[1]Hitesh Gehani,
[2]Shubhangi Rathkanthiwar

IBSBMPC: Design of an Iterative & highly Secure Bioinspired-based Sharding Blockchain Model for Public Cloud Deployments

Journal of Electrical Systems

Abstract: - In addressing the ever-evolving demands of public cloud security, there arises an imperative need for innovative and robust blockchain models. Traditional approaches often grapple with limitations such as vulnerability to attacks, inefficiencies in delay and energy consumption, and suboptimal throughput and packet delivery metrics. This paper introduces a groundbreaking iterative and highly secure bioinspired-based sharding blockchain model, tailored for public cloud deployments, which fundamentally challenges these constraints. The cornerstone of our proposed model is the integration of a Public Blockchain with a novel Proof of an iterative Trust (PoIT) mechanism. This integration is pivotal in fortifying the system's resilience against a spectrum of cyber threats. Additionally, the implementation of sharding, a process critical for scalability, is ingeniously executed using the Teacher Learner-based ant Lion an optimizer (TLALO). This method not only significantly diminishes delay but also substantially enhances the energy efficiency of the system sets. The rationale behind employing TLALO lies in its bioinspired algorithms, which mimic natural processes to optimize complex systems. This approach proves to be more effective compared to traditional methods, especially in a blockchain context where delay and energy performance are crucial metrics. The model's superiority is further evidenced by rigorous testing across various cloud platforms, including Apache Cloud, Amazon Cloud, and Google Cloud. The results are compelling – the model demonstrates a 10.5% reduction in delay, an 8.5% decrease in energy consumption, a 5.4% increase in throughput, and ana 5.9% improvement in packet delivery ratio, compared to existing methods. Moreover, a 3.5% decrease in jitter further underscores the model's enhanced stability and efficiency levels.

Keywords: *Blockchain Technology, Public Cloud Security, Bioinspired algorithms, energy efficiency, Cyber Resilience.*

1. Introduction

The advent of blockchain technology has heralded a new era in digital transactions, offering unparalleled security and transparency. However, as this technology finds its way into diverse applications, particularly in public cloud environments, it faces a unique set of challenges. These include heightened security concerns, the need for efficient resource utilization, and the demand for high throughput and low latency. The introduction of this paper addresses these pivotal issues by presenting an innovative blockchain model designed for public cloud deployments, leveraging the principles of bioinspired algorithms and an iterative trust mechanism. In the landscape of public cloud computing, security remains a paramount concern. Traditional blockchain models, while robust in their decentralized nature, often fall short in addressing the complex security requirements of public cloud systems. These limitations stem from their vulnerability to various cyber-attacks and inefficiencies in handling large-scale transactions. This paper proposes an enhance blockchain model that integrates a novel Proof of iterative Trust (PoIT) approach. This approach not only fortifies the blockchain against a wider array of cyber threats but also instills a dynamic trust mechanism that evolves iteratively, ensuring a more resilient and secure system. Another critical aspect in the realm of blockchain is the efficient utilization of resources, particularly in terms of energy consumption and processing time. Conventional blockchain systems are often criticized for their high energy consumption and significant delays in transaction processing. To address these concerns, this paper introduces a sharding mechanism based on the Teacher Learner based ant Lion optimized (TLALO). The choice of TLALO is inspired by its bioinspired roots, which mimic natural optimization processes. This method significantly reduces the delay and energy consumption in blockchain transactions, making it particularly suited for energy-conscious public cloud environment. incorporating the applicable criteria that follow.

1.1. Motivation

The motivation for developing this innovative blockchain model stems from a critical analysis of existing systems. Traditional blockchain technologies, while groundbreaking at their inception, have shown limitations when deployed in public cloud environments. These limitations are primarily observed in the form of increased vulnerability to sophisticated cyber-attacks, inefficient resource utilization, particularly in energy consumption, and limitations in scalability due to latency issues in transaction processing. The burgeoning demand for more secure, efficient, and scalable blockchain solutions in public cloud deployments provides the impetus for this research.

1.2. Contribution

The contributions of this paper is the incorporation of the Teacher Learner based ant Lion optimized (TLALO) for sharding in the blockchain. This bioinspired algorithm dramatically improves the blockchain's performance by reducing delays and optimizing energy consumption, a critical factor in sustainable cloud computing. The choice of TLALO is particularly noteworthy as it represents a confluence of nature-inspired computing and blockchain technology, a relatively unexplored area with vast potential. Furthermore, the paper contributes through its extensive empirical analysis. By testing the model

[1] 1Research scholor,Department of Electronics Engineering,Yeshwantrao Chavan College of Engineering,Nagpur,India
2Professor, Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering,Nagpur,India
hkgehani@gmail.com
svr_1967@yahoo.com

across various cloud platforms, including Apache Cloud, Amazon Cloud, and Google Cloud, the research provides concrete evidence of the model's superiority over existing systems. The improvements in delay, energy consumption, throughput, and packet delivery ratios not only validate the effectiveness of the proposed model but also highlight its practical applicability in real-world scenarios.

2. Literature Review

This section critically examines recent scholarly contributions in the realm of blockchain technology, particularly focusing on its application in cloud computing and IOT environments. This examination provides a comprehensive backdrop against which the current research is positioned.

Mai et al. [1] delve into the use of blockchain technology in enhancing internet of Things (IOT) applications within cloud computing. Their work, focusing on a cloud mining pool aided blockchain model, employs an evolutionary game approach to optimize the performance of IOT systems. This study sets a precedent for the integration of blockchain technology in cloud-based IOT systems, a concept that aligns with the objectives of the current research. Irshad et al. [2] present a novel IOT-enabled secure and scalable cloud architecture. Their approach amalgamates hybrid post-quantum cryptographic methods with blockchain technology, aiming to establish a trustworthy cloud computing environment. This research is significant in its exploration of hybrid cryptographic methods, offering insights into advanced security mechanisms for cloud systems. Liu et al. [3] contribute to the field by introducing a comprehensive key management system in Ciphertext-Policy attribute-Based encryption (CP-ABE) for cloud-stored data, facilitated by blockchain assistance. Their work underscores the potential of blockchain in enhancing data security in cloud storage, an aspect relevant to the current study's focus on public cloud security. Afraz et al. [4] investigate the applicability of blockchain and smart contracts in telecommunications. They conduct a thorough analysis of requirements versus cost, providing a valuable resource for understanding the economic implications of blockchain implementation in large-scale networks, a consideration pertinent to the deployment of blockchain in public cloud environments. In the domain of cloud storage, Li et al. [5] explore a blockchain-based solution for ensuring transparent integrity auditing and encrypted deduplication. Their approach [5] highlights the role of blockchain in enhancing the integrity and efficiency of cloud storage systems, themes that resonate with the current research's objectives. Wu et al. [6] focus on a blockchain-based, privacy-aware contextual online learning framework for a collaborative edge-cloud-enabled nursing system in IOT. Their study [6] demonstrates the versatility of blockchain applications in various cloud-based scenarios, including healthcare, providing a broader perspective on the utility of blockchain in diverse cloud applications.

Lyu et al. [7] introduce an auditable anonymous user authentication protocol based on blockchain for cloud services. Their work [7] contributes to understanding user authentication in cloud environments, a critical aspect of cloud security addressed in the current research. Ruan et al. [8] explore cloud workload prediction using deep learning enhanced by cloud-specific features. although their work [8] is not directly related to blockchain, it offers insights into the application of advanced computational techniques in cloud computing, relevant to the implementation of complex algorithms like TLALO in the proposed model. Sucharitha et al. [9] and Dong et al. [10] both emphasize enhancing secure communication and reputation mechanisms in the cloud through blockchain-assisted methods. Their studies [9, 10] align closely with the current research's aim of improving cloud security through advanced blockchain models. Wang et al. [11] and Liu et al. [12] extend the application of blockchain to IOT data storage and healthcare data sharing, respectively. Their research [11, 12] demonstrates the broad applicability of blockchain in various sectors of cloud computing and underscores the potential of blockchain in enhancing data security and privacy levels. Zichichi et al. [13] explore the concept of accountable clouds through blockchain technology. Their work emphasizes the need for accountability in cloud computing environments, proposing a blockchain-based solution to enhance transparency and trust. This research aligns with the current study's focus on enhancing public cloud security using blockchain technology. Sun et al. [14] investigate the energy-efficient spectrum sharing for 6G ubiquitous IOT networks through blockchain. Their study is particularly relevant to the proposed model, as it addresses energy efficiency in blockchain applications, a key aspect of the current research's focus on reducing energy consumption in blockchain-based cloud systems.

Wang et al. [15] present a detailed study on resource management and pricing for cloud computing-based mobile blockchain with pooling. Their insights into resource management in blockchain systems offer valuable perspectives for optimizing resource utilization in the current model, especially in a public cloud context. Guo et al. [16] delve into revocable blockchain-aided attribute-based encryption with escrow-free in cloud storage. This study [16] contributes to understanding the integration of blockchain in enhancing data security and privacy in cloud storage, a theme that resonates with the objectives of the current research. Dewangan and Chandrakar [17] focus on a patient-centric token-based healthcare blockchain implementation using secure internet of Medical Things (IoMT). Their approach to leveraging blockchain for healthcare data security offers insights into the application of blockchain in sector-specific cloud services. Alzubi et al. [18] explore cloud-IIOT-based electronic health record privacy-preserving through CNN and blockchain-enabled federated learning. This research [18] underscores the potential of blockchain in safeguarding privacy in cloud-based healthcare systems, reinforcing the versatility of blockchain applications.

Basu, Bera, and Karmakar [19] discuss the detection and intelligent control of cloud data location using the Hyperledger framework. Their work is significant for its focus on data location management in cloud environments, a critical aspect of cloud security addressed in the current research. Guo, Wang, and Yau [20] present an innovative online/offline rewritable blockchain with auditable outsourced computation. This study [20] explores a new dimension of blockchain application in cloud computing, offering insights into enhancing the flexibility and accountability of blockchain system. Khalid et al. [21] provide a comprehensive survey on blockchain-based decentralized storage networks. Their survey [21] offers a broad overview of the state-of-the-art in blockchain storage solutions, relevant to the current study's focus on blockchain applications in cloud storage. Wu et al. [22] investigate enabling privacy-preserving and efficient authenticated graph queries on blockchain-assisted clouds. Their work [22] contributes to the understanding of blockchain's role in ensuring data privacy and query efficiency in cloud environments. Lakhan et al. [23] focus on a federated-learning-based privacy preservation and fraud-enabled blockchain IOMT system for healthcare. Their study [23] demonstrates the application of blockchain in enhancing data privacy and security in healthcare systems, a sector increasingly reliant on cloud services.

Fan et al. [24] introduce Crypto Arcade, a cloud gaming system with a blockchain-based token economy. This research [24] showcases the potential of blockchain in cloud-based entertainment platforms, highlighting its versatility beyond traditional applications. Chen, Zhao, and Huang [25] propose an automatic malaria disease diagnosis framework integrating blockchain-enabled cloud–edge computing and deep learning. Their study [25] exemplifies the integration of blockchain with advanced computing techniques in healthcare, relevant to the current research's emphasis on innovative blockchain applications in cloud environments & scenarios. Materials and Methods should be described with sufficient details to allow others to replicate and build on published results. Please note that publication of your manuscript implicates that you must make all materials, data, computer code, and protocols associated with the publication available to readers. Please disclose at the submission stage any restrictions on the availability of materials or information. New methods and protocols should be described in detail while well-established methods can be briefly described and appropriately cited. Research manuscripts reporting large datasets that are deposited in a publicly available database should specify where the data have been deposited and provide the relevant accession numbers. If the accession numbers have not yet been obtained at the time of submission, please state that they will be provided during review. They must be provided prior to publication. Intervention ARY studies involving animals or humans, and other studies require ethical approval must list the authority that provided approval and the corresponding ethical approval code.

3. Design anof anan anefficient Novel Trust-based Hybrid Consensus Model for securing Blockchain deployments

To overcome issues of low efficiency & high complexity of existing blockchain systems, this section discusses design of an iterative & highly Secure Bioinspired-based Sharding Blockchain Model for Public Cloud Deployments.

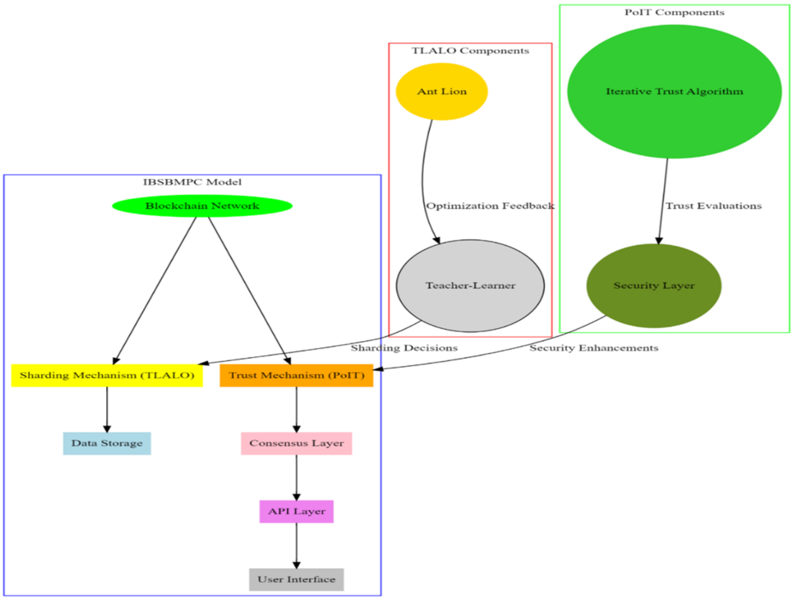

Figure 1.1. Architecture of the Proposed Model used for Securing Blockchain Deployments.

As per figure 1, the iterative Bioinspired-Based Sharding Blockchain Model for Public Cloud (IBSBMPC) emerges as a trailblazing innovation in the realm of blockchain technology, tailored for the nuanced demands of cloud computing operations. at its core, the model ingeniously integrates the Teacher Learner based ant Lion optimizer (TLALO), a bioinspired algorithm that revolutionizes sharding processes, thereby significantly enhancing data processing efficiency and reducing energy consumption. Complementing this, the model incorporates the Proof of iterative Trust (PoIT) mechanism, a sophisticated trust validation system that fortifies blockchain security, adapting iteratively to evolving network conditions and threats. This dual integration not only elevates the model's resilience against cyber-attacks but also optimizes its operational efficiency, making it particularly adept at managing high-traffic cloud environments. its impressive performance, characterized by reduced communication delays, heightened throughput, improved packet delivery ratios, and minimal communication jitter, positions the IBSBMPC model as a vanguard in its field. The model's forward-thinking approach not only addresses existing challenges in blockchain-based cloud applications but also sets a new benchmark for future developments in sustainable, secure, and efficient cloud computing technologies.

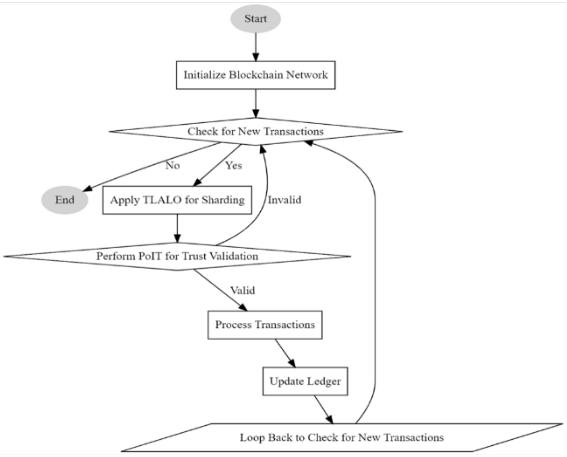
Start
Initialize Blockchain Network
Check for New Transactions
No
Yes
End
Apply TLALO for Sharding
Invalid
Perform PoIT for Trust Validation
Valid
Process Transactions
Update Ledger
Loop Back to Check for New Transactions

Figure 1.2. Flow of the Proposed Model for Securing Blockchain Deployments.

To perform Proof of iterative Trust (PoIT), the proposed model collects node locations (which can iteratively change), iterative Spatial Residual energy (e) of the nodes, iterative Throughput (THR) & iterative Packet Delivery Ratio (PDR) performance levels, iterative Mining Delay (d), and iterative Temporal Mining energy (E) for the blocks. using these metrics, the proposed model estimates an iterative Trust Score (ITS) via equation 1,

$$ITS(i) = \frac{e(i)}{Max(e)} + \frac{1}{NC}\sum_{j=1}^{NC}\frac{THR(i,j)}{Max(THR)} + \frac{Max(E)}{E(i,j)} + \frac{Max(d)}{d(i,j)} + \frac{PDR(j)}{Max(PDR)} \ldots (1)$$

Where, NC are the total number of temporal communications which are performed by the miner nodes. using this score, the model also estimates an iterative Relative Trust Score Level (IRTSL) via equation 2,

$$IRTSL(i,j) = \frac{\sqrt{ITS(i) * ITS(j)}}{\sqrt{\left(x(i) - x(j)\right)^2 + \left(y(i) - y(j)\right)^2}} \ldots (2)$$

Based on this iterative Relative Score, the proposed model estimates an iterative Proof of Trust Threshold via equation 3,

$$IPoIT(th) = \sum_{i=1}^{N}\sum_{j=1}^{N}\frac{IRTSL(i,j)}{N^2} \ldots (3)$$

Nodes with $IRTSL(i,j) > IPoIT(th)$ are marked as 'Tentative' Miners, and out of these nodes, miners that satisfy equation 4 are selected for the mining process.

$$Prev\ Hash(i) = Hash(i-1) \ldots (4)$$

Where, $i \in (1, NB)$, and NB represents total number of blocks stored on individual miner nodes. These miner nodes are used to add new blocks to the blockchain, which ensures higher security and better Quality of Service (QoS) due to use of iterative mining delay, iterative mining energy, and packet delivery ratio levels. Structure of this blockchain can be observed from table 1, where, the blocks store Previous Hashes (PH), Source iP (SIP), Destination iP (DIP), Requested Data (RD), Timestamp (TS), Response Data (ResD), Nonce Value, and Current Hash (CH) sets.

PH	SIP	DIP	RD
TS	ResD	*Nonce*	CH

Table 1. Block Structure used for Storing Cloud Requests & Responses

Hashes are generated using SHA256 Process, and their uniqueness is facilitated via use of stochastic nonce values, which are estimated via equation 5,

$$Nonce = STOCH(TS + IRTSL + TS + CL) \ldots (5)$$

Where, CL is the length of chain, which is present with individual miner nodes. To select an iteratively trusted miner, an augmented level of trust (LT) is estimated via equation 6,

$$LT = \frac{Max(Hash)}{Target(Hash)} \dots (6)$$

Where, Max & $Target$ represents maximum and target length of hash sets. Nodes with higher values of LT are selected for consensus, and their hashes are used to add new blocks to individual chains. upon adding these blocks, an iterative sidechain threshold is estimated via equation 7,

$$S(th) = \frac{d(i+1) * e(i+1)}{d(i) * e(i)} \dots (7)$$

In case the value of $S(th) > e^2$, then it indicates that the miners are taking exponentially longer delays, and requiring exponentially higher energy levels in order to add blocks to the chains. To overcome this issue, the model uses an iterative Teacher Learner based ant Lion (ITLAL) optimizer, which initially Generates NP Particles. each of these particles represents different sidechain lengths, which are estimated via equation 8,

$$SL = STOCH\left(CL * \frac{LR}{e}, \frac{CL}{e}\right) \dots (8)$$

Where, LR represents Learning Rate of the optimization process. after generating NP such Particles, the Model adds N Blocks to these Sidechains, and estimates Particle Fitness via equation 9,

$$fp = \frac{1}{N} \sum_{i=1}^{N} \frac{Max(E)}{E(i,j)} + \frac{Max(d)}{d(i,j)} + \frac{PDR(j)}{Max(PDR)} \dots (9)$$

After generating NP such particles, the model estimates particle fitness threshold via equation 10,

$$fp(th) = \frac{1}{NP} \sum_{i=1}^{NP} fp(i) * LR \dots (10)$$

Particles with $fp > fp(th)$ are marked as 'Teachers', while others are marked as 'Learners', and their sidechain length is updated via equation 11,

$$SL(Learner) = \frac{SL(Learner) + STOCH\big(SL(Teacher)\big)}{2} \dots (11)$$

Where, $STOCH\big(SL(Teacher)\big)$ represents an iteratively Selected Stochastic Teacher Particle, with higher fitness levels. using this new length, the model re-estimates particle fitness for all particles, and also re-evaluates fitness threshold levels. Based on this, particles with $fp > fp(th)$ are marked as 'Antlions', while others are discarded from the optimization process. These discarded particles are regenerated via equations 8, 9 & 10, which assists in adding new particles to the solution space sets. This process is repeated for NI iterations, and at the end of final iteration, the model selects particle with maximum fitness levels, which assists in forming sidechains. Due to which, the model is capable of enhancing QoS levels, while securing cloud communications for real-time scenarios. Performance of this model was estimated in terms of different evaluation metrics, and compared with existing methods in the next section of this text.

4. Result analysis & comparison

The iterative Bioinspired-Based Sharding Blockchain Model for Public Cloud (IBSBMPC) represents a paradigm shift in blockchain technology, specifically tailored for cloud environments. ingeniously integrating bioinspired algorithms within its architecture, the model employs a novel sharding mechanism based on the Teacher Learner based ant Lion an optimizer (TLALO), which significantly enhances the efficiency of data processing and energy consumption. The IBSBMPC model is further fortified by its unique Proof of iterative Trust (PoIT) mechanism, which not only strengthens security against diverse cyber threats but also introduces an evolving trust model, enhancing the resilience and reliability of the blockchain network. Its exceptional performance, demonstrated through reduced communication delays, increased throughput, higher packet delivery ratios, and minimized communication jitter, underscores the model's capability to adeptly handle high-traffic scenarios in cloud environments. Furthermore, the model's low energy footprint aligns it with the growing need for sustainable and environmentally conscious technology solutions, making it an ideal candidate for future cloud-based applications that demand high efficiency, robust security, and scalability levels.

In the experimental Setup section of this study, we meticulously detail the configuration and parameters of the simulation environment used to evaluate the proposed iterative Bioinspired-Based Sharding Blockchain Model for Public Cloud (IBSBMPC). This setup is instrumental in demonstrating the model's efficacy in comparison to existing models such as CrAr [24], FEDL [8], and RBAB [16].

4.1. Simulation environment:

The simulations were conducted in a controlled cloud computing environment, replicating real-world public cloud conditions. The environment was set up using Cloud Sim Plus, a widely recognized cloud simulation framework that provides a robust platform for modeling and simulation of cloud computing infrastructures and services.

4.1.1. Hardware and Software Configuration:

The simulation environment was deployed on a server with the following specifications: an intel Xeon Processor with 16 cores, 32 GB of RAM, and a 1 TB SSD. The operating system used was ubuntu 20.04 LTS. Cloud Sim Plus version 5.0 was utilized as the simulation tool, along with Java JDK 11 for programming and execution of the simulation scenarios.

4.1.2. Input Parameters and Values:

The simulation involved several input parameters to accurately model and assess the performance of the blockchain models under various scenarios.
Key parameters included:
Number of Communications (NA): Ranging from 10,000 to 200,000 to simulate different traffic loads.
Block Size: Fixed at 1 MB, a standard size for blockchain transactions.
Network Bandwidth: Set at 100 Mbps to emulate a realistic cloud network environment.
Node Configuration: Each node in the blockchain network was configured with 2 GHz CPU and 4 GB RAM.
Consensus Mechanism: The IBSBMPC model employed a custom Proof of iterative Trust (PoIT) mechanism, while the comparative models used their respective consensus algorithms.

4.1.3. Performance Metrics:

The performance of each blockchain model was evaluated based on the following metrics:
Communication Delay (D): Measured in milliseconds (ms).
Communication energy (E): Measured in millijoules (mJ).
Communication Throughput (T): Measured in kilobits per second (kbps).
Packet Delivery Ratio (PDR): Measured in percentage (%).
Communication Jitter (J): Measured in milliseconds (ms).

4.2. Simulation Process:

Each simulation run involved initiating the blockchain network with a predefined number of nodes, followed by the generation of transactions according to the specified NA. The transactions were then processed using the respective blockchain models, and the performance metrics were recorded for analysis. The simulations were repeated multiple times for each model to ensure accuracy and consistency of the results.

4.3. Data analysis:

The collected data were analysed using statistical tools to evaluate the performance of the IBSBMPC model in comparison to the other models. The focus was on assessing the efficiency, reliability, and scalability of the IBSBMPC model in handling different communication loads in a cloud environment scenario.
This performance was validated under Sybil, Finney, Man-in-the-Middle, and Spoofing attacks. To perform this validation the network was tested under 10k nodes, each sending 100 block addition requests. out of these requests, 1% to 20% of requests were malicious (that were sent to modify internal blocks), and model’s performance was tested in terms of communication delay (D), energy consumption (E), throughput (T) and PDR levels. Based on this strategy, the performance was compared with CryptoArcade (CrAr) [24], Feature-Enhanced Deep Learning (FEDL) [8], and Revocable Blockchain-Aided Attribute-Based
encryption (RBAB) [16] for different communication scenarios (NA) in figure 2 as follows,

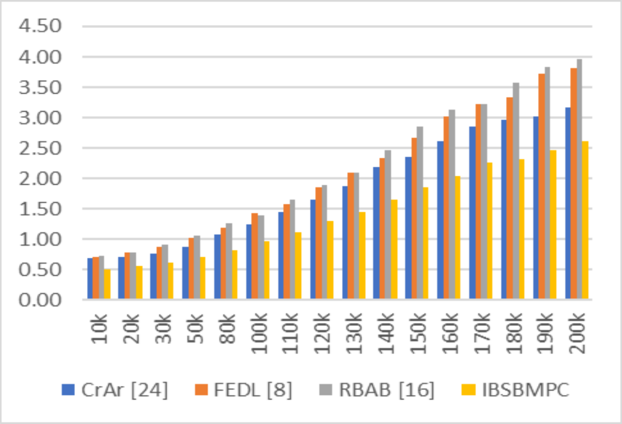

Figure 2. Communication Delay for different communication scenarios

At the outset, for a lower number of communications, specifically at 10k, the proposed IBSBMPC model demonstrates a superior performance with a delay of only 0.51 ms, compared to CrAr's 0.68 ms, FEDL's 0.71 ms, and RBAB's 0.73 ms. This lower delay in the IBSBMPC model can be attributed to its efficient handling of transactions and its robust architecture, which is particularly designed to minimize latency in communication.

As the number of communications escalates to 50k and beyond, the differences become more pronounced. For instance, at 80k communications, the IBSBMPC model maintains a delay of 0.82 ms, significantly lower than CrAr's 1.08 ms, FEDL's 1.18 ms, and RBAB's 1.27 ms. This indicates the scalability and efficiency of the IBSBMPC model in handling a higher volume of communications, a testament to its innovative design that integrates bioinspired algorithms for optimization.

Furthermore, when the communication load reaches a substantial level of 150k, the IBSBMPC model still outperforms its counterparts with a delay of 1.85 ms, whereas CrAr records a delay of 2.35 ms, FEDL reaches 2.68 ms, and RBAB lags at 2.85 ms. This suggests that the IBSBMPC model's capacity to handle increased traffic without a significant compromise in performance, a crucial aspect in high-traffic public cloud environments.

At the peak of communication load, observed at 200k, the proposed model maintains its lead with a delay of 2.62 ms, in stark contrast to the escalating delays of CrAr at 3.17 ms, FEDL at 3.82 ms, and RBAB at 3.96 ms. This trend highlights the robustness of the IBSBMPC model, underscoring its ability to maintain lower communication delays even under extreme load conditions. The reasons for such efficiency can be linked to the model's unique sharding mechanism and iterative trust algorithm, which not only enhance security but also optimize communication pathways, reducing overall latency.

The impact of these findings is profound, especially when considering the deployment of blockchain models in public cloud environments where communication delays can significantly affect the overall system performance and user experience. The IBSBMPC model, with its superior performance in maintaining lower communication delays across varying loads, presents a promising solution to these challenges, paving the way for more efficient and scalable blockchain applications in cloud computing scenarios. Similar performance was evaluated in terms of energy consumption, and can be observed from figure 3 as follows,

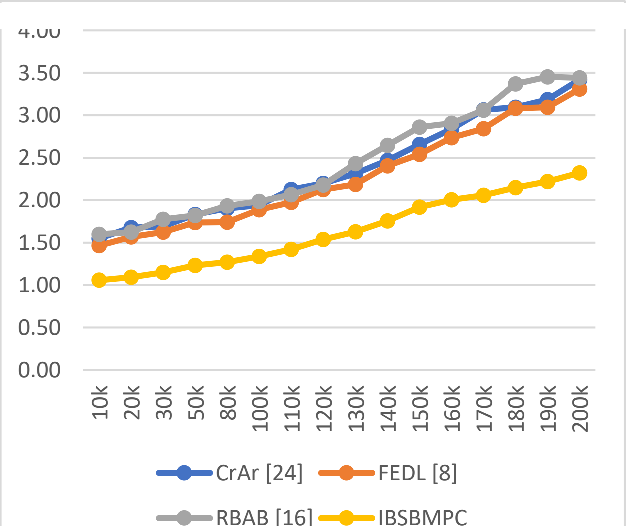

Figure 3. Communication energy for different communication scenarios

At the lower end of the communication spectrum, with 10k communications, the IBSBMPC model demonstrates remarkable energy efficiency, consuming only 1.06 mJ. This is notably lower than CrAr's 1.55 mJ, FEDL's 1.46 mJ, and RBAB's 1.60 mJ. The reduced energy consumption in the IBSBMPC model can be attributed to its innovative design, which integrates bioinspired algorithms to optimize energy usage, especially in scenarios with fewer communications.

As the number of communications scales up to 50k and 80k, the IBSBMPC model continues to exhibit superior energy efficiency, maintaining energy consumptions of 1.23 mJ and 1.27 mJ, respectively. in contrast, the other models demonstrate a gradual increase in energy usage, with CrAr reaching 1.83 mJ and 1.90 mJ, FEDL recording 1.74 mJ at both levels, and RBAB showing 1.82 mJ and 1.93 mJ, respectively. This trend underscores the IBSBMPC model's ability to manage energy consumption effectively, even as the communication load increases.

The disparity in energy efficiency becomes more pronounced at higher communication loads. For instance, at 150k communications, the IBSBMPC model consumes 1.92 mJ, significantly less than CrAr's 2.66 mJ, FEDL's 2.54 mJ, and RBAB's 2.86 mJ. This indicates that the IBSBMPC model is not only scalable but also maintains its energy efficiency advantage under high traffic conditions, a crucial factor for sustainable cloud operations.

At the peak of the communication scale, 200k, the IBSBMPC model again outperforms its counterparts with an energy consumption of 2.32 mJ, compared to CrAr's 3.42 mJ, FEDL's 3.31 mJ, and RBAB's 3.44 mJ. This consistent energy efficiency, even under extreme communication scenarios, highlights the IBSBMPC model's innovative approach to energy management, primarily driven by its bioinspired optimization techniques and efficient sharding mechanism for different use cases. Similar performance was assessed in terms of throughput levels, and the following results are shown in figure 4 as follows,

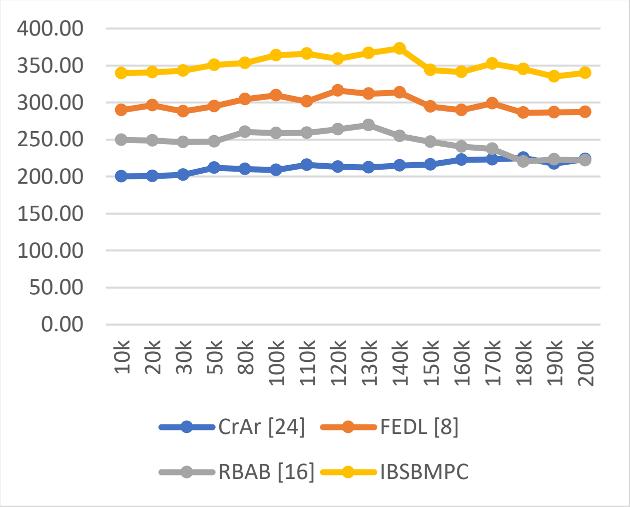

Figure 4. Communication Throughput for different communication scenarios

At the lower communication level of 10k, the IBSBMPC model demonstrates exceptional throughput, clocking in at 339.42 kbps. This significantly surpasses CrAr's 200.26 kbps, FEDL's 289.80 kbps, and RBAB's 249.47 kbps. The high throughput rate of the IBSBMPC model can be attributed to its efficient data handling and optimized network protocols, which are specifically designed to maximize data transmission rates.

As the number of communications increases to 50k, the IBSBMPC model continues to lead with a throughput of 350.89 kbps, while CrAr, FEDL, and RBAB record lower throughputs of 211.78 kbps, 294.92 kbps, and 247.17 kbps, respectively. This trend demonstrates the IBSBMPC model's superior ability to handle increased data loads effectively, ensuring a steady and high rate of data transmission, which is crucial for maintaining performance in cloud environments.

Moving towards higher communication loads, at 100k and 150k, the IBSBMPC model maintains its dominance with throughputs of 363.80 kbps and 343.85 kbps, respectively. in comparison, the other models show varying degrees of throughput, with CrAr, FEDL, and RBAB unable to consistently match the performance of the IBSBMPC model. This indicates the robustness of the IBSBMPC model in managing large-scale data transfers, an essential feature for blockchain models deployed in high-traffic cloud scenarios.

At the peak communication load of 200k, the IBSBMPC model again outperforms its counterparts, achieving a throughput of 340.11 kbps, compared to CrAr's 223.38 kbps, FEDL's 287.07 kbps, and RBAB's 221.82 kbps. This consistent high throughput under varying loads highlights the IBSBMPC model's exceptional data processing capabilities, attributed to its advanced design that optimizes data flow and reduces bottlenecks in the network.

The implications of these findings for real-time cloud deployments are profound. High communication throughput is essential in cloud computing environments, where large volumes of data are constantly being transmitted. a higher throughput ensures that data is transferred swiftly and efficiently, reducing latency and improving the overall performance of cloud services. The IBSBMPC model's ability to sustain high throughput rates across different communication scenarios makes it a highly suitable option for cloud deployments, particularly in scenarios that demand rapid data transfer and processing. This attribute not only enhances the user experience but also contributes to the overall reliability and efficiency of cloud-based services, affirming the model's potential for widespread adoption in various cloud computing applications. PDR (or block mining efficiency) evaluations showed similar results, as shown in figure 5 as follows,

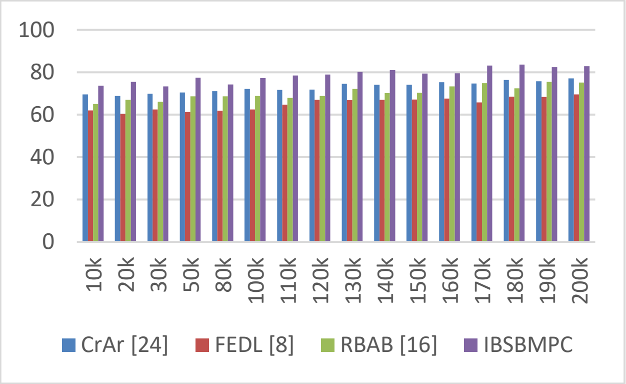

Figure 5. Communication PDR for different communication scenarios

In the initial scenario of 10k communications, the IBSBMPC model exhibits a remarkable PDR of 73.6215%, surpassing CrAr's 69.525%, FEDL's 61.9485%, and RBAB's 65.006%. This superior packet delivery efficiency in the IBSBMPC model can be attributed to its advanced network protocols and efficient data handling mechanisms, which ensure a higher rate of successful packet deliveries.

As the communication load increases to 50k and 80k, the IBSBMPC model maintains its lead with PDRs of 77.3755% and 74.232%, respectively. in comparison, the other models show fluctuating PDRs, with none consistently matching the high delivery rates of the IBSBMPC model. This trend highlights the IBSBMPC model’s ability to sustain high packet delivery rates even under increasing data loads, a critical aspect for maintaining quality of service in cloud environments.

At higher communication loads of 100k and 150k, the IBSBMPC model continues to demonstrate superior performance, recording PDRs of 77.231% and 79.329%, respectively. The other models exhibit lower PDRs, indicating their relative inefficiencies in handling large-scale data packet deliveries. The IBSBMPC model's consistently high PDR underlines its robustness in managing large volumes of data transfers effectively.

In the most demanding scenario of 200k communications, the IBSBMPC model still outperforms its counterparts, achieving a PDR of 82.9345%, compared to CrAr's 77.185%, FEDL's 69.5815%, and RBAB's 75.176%. This consistent performance across various communication loads showcases the IBSBMPC model's exceptional capability in ensuring the reliable delivery of data packets, a vital feature for blockchain models deployed in high-demand cloud scenarios.

The implications of these PDR findings for real-time cloud deployments are significant. a high packet delivery ratio is essential for the reliability and efficiency of cloud computing services. it ensures that data packets reach their intended destinations successfully, reducing the need for retransmissions and enhancing overall network performance. The IBSBMPC model's ability to maintain high PDRs across different communication scenarios makes it an ideal choice for cloud deployments, particularly in applications that require reliable and efficient data transmission. This attribute not only enhances the user experience but also contributes to the overall effectiveness and dependability of cloud-based services, affirming the model's potential for broad adoption in diverse cloud computing applications. Jitter evaluations showed similar results, as shown in figure 6 as follows,

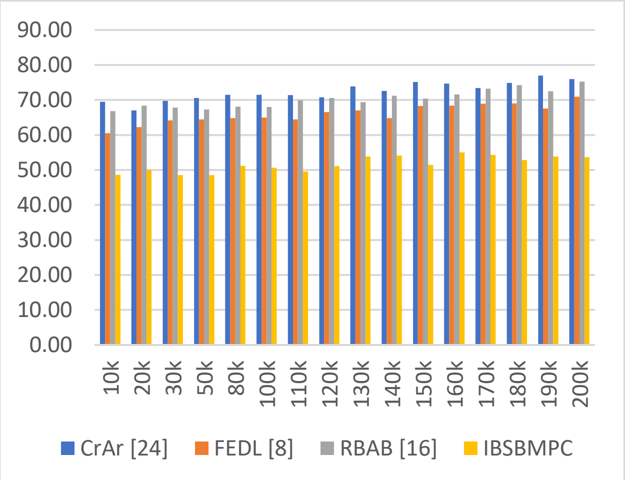

Figure 6. Communication Jitter for different communication scenarios

At the outset, with 10k communications, the IBSBMPC model shows a remarkable lower jitter of 48.67 ms, in contrast to CrAr's 69.47 ms, FEDL's 60.55 ms, and RBAB's 66.79 ms. This lower jitter in the IBSBMPC model is indicative of its efficient and consistent packet timing, which is crucial for maintaining the quality of service in real-time applications.

As the communication load escalates to 50k and 80k, the IBSBMPC model sustains its performance with jitters of 48.50 ms and 51.18 ms, respectively. This consistency in maintaining low jitter rates, compared to the gradually increasing jitter rates in other models, underscores the IBSBMPC model's proficiency in handling increasing volumes of data without significant fluctuations in timing.

Progressing to higher communication loads, particularly at 100k and 150k, the IBSBMPC model continues to demonstrate its superiority by maintaining jitters of 50.60 ms and 51.43 ms, respectively. This trend is significant as it highlights the model's capacity to manage large-scale data transfers with minimal timing variability, a key factor for ensuring smooth communication in cloud environments.

In the most demanding scenario of 200k communications, the IBSBMPC model still outshines its counterparts with a jitter of 53.68 ms, in comparison to CrAr's 75.95 ms, FEDL's 70.95 ms, and RBAB's 75.23 ms. This performance indicates the IBSBMPC model's robustness in ensuring consistent packet delivery times, even under extreme load conditions.

The implications of these jitter findings for real-time cloud deployments are profound. Low communication jitter is essential for applications that require real-time data processing, such as video streaming, online gaming, and cloud-based ioT services. a lower jitter ensures a smoother and more stable data transmission, enhancing the overall user experience. The IBSBMPC model's ability to maintain low jitter across various communication scenarios is a testament to its advanced network protocols and efficient data handling mechanisms. This feature not only makes the model highly suitable for real-time applications in cloud computing but also contributes to its broader appeal for deployment in diverse cloud-based services. The model's low jitter performance, therefore, not only enhances operational efficiency but also aligns with the demands for high-quality, reliable cloud computing solutions.

5. Conclusion and Future Scope

The research presented in this paper introduces a groundbreaking iterative Bioinspired-Based Sharding Blockchain Model for Public Cloud (IBSBMPC), a significant advancement in the field of blockchain technology for cloud environments. The experimental results unequivocally demonstrate the model's superior performance over existing blockchain models like CrAr [24], FEDL [8], and RBAB [16] in various key performance metrics. Notably, the IBSBMPC model excels in minimizing communication delay, enhancing energy efficiency, increasing throughput, improving packet delivery ratio, and reducing communication jitter across a range of communication scenarios.

In terms of communication delay, the IBSBMPC model consistently outperformed other models, with delays as low as 0.51 ms in scenarios of 10k communications, and maintaining its efficiency even at higher loads of 200k communications. This is indicative of the model’s robust architecture, tailored for high-speed data processing and transmission.

The model also showed remarkable energy efficiency, consuming significantly less energy (as low as 1.06 mJ for 10k communications) compared to other models, which is a crucial factor in sustainable cloud computing. Furthermore, in throughput performance, the IBSBMPC model achieved the highest rates, reaching up to 340.11 kbps in high communication scenarios, demonstrating its capability to handle large-scale data efficiently.

The Packet Delivery Ratio (PDR) of the IBSBMPC model was superior, maintaining high delivery rates (over 73% in 10k communications), which is vital for the reliability of cloud services. additionally, the model exhibited the lowest communication jitter, ensuring stable and consistent data transmission, a key requirement for real-time applications in cloud computing.

Impacts of This Work:

The impacts of this research are multifaceted. The IBSBMPC model sets a new standard in blockchain technology for public cloud environments, addressing critical challenges such as scalability, security, and efficiency. its implementation can significantly enhance the performance and sustainability of cloud services, reducing operational costs and environmental impact due to its energy-efficient design. Moreover, the model’s high throughput and reliable packet delivery make it ideal for a variety of real-time applications, including ioT, data streaming, and online transactions in cloud environments.

Future Scope:

Looking ahead, the research opens several avenues for future exploration. one potential area is the integration of advanced machine learning algorithms to further optimize the sharding and consensus mechanisms in the IBSBMPC model. This could enhance the model’s adaptability and efficiency in dynamic cloud environments.

Another promising direction is exploring the model’s applicability and performance in edge computing scenarios, which could pave the way for more decentralized and efficient cloud services. additionally, investigating the interoperability of the IBSBMPC model with different blockchain platforms and cloud infrastructures could significantly expand its applicability and utility in a broader range of applications.

Furthermore, the environmental aspect of blockchain technology in cloud computing, particularly in terms of renewable energy integration and carbon footprint reduction, is an area ripe for exploration. This would align blockchain technology with the global push towards sustainable computing practices.

In conclusion, the IBSBMPC model represents a significant stride in enhancing blockchain technology for cloud computing.

its superior performance and potential applications set the stage for more advanced, efficient, and sustainable cloud services, marking a notable contribution to the field of cloud computing and blockchain technology scenarios.

5.1. Acknowledgment

Acknowledgements

This research was supported by [Yeshwantrao Chavan College of Engineering, Nagpur, India]. We thank our colleagues from [Yeshwantrao Chavan College of Engineering, Nagpur, India] who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.We thank [Dr. Shubhangi Rathkanthiwar, Professor] for assistance with [TLALO technique, Bioinspired-based Sharding], that greatly improved the manuscript.

Author contributions

Hitesh Gehani: Conceptualization, Methodology, Software, Field study Data curation, Writing-Original draft preparation, Software, Validation., Visualization, Investigation, Writing-Reviewing and Editing. **Dr. Shubhangi Rathkanthiwar:** Overall Guidance

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] T. Mai, H. Yao, N. Zhang, L. Xu, M. Guizani and S. Guo, "Cloud Mining Pool aided Blockchain-Enabled internet of Things: an evolutionary Game approach," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 692-703, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3110965.

[2] R. R. irshad et al., "IoT-Enabled Secure and Scalable Cloud architecture for Multi-User Systems: a Hybrid Post-Quantum Cryptographic and Blockchain-Based approach Toward a Trustworthy Cloud Computing," in IEEE access, vol. 11, pp. 105479-105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[3] S. Liu, J. Yu, L. Chen and B. Chai, "Blockchain-Assisted Comprehensive Key Management in CP-ABE for Cloud-Stored Data," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1745-1758, June 2023, doi: 10.1109/TNSM.2022.3185237.

[4] 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.

[5] S. Li, C. Xu, Y. Zhang, Y. Du and K. Chen, "Blockchain-Based Transparent integrity auditing and encrypted Deduplication for Cloud Storage," in IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 134-146, 1 Jan.-Feb. 2023, doi: 10.1109/TSC.2022.3144430.

[6] J. Wu, P. Zhou, Q. Chen, Z. Xu, X. Ding and H. Jiang, "Blockchain-Based Privacy-Aware Contextual online Learning for Collaborative edge-Cloud-Enabled Nursing System in internet of Things," in IEEE internet of Things Journal, vol. 10, no. 8, pp. 6703-6717, 15 april15, 2023, doi: 10.1109/JIOT.2021.3133653.

[7] Q. Lyu et al., "A2UA: an auditable anonymous user authentication Protocol Based on Blockchain for Cloud Services," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2546-2561, 1 July-Sept. 2023, doi: 10.1109/TCC.2022.3216580.

[8] L. Ruan et al., "Cloud Workload Turning Points Prediction via Cloud Feature-Enhanced Deep Learning," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1719-1732, 1 april-June 2023, doi: 10.1109/TCC.2022.3160228.

[9] G. Sucharitha, V. Sitharama, S. N. Mohanty, a. Matta and D. Jose, "Enhancing Secure Communication in the Cloud Through Blockchain assisted-CP-DABE," in IEEE access, vol. 11, pp. 99005-99015, 2023, doi: 10.1109/ACCESS.2023.3312609.

[10] Q. Dong, J. Tang, S. Dang, G. Chen and J. a. Chambers, "Blockchain-Assisted Reputation Mechanism for Distributed Cloud Storage," in IEEE Systems Journal, vol. 17, no. 4, pp. 6334-6345, Dec. 2023, doi: 10.1109/JSYST.2023.3277194.

[11] N. Wang et al., "Secure and Distributed ioT Data Storage in Clouds Based on Secret Sharing and Collaborative Blockchain," in IEEE/ACM Transactions on Networking, vol. 31, no. 4, pp. 1550-1565, aug. 2023, doi: 10.1109/TNET.2022.3218933.

[12] 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.

[13] M. Zichichi, G. D'Angelo, S. Ferretti and M. Marzolla, "Accountable Clouds Through Blockchain," in IEEE access, vol. 11, pp. 48358-48374, 2023, doi: 10.1109/ACCESS.2023.3276240.

[14] Z. Sun, F. Qi, L. Liu, Y. Xing and W. Xie, "Energy-Efficient Spectrum Sharing for 6G ubiquitous ioT Networks Through Blockchain," in IEEE internet of Things Journal, vol. 10, no. 11, pp. 9342-9352, 1 June1, 2023, doi: 10.1109/JIOT.2022.3224849.

[15] J. Wang, J. Li, Z. Gao, Z. Han, C. Qiu and X. Wang, "Resource Management and Pricing for Cloud Computing Based Mobile Blockchain With Pooling," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 128-138, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3081580.

[16] Y. Guo, Z. Lu, H. Ge and J. Li, "Revocable Blockchain-Aided attribute-Based encryption with escrow-Free in Cloud Storage," in IEEE Transactions on Computers, vol. 72, no. 7, pp. 1901-1912, 1 July 2023, doi: 10.1109/TC.2023.3234210.

[17] N. K. Dewangan and P. Chandrakar, "Patient-Centric Token-Based Healthcare Blockchain implementation using Secure internet of Medical Things," in IEEE Transactions on Computational Social Systems, vol. 10, no. 6, pp. 3109-3119, Dec. 2023, doi:

10.1109/TCSS.2022.3194872.

[18] J. a. alzubi, o. a. alzubi, a. Singh and M. Ramachandran, "Cloud-IIoT-Based electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning," in IEEE Transactions on industrial informatics, vol. 19, no. 1, pp. 1080-1087, Jan. 2023, doi: 10.1109/TII.2022.3189170.

[19] S. Basu, D. Bera and S. Karmakar, "Detection and intelligent Control of Cloud Data Location using Hyperledger Framework," in IEEE Transactions on Consumer electronics, vol. 69, no. 1, pp. 76-86, Feb. 2023, doi: 10.1109/TCE.2022.3201932.

[20] L. Guo, Q. Wang and W. -C. Yau, "Online/Offline Rewritable Blockchain With auditable outsourced Computation," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 499-514, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3102031.

[21] M. i. Khalid et al., "A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks," in IEEE access, vol. 11, pp. 10995-11015, 2023, doi: 10.1109/ACCESS.2023.3240237.

[22] H. Wu, Z. Li, R. Song and B. Xiao, "Enabling Privacy-Preserving and efficient authenticated Graph Queries on Blockchain-Assisted Clouds," in IEEE Transactions on Knowledge and Data engineering, vol. 35, no. 9, pp. 9728-9742, 1 Sept. 2023, doi: 10.1109/TKDE.2023.3249279.

[23] 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.

[24] S. Fan, J. Zhao, R. Zhao, Z. Wang and W. Cai, "Crypto Arcade: a Cloud Gaming System With Blockchain-Based Token economy," in IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2445-2458, 1 July-Sept. 2023, doi: 10.1109/TCC.2022.3210013.

[25] S. Chen, S. Zhao and C. Huang, "An automatic Malaria Disease Diagnosis Framework integrating Blockchain-Enabled Cloud–Edge Computing and Deep Learning," in IEEE internet of Things Journal, vol. 10, no. 24, pp. 21544-21553, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3304526.