated to provide fine-grained access control and computational efficiency for privacy-preserving data sharing in fog computing. The modified ABE integrates lightweight cryptographic operations, reducing computational overhead while ensuring secure, policy-based access control.

Experimental evaluations demonstrate that the proposed framework reduces communication delay by 16.5%, improves energy efficiency by 10.4%, and increases throughput by 23.5% compared to existing state-of-the-art models such as DRLBTS, QoS_ML_DSS, and SLGAF. These results highlight the effectiveness of the model in providing a scalable, secure, and energy-efficient blockchain solution for privacy-sensitive fog computing applications in healthcare, smart cities, and industrial IoT.

Keywords: Blockchain, Fog Computing, Attribute-Based Encryption, Hybrid Consensus, Grey Wolf Optimization, Privacy Preservation, QoS, Internet of Medical Things.

1. INTRODUCTION

In recent years, the proliferation of Internet of Medical Things (IoMT) devices has revolutionized healthcare by enabling real-time patient monitoring and personalized medical services. However, this advancement brings forth significant challenges concerning data privacy, security, and efficient management of the vast amounts of sensitive medical data generated [1]. Fog computing has emerged as a viable solution, extending cloud services to the network's edge to reduce latency and bandwidth usage, thereby enhancing the performance of IoMT systems. By processing data closer to its source, fog computing addresses the limitations of centralized cloud infrastructures, offering improved Quality of Service (QoS) for time-sensitive medical applications [2]. Blockchain technology further augments the security and privacy of IoMT by providing a decentralized framework for data management. Its inherent features, such as immutability and transparency, ensure that medical data remains tamper-proof and accessible only to authorized entities. However, traditional blockchain consensus mechanisms like Proof-of-Work (PoW) and Proof-of-Stake (PoS) present challenges in the context of IoMT and fog computing environments [3]. PoW is notorious for its high energy consumption, making it unsuitable for resource-constrained IoMT devices. On the other hand, PoS, while more energy-efficient, may lead to centralization risks, as nodes with significant stakes dominate the network [4]. To address these challenges, this research proposes a novel approach that integrates a Grey Wolf Optimization (GWO)-enhanced hybrid consensus model within a blockchain framework tailored for fog computing environments. The GWO algorithm dynamically balances the computational demands of PoW and the stake-based validation of PoS, optimizing energy efficiency and scalability. By employing a trust-based miner selection mechanism, the model ensures that nodes are chosen based on their reliability and performance metrics, thereby enhancing the overall security and efficiency of the network. In addition to the hybrid consensus model, this study introduces a Modified Attribute-Based Encryption (ABE) scheme to bolster data privacy and access control. The Modified ABE is designed to be computationally lightweight, facilitating fine-grained access control without imposing significant overhead on IoMT devices. This ensures that sensitive medical data is encrypted and accessible only to authorized personnel, maintaining patient confidentiality and compliance with healthcare regulations.

Experimental evaluations demonstrate that the proposed model significantly reduces communication delays and energy consumption while enhancing throughput compared to existing methods. These improvements underscore the model's potential to provide a scalable, secure, and efficient solution for IoMT applications within fog computing infrastructures. By leveraging the synergistic strengths of blockchain technology, advanced encryption schemes, and machine learning optimization algorithms, this research offers a comprehensive framework to address the pressing challenges of privacy preservation and QoS in modern healthcare systems.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

2. LITERATURE REVIEW

The widespread adoption of fog computing, which extends cloud computing to the network edge, necessitates advanced privacy-preserving models due to its decentralized nature and the sensitive data it processes. Fog computing is ideal for latency-sensitive applications such as IoT, smart cities, and autonomous systems, where real-time processing is crucial. However, ensuring privacy while maintaining high-quality service (QoS) remains a major challenge [1][4]. Traditional models often fail to balance privacy protection with performance requirements.

This literature survey explores state-of-the-art privacy-preserving and QoS-aware models, focusing on blockchain-based and attribute-based approaches for multi-domain systems [8][9]. It examines how these models address privacy concerns, including location, data, and meta-information privacy, while sustaining QoS in fog environments. The integration of machine learning (ML) with blockchain technology is analyzed as a means to enhance both privacy and security in distributed fog networks.

The study evaluates the scalability and efficiency of these models in large-scale, dynamic fog systems, discussing trade-offs between privacy preservation and QoS optimization, especially in resource-constrained settings. Technologies like federated learning and homomorphic encryption are also assessed [12][17]. Additionally, the impact of privacy-preserving techniques on latency-sensitive applications, such as IoT networks and smart city infrastructures, is examined [23].

QoS in fog computing is defined by key performance, security, and resource efficiency metrics. Challenges in implementing privacy-preserving techniques include integration complexities, resource allocation, and maintaining system performance. Trust models and reputation systems play a role in enabling secure collaboration among fog nodes while preserving user privacy. Hybrid approaches combining blockchain and attribute-based encryption are identified as promising solutions for achieving a balance between security and performance [18][23]. The study also investigates regulatory considerations and the potential of adaptive ML-powered privacy mechanisms to optimize privacy settings in real time.

Practical case studies from sectors like healthcare, smart transportation, and industrial IoT highlight the benefits and limitations of existing privacy-preserving techniques in fog computing deployments [23]. By examining hybrid privacy models and emerging technologies, this research provides valuable insights into balancing privacy and performance in fog computing, paving the way for more secure, efficient, and scalable systems.

Key QoS Parameters:

Latency: Delay in data transmission and processing, crucial for real-time applications [24].

Throughput: Volume of data processed per unit time, affecting system efficiency [18] [24].
Energy Efficiency: Optimizing power consumption in resource-constrained fog nodes [18] [24] [25].
Reliability: Ensuring robustness against failures and attacks.
Privacy & Security: Protecting sensitive user data using cryptographic techniques [18].
Resource Allocation: Dynamic task scheduling for CPU, bandwidth, and storage optimization.

Table 1 summarizes the major contributions by the researchers and challenges that still need to address.

Table 1: Major contributions and challenges

Researcher	Major Contribution	Challenges
Liu et al. [29], Jiang et al [31].	Scalability in heterogeneous and mobile mining	Long-term sustainability; Adapting to dynamic environments. Energy Efficiency is not addressed
Huang et al.[25]	Proof-of-Work in permissioned blockchains; Hybrid consensus systems	Defining consensus for security and participation; Designing incentives for different consensus models
Asheralieva and Niyato, [38]	Learning-based resource management; Offloading strategy for blockchain	Security evaluation; Energy Efficiency
Wang et al., [26] Liu et al.	Proof-of-federated-learning consensus mechanism; Sustainable incentive mechanism for blockchain storage	Scalability concerns in federated learning; Privacy preservation; Economic implications
Du et al., [39]	Resource pricing and allocation in MEC-enabled blockchain; Compensation for power loss by Proof-of-Stake consortium blockchain microgrid	Dynamic resource management; Effective pricing mechanisms; Energy Efficiency, optimization
Alofi et al., [40]	Optimizing energy consumption with evolutionary algorithms;	Balancing optimization and system efficiency

Fog computing enables real-time processing but introduces security challenges due to its open architecture and resource constraints. Researchers [10][15] have assessed existing security models to mitigate these risks.

Security Models

- **MOMKT**: Achieves 95% accuracy in detecting intrusions with high energy efficiency [41].
- **Content-Aware Filtering**: Improves attack mitigation but has scalability limitations [41].
- **Hybrid Approaches**: CP-ABE achieves 98% efficiency in unauthorized access prevention [42].

Research Gaps

Key gaps in existing studies include:

- Limited evaluation of privacy preservation models in fog computing [22-25].
- Lack of blockchain-based security frameworks [27].
- Absence of attribute-based privacy integrated with blockchain [27-30].
- No machine learning-based QoS optimization models for fog privacy [30-32].
- Insufficient integration of machine learning for enhanced security and QoS [33].

Machine learning-powered blockchain solutions can address these challenges, ensuring secure and high-QoS fog computing.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

3. METHODOLOGY

QoS-Aware Privacy Preservation in Fog Computing for IoMT

This research proposes a QoS-aware, attribute-based privacy preservation system for fog computing in IoMT (Internet of Medical Things). The approach integrates fog computing, blockchain, attribute-based encryption (ABE), and machine learning (ML) to enhance security, privacy, and system efficiency.

System Design and Architecture

The framework is structured as follows:

- **IoMT Devices**: Collect real-time health data using wearables (e.g., ECG monitors, smart watches).
- **Fog Nodes**: Handle local data processing, reducing latency.
- **Blockchain Layer**: Ensures secure, immutable medical records.
- **Machine Learning Layer**: Enhances QoS by dynamically managing resources.

Hybrid Blockchain Consensus (PoS & PoW)

To balance security and efficiency, a hybrid Proof of Work (PoW) and Proof of Stake (PoS) model is implemented:

- **PoW**: Guarantees blockchain integrity through computationally intensive validation.
- **PoS**: Enhances energy efficiency by selecting validators based on their stake.

Additionally, smart contracts enforce attribute-based access control (ABAC) to secure sensitive medical data while ensuring transaction integrity and traceability.

Privacy Preservation with Attribute-Based Encryption (ABE)

A Modified ABE scheme strengthens privacy by enforcing fine-grained access control:

1. Encryption: Data is encrypted based on user attributes.
2. Access Control: Policies define decryption eligibility.
3. Key Management: Secure key generation and storage on the blockchain.
4. Blockchain Integration: Encrypted data and keys are stored immutably.
5. Decryption: Only authorized users can retrieve and decrypt data.

This integration ensures secure, decentralized access control in fog-based IoMT applications.

Machine Learning Optimization with Grey Wolf Optimizer (GWO)

Machine learning is applied to optimize latency, throughput, and resource allocation using nature-inspired optimization algorithms:

- Grey Wolf Optimizer (GWO): Mimics the hunting behavior of grey wolves to enhance QoS in communication networks.

This research presents a comprehensive, scalable, and secure framework for privacy-preserving, high-QoS fog computing in healthcare, smart cities, and industrial IoT.

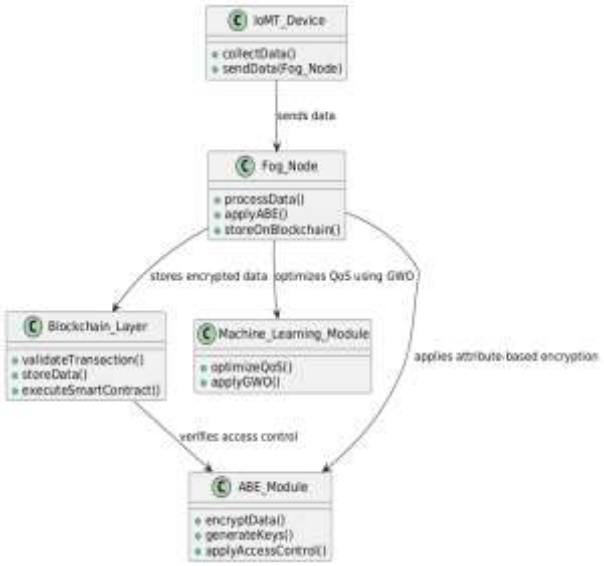


Fig1: Proposed Model

DataSet

In this research, a synthetic dataset is generated using NumPy and Pandas to simulate patient data for evaluating the proposed QoS-aware privacy preservation framework in IoMT systems. Initially, the HeartPy dataset with heart rate data was considered, but due to its lack of patient-specific information, a custom dataset was created, incorporating patient heart rate, personal details, and treating doctor information. This synthetic dataset provides a controlled environment for proof-of-concept validation without relying on external data sources, ensuring the system's ability to securely process and analyze medical data while maintaining high QoS. The dataset comprises 50,000 patients, 5,000 doctors, and 500 hospitals, structured to reflect real world healthcare relationships while ensuring privacy, consistency, and completeness.

Each patient's data is stored in an individual blockchain block using Modified Attribute Based Encryption (ABE), ensuring secure and fine grained access control. This dataset serves as a realistic clinical data model for testing and analysis. The dataset attributes are detailed in Table 2.

Table 2:Dataset Information

Dataset	Attributes
Patient Information	Patient_ID, Name, Age, Gender, id_doc_type, id_doc_number, Location, Town, Hospital_ID, Assigned_Doctors, Heart_Rate_Samples, Clinical_Parameters, Emergency_Access(yes/no)
Doctor Information	Doctor_ID, Name, Specialization, Registration_Number, Qualification, Experience, Assigned_Hospital
Hospital	Hospital_ID, Name, Address, Contact, Doctor_List, Emergency_Access_Patients

The synthetic dataset provides a realistic, scalable, and privacy-compliant alternative to real-world healthcare records. It enables attribute-based encryption (ABE) for secure blockchain storage, making it an ideal dataset for research in fog computing privacy, security, and Quality of Service (QoS).

3.1 System Evaluation and Testing

The proposed system is evaluated through extensive testing of the security, privacy, and QoS performance.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

Evaluation Methods:

• **Security Evaluation:** The privacy and security of medical data are tested by varying percentage of attacked nodes from 2% to 20%. The effectiveness of the ABE encryption and the hybrid PoS/PoW blockchain approach is assessed by simulating attack and analyzing the system's resilience.

• **QoS Evaluation:** Key QoS metrics such as latency, throughput and energy consumption, are evaluated using dataset generated. The system is tested under varying conditions to assess the performance of the machine learning algorithms in optimizing resource allocation and minimizing delays.

• **Performance Testing**: The blockchain layer's performance is evaluated by measuring block validation times**,** transaction throughput**,** and block propagation delays**.**

4. DESIGN AND IMPLEMENTATION OF BLOCKCHAIN USING POW AND POS CONSENSUS

Blockchain technology has become a transformative solution for enhancing security, transparency, and trust in distributed systems. In fog computing, it offers a decentralized approach to securing data and transactions across fog nodes. However, conventional blockchain mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) encounter limitations, including high energy consumption and scalability constraints. This chapter explores the design and implementation of a hybrid blockchain model that integrates PoW and PoS consensus mechanisms to overcome these challenges, improving both security and performance in fog computing environments. Blockchain is highly applicable in fog computing for several reasons:

- Decentralized Trust: Blockchain eliminates the need for a central authority, enabling secure peer-to-peer transactions among fog nodes.
- Data Integrity: Cryptographic hashing ensures that data stored on the blockchain is tamper-proof.
- Authentication and Authorization: Blockchain provides a robust framework for verifying the identities of fog nodes and ensuring only authorized entities can access resources.
- Auditability: The immutable ledger of blockchain allows for traceability and accountability of transactions.

By integrating blockchain into fog computing, it becomes possible to address vulnerabilities such as man-in-the-middle attacks, unauthorized data access, and node impersonation.

While blockchain offers significant benefits in fog computing, its implementation comes with several challenges:

Resource Limitations: Fog nodes have constrained computational and storage capacities, making traditional blockchain operations difficult to sustain.

Latency Issues: Consensus mechanisms like PoW introduce delays, which can negatively impact real-time fog applications.

High Energy Consumption: The computational demands of PoW are energy-intensive, making it unsuitable for resource-constrained fog environments.

Scalability Concerns: As the number of fog nodes grows, the blockchain network must efficiently scale to maintain optimal performance.

Interoperability Challenges: Integrating blockchain with diverse fog architectures and communication protocols requires seamless compatibility and standardization.

PoW and PoS-Based Blockchain Implementation

PoW is a consensus mechanism where miners compete to solve complex cryptographic puzzles to validate transactions and append blocks to the blockchain. While PoW ensures strong security and immutability, it suffers from high energy consumption and increased latency.

PoS selects validators based on the amount of cryptocurrency they hold and are willing to stake. Unlike PoW, PoS eliminates the need for intensive computations, making it more energy-efficient while enabling faster transaction processing.

Hybrid PoW-PoS Model

To optimize both security and efficiency, a hybrid approach is adopted that leverages the advantages of PoW and PoS:

PoW is utilized for the initial block validation, ensuring robust security and resistance against malicious attacks.

PoS is applied for subsequent validations, reducing computational overhead, lowering energy consumption, and enhancing transaction speed.

This hybrid model enhances blockchain performance in fog computing by improving scalability, minimizing latency, and maintaining security.

Algorithm for Proposed Hybrid Blockchain Implementation (PoW and PoS)

Algorithm for Hybrid PoW-PoS Blockchain Consensus

Input:

- **Tx**: Set of pending transactions
- **B**: Blockchain ledger
- **S**: Stake values of participating nodes

Output:

- **B'**: Updated blockchain with the newly added block

Algorithm: Hybrid PoW-PoS Consensus

Transaction Initialization

Collect pending transactions **Tx** from the network.

Form a candidate block **B_new** containing **Tx**.

PoW Phase (Initial Block Validation for Security)

Select a miner **M** from the network.

Miner solves a cryptographic puzzle:

$$H\left(B_{prev} \,||\, Tx \,||\, N\right) < T$$

where:

- H is the hash function.
- B_{prev} is the previous block's hash.
- N is the nonce.
- T is the target difficulty threshold.

If **valid**, miner broadcasts the solution to the network.

PoS Phase (Efficient Validation and Finalization)

Select a committee of **k** validators based on stake **S**:

$$P_i = \frac{S_i}{\sum S}$$

where:

- P_i is the probability of validator **i** being selected.
- S_i is the stake of validator **i**.

Validators verify transactions in **B_new**.

If $\sum V > \theta$, where V is the total votes and θ is the consensus threshold, finalize **B_new**.

Block Addition

Append **B_new** to blockchain:

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

$B' = B \cup B_{new}$

4.2. Update stake balances for validators.

6. **Repeat**: Continue for the next block.

5. DESIGN AND IMPLEMENTATION OF MODIFIED ABE FOR PRIVACY PRESERVATION

Attribute-Based Encryption (ABE) is a public-key encryption technique that provides fine-grained access control by assigning access permissions based on attributes rather than user identities. This approach is well-suited for secure data sharing among multiple users with different access privileges. The Modified Attribute-Based Encryption (ABE) Scheme for blockchain ensures that only users with the required attributes can access encrypted data. The encryption and decryption processes are securely integrated with the blockchain for key management and retrieval.

Process Workflow:

Input: Data to be shared, Access control policies, Attribute set and public parameters

Encryption & Storage:

1. **Key Generation:**
   - A master key is generated using public parameters and SHA-256 for secure initialization.
   - The hashes are combined iteratively using an AND operation to derive a single key.
   - The key is adjusted to 32 bytes and encoded in Base64 format.
   - A Fernet object is initialized with the derived key for encryption.
2. **Encryption:**
   - Data is encrypted using the attribute set and ABE encryption algorithm.
   - An access structure is defined based on policies and attributes.
   - A secret key is generated for each authorized user using the master key and access structure.
3. **Blockchain Integration:**
   - The encrypted data and corresponding secret keys are stored securely on the blockchain.

- **Decryption & Access Control:**

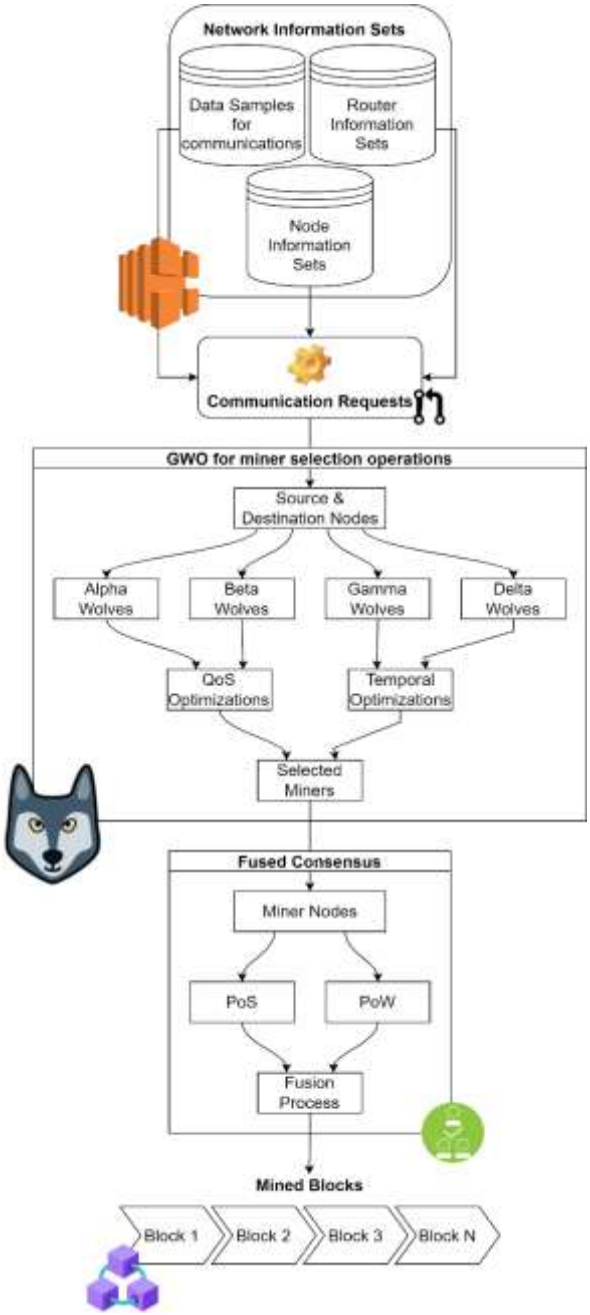
4. **Access Request:**
   - When a user requests access, their attributes are verified against the stored access structure.
   - The corresponding **secret key** is retrieved from the blockchain.
5. **Decryption:**
   - The data is decrypted using the retrieved secret key and ABE decryption algorithm.

- **Output:**
- The decrypted data is provided only to authorize users based on their attributes.

6. DESIGN AND IMPLEMENTATION OF QOS OPTIMIZATION USING MACHINE LEARNING TECHNIQUES

In fog computing, Quality of Service (QoS) is crucial due to the distributed and resource-constrained nature of fog nodes. Optimizing QoS requires addressing key factors such as latency, bandwidth, computational efficiency, and reliability.

Figure 2. Design of the proposed model for efficient mining operations



Machine learning (ML) offers an effective approach for dynamic resource allocation and QoS enhancement. This chapter presents a QoS optimization framework using the Grey Wolf Optimizer (GWO) to improve throughput, reduce delays, and enhance overall system performance in fog computing environments. Machine learning enables intelligent decision-making and predictive analytics in distributed systems, making it ideal for adaptive resource management in fog computing.

Key Benefits:

- **Energy Efficiency:** Reduces power consumption through optimized resource allocation.
- **Latency Reduction:** Dynamically schedules tasks to minimize response times.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

- **Throughput Enhancement:** Improves overall system performance by optimizing resource distribution.

Grey Wolf Optimizer (GWO) for QoS Optimization

The Grey Wolf Optimizer (GWO) is a nature-inspired optimization algorithm that simulates the hunting behaviour of grey wolves. It is well-suited for multi-objective optimization in fog computing, balancing latency, throughput, and energy efficiency.

GWO Optimization Process:

1. **Initialization:**
   - Generate an initial population of solutions (wolves).
   - Define objective functions (e.g., minimize latency, maximize throughput).
2. **Leadership Hierarchy Formation:**
   - Identify alpha, beta, and delta wolves based on their fitness values.
3. **Position Update:**
   - Adjust the positions of wolves using mathematical models that mimic encircling, hunting, and attacking prey.
4. **Convergence Check:**
   - Repeat iterations until an optimal solution is reached or a stopping criterion is met.

Figures 2 illustrate the proposed model for efficient mining operations.

7. RESULTS AND DISCUSSION

The proposed model combines Proof-of-Work (PoW) and Proof-of-Stake (PoS) to create a hybrid blockchain that improves mining efficiency and addresses the limitations of standalone consensus mechanisms. Implemented in Python and simulated on Google Colab using a synthetic patient dataset, the system evaluates a QoS-aware Attribute-Based Privacy Preservation framework for Fog Computing. The implementation leverages cryptographic and blockchain libraries, incorporating:

- Trust-based miner selection
- Grey Wolf Optimizer (GWO) for node trust evaluation
- Attribute-Based Encryption (ABE) for secure data sharing

This ensures enhanced security, efficient consensus, and optimized resource utilization in blockchain-based fog computing environments.

The simulation utilized a synthetic dataset containing patient vital signs, including heart rate data, along with clinical parameters and doctor information for 50,000 patients. The proposed hybrid consensus model was evaluated based on the following key performance metrics:

- Blockchain Throughput (Tx/s): Number of transactions processed per second.
- Transaction Processing Speed (TPS): Successfully validated transactions per second.
- Packet Delivery Ratio (PDR): Ratio of successfully transmitted packets to total packets sent.
- Mining Delay: Average time required to validate and append a block to the blockchain.
- Security Evaluation: Impact of attack probability on blockchain integrity and data confidentiality.

Modified ABE consistently performs better than Traditional ABE for all data sizes.

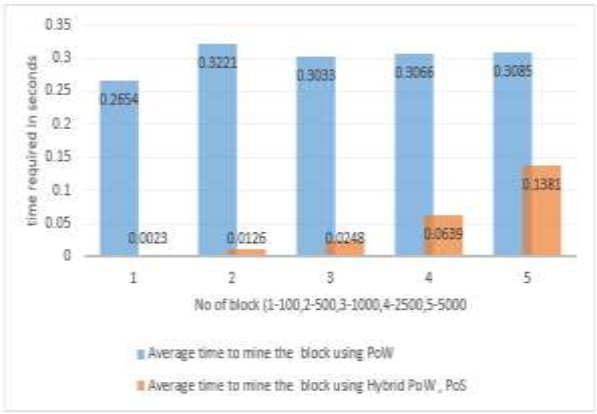
Simulation Results and Analysis of proposed PoW and PoS hybrid consensus approach for Blockchain implementation:

Table 4 presents a comparative analysis of different blockchain models, measuring the average block mining time across varying blockchain sizes, with time recorded in seconds.

Table: Average time to mine the blocks using various approaches

Number of blocks in the Blockchain	PoW approach		Proposed hybrid PoW and PoS	
	Average time to mine the block	Total Time Required	Average time to mine the block	Total Time Required
100	0.2654s	26.5825s	0.0023	0.3217s
500	0.3221s	161.2792s	0.0126	6.5180s
1000	0.3033s	303.7354s	0.0248s	25.3494s
2500	0.3066S	767.6972s	0.0639s	160.9989s
5000	0.3085s	1597.643s	0.1381	692.8182s

PoW is significantly slower because of its computationally intensive nature, as illustrated in Fig. 5. The hybrid approach considerably decreases the overall mining time, with the ML-optimized version yielding the best performance.



Simulation Results and Analysis of proposed modified ABE in blockchain:

Table 5 and 6 shows the comparative analysis of execution of AES, traditional ABE and proposed Modified ABE by varying data size to be encrypted from 1 MB to 100 MB.

Table: Encryption time comparison

Data Size In MB	AES Encryption time (seconds)	Traditional ABE Encryption time (seconds)	Modified ABE Encryption time (seconds)
1	0.03471	0.018164	0.011528
5	0.17344	0.069698	0.054246
10	0.49972	0.350899	0.309402
20	0.69235	0.284355	0.251531
50	1.7786	0.85201	0.712643
100	3.55436	1.541922	1.493984

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 136 – 146, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1012

• Modified ABE performs better than AES for larger data sizes, particularly at 50MB and 100MB, where AES's encryption and decryption times are much higher.

Table: Decryption time comparison

Data Size In MB	AES Decryption time (seconds)	Traditional ABE Decryption time (seconds)	Modified ABE Decryption time (seconds)
1	0.03317	0.013071	0.00988
5	0.16553	0.052335	0.05011
10	0.33035	0.243725	0.22223
20	0.70438	0.278316	0.21971
50	1.67702	0.720687	0.66962
100	3.34859	2.638511	1.43718

Fig: Encryption Time Comparison

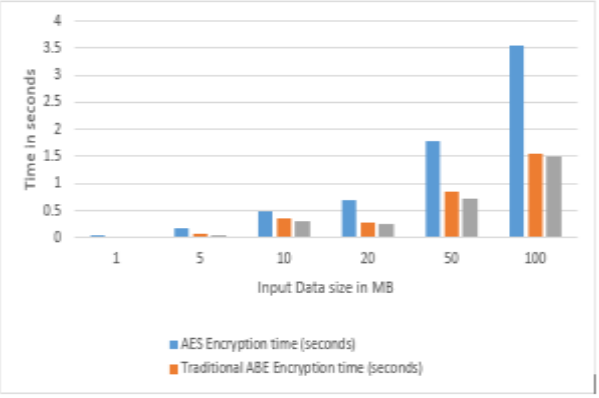
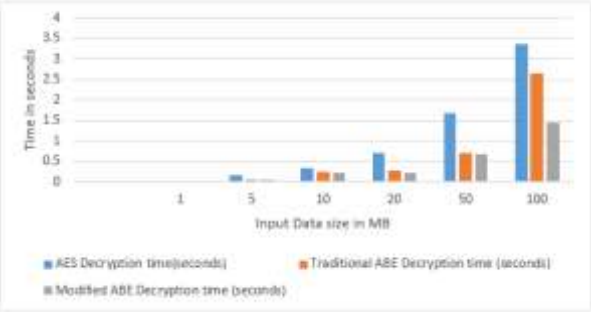


Fig 7: Decryption time comparison



As shown in Fig. 6, the Modified ABE algorithm achieves an average encryption time reduction of approximately 9% compared to the Traditional ABE algorithm.

The proposed Modified ABE encryption algorithm significantly reduced decryption time, with an average decrease of 33.90%, as shown in Fig. 7, enhancing its applicability for real-time fog computing environments. The blockchain-based privacy-preserving model integrates ABE encryption with hybrid PoW-PoS mining to strengthen security, access control, and QoS. Experimental results demonstrate high efficiency, low latency, and enhanced data security, making it well-suited for secure fog computing applications in IoMT and healthcare.

Simulation Results and Analysis of Machine Learning implementation in Blockchain architecture to improve QoS

Table 7 compares the Proposed Hybrid PoW-PoS approach with the Machine Learning Optimized Hybrid PoW-PoS approach based on the average block mining time and the total time required for varying numbers of blocks in the blockchain.

Table 7: Comparative analysis of Hybrid and Machine Learning Approach

Number of blocks in the Blockchain	Proposed hybrid PoW and PoS		Machine learning Optimized hybrid PoW and PoS	
	Average time to mine the block	Total Time Required	Average time to mine the block	Total Time Required
100	0.0023s	0.3217s	0.0004s	0.0487s
500	0.0126s	6.5180s	0.0004s	0.3388s
1000	0.0248s	25.3494s	0.0004s	5.6025s
2500	0.0639s	160.9989s	0.0004s	11.2174s
5000	0.1381s	692.8182s	0.0004s	13.3629s
10000	0.3041s	3043.2345s	0.0004s	18.4568s
20000	0.6510s	13020.457s	0.0005s	22.3478s
50000	1.3923s	69619.237s	0.0006s	37.7245s

The findings highlight the efficiency gains achieved through the integration of machine learning into the hybrid PoW-PoS approach. The Proposed Hybrid PoW-PoS model exhibits an increasing trend in average mining time per block as the number of blocks grows, whereas the Machine Learning Optimized Hybrid PoW-PoS maintains a consistently lower and stable average mining time. Similarly, the total mining time for the Proposed Hybrid PoW-PoS increases exponentially with the number of blocks, while the ML-optimized variant significantly reduces total time, even for larger block sizes. For instance, for 5000 blocks, the Machine Learning Optimized Hybrid PoW-PoS completes mining in just 13.3629 seconds—approximately 98.1% faster than the Hybrid PoW-PoS, which takes 692.8182 seconds. This substantial improvement demonstrates the scalability and high performance of machine learning integration in blockchain mining.

The hybrid model further enhances efficiency through a trust-based miner selection process leveraging Grey Wolf Optimization (GWO), which prioritizes nodes with superior temporal performance under heterogeneous mining conditions. By optimizing resource utilization and reliability, this approach reduces mining delays and improves overall blockchain efficiency. The GWO-based model employs a temporal fitness function to assess nodes based on mining delay, energy consumption, throughput, and efficiency, ensuring high-QoS node selection. This not only accelerates consensus but also enhances blockchain reliability. Additionally, self-correcting mechanisms dynamically adapt to network changes, maintaining optimal performance even in adversarial conditions.

Comparative Analysis

By integrating hybrid consensus with trust-based miner selection, the proposed model exhibits superior QoS resilience compared to existing approaches such as DRLBTS, QoS_ML_DSS, and SLGAF. Its efficiency is validated through QoS metric evaluations under varying attacker node percentages, ranging from 2% to 20%. The evaluation was

conducted on a simulated network of 1000 nodes, with QoS values computed over a dataset of 50,000 blocks.

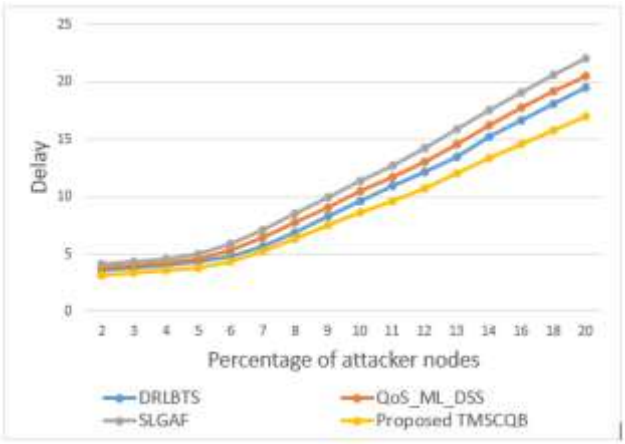
The results demonstrate the model's ability to accurately predict performance, reinforcing its potential for large-scale deployment across diverse applications. Table 8 presents the measured end-to-end delays (D) under multiple Sybil attack scenarios, highlighting the model's capability to maintain high QoS even in adversarial conditions. This evaluation underscores the robustness of the proposed hybrid consensus mechanism, making it well-suited for environments demanding both high security and performance.

In summary, the proposed model represents a significant advancement in blockchain consensus mechanisms by integrating hybrid consensus, trust-based miner selection, and self-correcting capabilities. These innovations collectively enhance mining speed, reduce delays, and improve QoS, positioning the model as a viable solution for real-world blockchain applications.

Table 8 Communication delay required under different attacks

NA (%)	D (ms) DRLBTS	D (ms) QoS_ML_DSS	D (ms) SLGAF	D (ms) Proposed TMSCQB
2	3.61	3.81	4.08	3.13
3	3.84	4.04	4.31	3.33
4	4.06	4.27	4.59	3.53
5	4.30	4.61	5.04	3.82
6	4.74	5.28	5.85	4.35
7	5.62	6.38	7.09	5.22
8	6.92	7.73	8.52	6.34
9	8.29	9.12	9.97	7.48
10	9.65	10.47	11.37	8.60
11	10.92	11.73	12.72	9.67
12	12.13	13.06	14.19	10.76
13	13.52	14.62	15.85	12.03
14	15.19	16.23	17.53	13.38
16	16.67	17.72	19.09	14.62
18	18.07	19.16	20.61	15.81
20	19.48	20.52	22.07	16.97

Figure 8 Comparative analysis of obtained Communication Delay



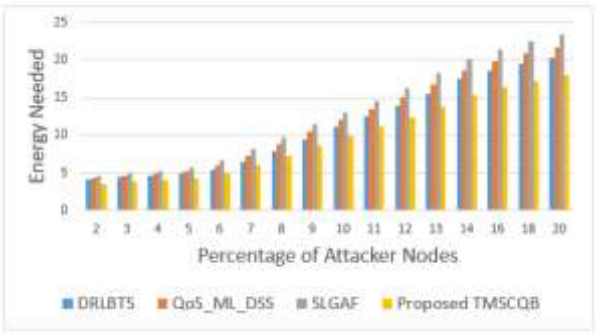
The evaluation results, illustrated in Figure 8, confirm the superior performance of the proposed Grey Wolf Optimization (GWO)-powered approach in minimizing communication delays, even under adversarial attacks. The model achieves reductions of 10.5% compared to DRLBTS, 12.4% compared to QoS_ML_DSS, and 16.5% compared to SLGAF, demonstrating its robustness and efficiency. This improvement is driven by two key factors: Effective Miner Selection, where the GWO-based selection prioritizes nodes with superior temporal performance, optimizing mining delay, energy consumption, throughput, and efficiency; and Low-Complexity Hybrid Consensus, where the PoW-PoS mechanism reduces computational and communication complexity, accelerating block propagation and validation. Additionally, as shown in Table 8, the GWO-powered approach significantly enhances energy efficiency by minimizing redundant computations and streamlining consensus. These advancements make the proposed model highly practical for real-world blockchain deployments, especially in resource-constrained environments or scenarios with high attack probabilities. By ensuring both low delay and energy consumption, the GWO-powered approach establishes itself as a scalable, high-performance solution for blockchain networks requiring enhanced QoS and resilience.

Table 9: The energy requirements for communication under varying attack scenarios

NA (%)	E (mJ) DRLBTS	E (mJ) QoS_ML_DSS	E (mJ) SLGAF	E (mJ) Proposed TMSCQB
2	4.16	4.37	4.68	3.62
3	4.43	4.64	4.96	3.84
4	4.68	4.91	5.27	4.07
5	4.96	5.31	5.79	4.39
6	5.44	6.07	6.73	4.98
7	6.45	7.34	8.15	6.00
8	7.94	8.90	9.80	7.29
9	9.51	10.49	11.46	8.61
10	11.08	12.03	13.07	9.91
11	12.54	13.49	14.62	11.13
12	13.94	15.01	16.31	12.39
13	15.54	16.81	18.22	13.84
14	17.47	18.67	20.15	15.40
16	18.60	19.84	21.41	16.37
18	19.52	20.87	22.51	17.21
20	20.33	21.70	23.44	17.91

The evaluation results in Table 9 and Fig. 9 highlight the significant energy efficiency of the proposed Grey Wolf Optimization (GWO)-powered approach in blockchain communication.

Fig 9: The energy requirements for communication under varying attacks



The model reduces energy consumption by 8.3% compared to DRLBTS, 9.5% compared to QoS_ML_DSS, and 10.4% compared to SLGAF, even under attack scenarios. This

improvement enhances the sustainability and efficiency of blockchain systems, making it ideal for resource-constrained environments.

Similarly, the throughput obtained for communication can be observed from Table 10 as follows,

Table 10 Throughput obtained for communication under different attacks

NA (%)	THR (kbps) DRLBTS	THR (kbps) QoS_ML_DSS	THR (kbps) SLGAF	THR (kbps) Proposed TMSCQB
2	1729	1843	1993	2393
3	1659	1772	1913	2290
4	1581	1685	1820	2177
5	1485	1586	1712	2052
6	1321	1429	1548	1914
7	1186	1276	1387	1773
8	1067	1146	1244	1600
9	942	1023	1113	1431
10	808	891	977	1254
11	674	756	834	1084
12	548	624	694	935
13	463	516	573	803
14	421	451	493	683
16	399	418	450	589
18	376	395	423	530
20	354	372	399	491

As shown in Fig. 10, the evaluation results highlight the substantial improvement in throughput achieved by the proposed Grey Wolf Optimization (GWO)-powered model. It outperforms DRLBTS by 23.5%, QoS_ML_DSS by 19.4%, and SLGAF by 18.5% under various attack conditions. This notable enhancement demonstrates the model's robustness and efficiency in sustaining high data rates across diverse communication scenarios, even in the presence of adversarial threats.

8. CONCLUSION AND FUTURE SCOPE

The proposed Grey Wolf Optimization (GWO)-powered hybrid consensus model marks a significant advancement in blockchain-based fog computing by addressing key challenges in energy efficiency, security, and scalability within dynamic and resource-constrained environments. By integrating Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms with trust-based miner selection via GWO, the model optimizes resource utilization, enhances system robustness, and ensures high Quality of Service (QoS).

To reinforce privacy preservation and access control, the framework incorporates a Modified Attribute-Based Encryption (ABE) scheme, improving computational efficiency and enabling lightweight attribute-based key generation. This ensures that only authorized entities can access sensitive medical and fog computing data while maintaining fine-grained, decentralized access control.

Experimental evaluations validate the model's effectiveness, demonstrating reductions of 10.5%–16.5% in communication delay, improvements of 8.3%–10.4% in energy efficiency, and enhancements of 18.5%–23.5% in throughput compared to state-of-the-art approaches such as DRLBTS, QoS_ML_DSS, and SLGAF. Additionally, temporal parameter optimization using GWO strengthens resilience against adversarial threats, including Sybil attacks, ensuring adaptive security and trust management.

With a low-complexity hybrid consensus mechanism and lightweight cryptographic enhancements, the model is well-suited for real-time applications in resource-constrained environments. The integration of GWO-optimized consensus and Modified ABE establishes a strong foundation for scalable, privacy-aware, and resilient blockchain solutions in domains such as healthcare, smart cities, and industrial IoT.

Future research can further enhance the proposed model by integrating quantum-resistant cryptographic algorithms and AI-driven anomaly detection to improve security against evolving threats. Cross-chain interoperability with platforms like Hyperledger and Ethereum can increase adaptability, while advanced privacy-preserving techniques such as homomorphic encryption and multi-authority ABE can strengthen secure data sharing. Additionally, federated learning integration can enable privacy-preserving machine learning in fog computing, ensuring collaborative intelligence without compromising user data privacy.

9. REFERENCES

[1] Yi, Shanhe & Qin, Zhengrui & Li, Qun. (2015). Security and Privacy Issues of Fog Computing: A Survey. 685-695. 10.1007/978-3-319-21837-3_67.

[2] Mukherjee, M., et al. (2018). Security and privacy in fog computing: Challenges. *IEEE Communications Magazine*, *56*(5), 36–42.

[3] Johri, P., Balu, V., Jayaprakash, B., Jain, A., Thacker, C., & Kumari, A. (2023). Quality of service-based machine learning in fog computing networks for e-healthcare services with data storage system. Soft Computing. https://doi.org/10.1007/s00500-023-09041-8

[4] Ahmad, R. W., et al. (2021). Blockchain for IoT-based smart homes: A comprehensive survey. *Journal of Network and Computer Applications*, *186*, 103090.

[5] Hammi, B., et al. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142.

[6] Resul Das, Muhammad Muhammad Inuwa, A review on fog computing: Issues, characteristics, challenges, and potential applications,Telematics and Informatics Reports, Volume 10,2023,100049,ISSN 2772-5030,https://doi.org/10.1016/j.teler.2023.100049.

[7] Pengfei Hu, Sahraoui Dhelim, Huansheng Ning, Tie Qiu,Survey on fog computing: architecture, key technologies, applications and open issues, Journal of Network and Computer Applications, Volume 98, 2017, Pages 27-42, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2017.09.002.

[8] Sabireen H., Neelanarayanan V., A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges, ICT Express, Volume 7, Issue 2, 2021, Pages 162-176, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2021.05.004.

[9] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog Computing and the Internet of Things: A Review. Big Data and Cognitive Computing, 2(2), 10. https://doi.org/10.3390/bdcc2020010

[10] Charith Perera, Yongrui Qin, Julio C. Estrella, Stephan Reiff-Marganiec, and Athanasios V. Vasilakos. 2017. Fog Computing for Sustainable Smart Cities: A Survey. ACM Comput. Surv. 50, 3, Article 32 (May 2018), 43 pages. https://doi.org/10.1145/3057266

[11] F. A. Kraemer, A. E. Braten, N. Tamkittikhun and D. Palma, "Fog Computing in Healthcare–A Review and Discussion," in IEEE Access, vol. 5, pp. 9206-9222, 2017, doi: 10.1109/ACCESS.2017.2704100.

[12] M. Aazam, S. Zeadally and K. A. Harras, "Deploying Fog Computing in Industrial Internet of Things and Industry 4.0," in IEEE Transactions on Industrial

Informatics, vol. 14, no. 10, pp. 4674-4682, Oct. 2018, doi: 10.1109/TII.2018.2855198

[13] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 416-464, Firstquarter 2018, doi: 10.1109/COMST.2017.2771153

[14] Alzahrani, N., & Bulusu, N. (2018). Block-Supply Chain: A new anti-counterfeiting supply chain using NFC and blockchain. *Proceedings of the ACM International Conference on Distributed Ledger Technology*.

[15] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," 2016 IEEE 18th International Conference on High Performance Computing and Communications; 2016, pp. 1392-1393, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[16] Jun Feng, Laurence T. Yang, Nicholaus J. Gati, Xia Xie, Benard S. Gavuna, Privacy-preserving computation in cyber-physical-social systems: A survey of the state-of-the-art and perspectives, Information Sciences, Volume 527, 2020, Pages 341-355, ISSN 0020-0255,https://doi.org/10.1016/j.ins.2019.07.036.

[17] Johri, P., Balu, V., Jayaprakash, B., Jain, A., Thacker, C., & Kumari, A. (2023). Quality of service-based machine learning in fog computing networks for e-healthcare services with data storage system. Soft Computing. https://doi.org/10.1007/s00500-023-09041-8

[18] Norah Alsaeed, Farrukh Nadeem, Faisal Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing", Future Generation Computer Systems, Volume 151,2024,Pages 162-181,https://doi.org/10.1016/j.future.2023.09.032

[19] Johri, P., Balu, V., Jayaprakash, B., Jain, A., Thacker, C., & Kumari, A. (2023). Quality of service-based machine learning in fog computing networks for e-healthcare services with data storage system. Soft Computing. https://doi.org/10.1007/s00500-023-09041-8

[20] Lakhan, A., Mohammed, M.A., Nedoma, J. et al. DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system. Sci Rep 13, 4124 (2023). https://doi.org/10.1038/s41598-023-29170-2

[21] Norah Alsaeed, Farrukh Nadeem, Faisal Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing",Future Generation Computer Systems,Volume 151,2024,Pages 162-181,https://doi.org/10.1016/j.future.2023.09.032

[22] Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. Sensors, 22(3), 927. https://doi.org/10.3390/s22030927

[23] Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., & Zanolini, L. (2020). A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. Mathematics, 8(10), 1782. https://doi.org/10.3390/math8101782

[24] Chopade, S.S., Gupta, H.P. & Dutta, T. Survey on Sensors and Smart Devices for IoT Enabled Intelligent Healthcare System. Wireless Pers Commun 131, 1957–1995 (2023). https://doi.org/10.1007/s11277-023-10528-8

[25] L. Huang, G. Li, J. Wu, L. Li, J. Li and R. Morello, "Software-defined QoS provisioning for fog computing advanced wireless sensor networks," 2016 IEEE SENSORS, Orlando, FL, USA, 2016, pp. 1-3, doi: 10.1109/ICSENS.2016.7808814

[26] C. Zhou, A. Fu, S. Yu, W. Yang, H. Wang and Y. Yang, "Privacy-Preserving Federated Learning in Fog Computing," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 10782-10793, Nov. 2020, doi: 10.1109/JIOT.2020.2987958.

[27] M. S. Pardeshi and S. -M. Yuan, "SMAP Fog/Edge: A Secure Mutual Authentication Protocol for Fog/Edge," in IEEE Access, vol. 7, pp. 101327-101335, 2019, doi: 10.1109/ACCESS.2019.2930814

[28] J. Wu, M. Dong, K. Ota, J. Li and Z. Guan, "FCSS: Fog-Computing-based Content-Aware Filtering for Security Services in Information-Centric Social Networks," in IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 4, pp. 553-564, 1 Oct.-Dec. 2019, doi: 10.1109/TETC.2017.2747158

[29] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu and Y. Liu, "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 3-12, Feb. 2018, doi: 10.1109/TETCI.2017.2764109.

[30] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie and R. H. Deng, "Lightweight and Privacy-Aware Fine-Grained Access Control for IoT-Oriented Smart Health," in *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6566-6575, July 2020, doi: 10.1109/JIOT.2020.2974257

[31] Tong Li, Chongzhi Gao, Liaoliang Jiang, Witold Pedrycz, Jian Shen, Publicly verifiable privacy-preserving aggregation and its application in IoT, Journal of Network and Computer Applications, Volume 126, 2019, Pages 39-44, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.09.018.

[32] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au and X. Luo, "A Survey on Access Control in Fog Computing," in *IEEE Communications Magazine*, vol. 56, no. 2, pp. 144-149, Feb. 2018, doi: 10.1109/MCOM.2018.1700333.

[33] Kukreti, A. (2023). Access control and authentication for secure systems and networks. *NeuroQuantology*. https://doi.org/10.48047/nq.2022.20.5.nq22814

[34] D. Singh, S. Sinha and V. Thada, "Review of Attribute Based Access Control (ABAC) Models for Cloud Computing," *2021 International Conference on Computational Performance Evaluation (ComPE)*, Shillong, India, 2021, pp. 710-715, doi: 10.1109/ComPE53109.2021.9752139.

[35] Shruti, Rani, S., Sah, D. K., & Gianini, G. (2023). Attribute-Based Encryption Schemes for Next Generation Wireless IoT Networks: A Comprehensive Survey. Sensors, 23(13), 5921. https://doi.org/10.3390/s23135921

[36] Namane, S., & Ben Dhaou, I. (2022). Blockchain-Based Access Control Techniques for IoT Applications. Electronics, 11(14), 2225. https://doi.org/10.3390/electronics11142225

[37] Mehdi Sookhak, Mohammad Reza Jabbarpour, Nader Sohrabi Safa, F. Richard Yu, Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues, Journal of Network and Computer Applications, Volume 178, 2021, 102950, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102950.

[38] A. Asheralieva and D. Niyato, "Throughput-Efficient Lagrange Coded Private Blockchain for Secured IoT Systems," in *IEEE Internet of Things Journal*, vol. 8, no.

19, pp. 14874-14895, 1 Oct.1, 2021, doi: 10.1109/JIOT.2021.3071563.

[39] J. Du *et al*., "Resource Pricing and Allocation in MEC Enabled Blockchain Systems: An A3C Deep Reinforcement Learning Approach," in *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 33-44, 1 Jan.-Feb. 2022, doi: 10.1109/TNSE.2021.3068340

[40] A. Alofi, M. A. Bokhari, R. Bahsoon and R. Hendley, "Optimizing the Energy Consumption of Blockchain-Based Systems Using Evolutionary Algorithms: A New Problem Formulation," in *IEEE Transactions on Sustainable Computing*, vol. 7, no. 4, pp. 910-922, 1 Oct.-Dec. 2022, doi: 10.1109/TSUSC.2022.3160491

[41] A. Mourad, H. Tout, O. A. Wahab, H. Otrok and T. Dbouk, "Ad Hoc Vehicular Fog Enabling Cooperative Low-Latency Intrusion Detection," in *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 829-843, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008488

[42] Zhao, Y., Ren, M., Jiang, S. et al. An efficient and revocable storage CP-ABE scheme in the cloud computing. Computing 101, 1041–1065 (2019). https://doi.org/10.1007/s00607-018-0637-2