Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING CLOUD SECURITY AND PERFORMANCE USING INTELLIGENT LOAD BALANCING WITH BLOCKCHAIN APPROACH

KRISHNA SOWJANYA K[1*], MOULEESWARAN S K[2]

[1*]Research Scholar, Dayananda Sagar University, Ramanagara, Bengaluru, 562112, India,

Email: ksowjanya798@gmail.com

[2]Professor, Dayananda Sagar University, Ramanagara, Bengaluru, 562112, India,

Email: mouleeswaran-cse@dsu.edu.in

ABSTRACT

Cloud computing has transformed how organizations store, process, and access data, but security and performance concerns remain. This research presents a novel approach that combines intelligent load balancing with blockchain technology to address these challenges. By integrating the Golden Eagle Optimizer (GEO) algorithm for load balancing, the system optimizes performance and resource allocation in cloud environments. Blockchain enhances security, transparency, and trust, addressing issues like security vulnerabilities and performance inconsistencies. The GEO algorithm achieves a success rate of 0.9493 and a security score of 0.9535, making it an effective optimization solution. Using Python Jupyter for optimization, the system ensures high availability and considers security factors when distributing workloads across servers. The combination of blockchain and GEO results in a secure, efficient, and resilient cloud system with improved Quality of Service (QoS). This approach has significant implications for the future development of secure cloud computing systems.

Keywords: *Golden Eagle Optimizer (GEO), Quality of Service (QoS), Blockchain, Cloud Security, Load Balancing.*

1. INTRODUCTION

The process of dividing up incoming network traffic equally among several servers or resources is known as load balancing [1-3]. Ensuring optimal resource utilization, minimizing overload, and maximizing performance. However, traditional load-balancing methods may not be sufficient to handle the complexities and security requirements of cloud environments [4-6]. Many machine learning-based methods have been proposed to solve the process of data aggregation and routing issues for IoT-based constraint networks and drastically reduce the disturbance of wireless channels [7-9]. Cloud infrastructure exchanges confidential data with clients to give them access to remote resources, like computing and storage functions within the Internet of Things [10-13]. Software-defined networking (SDN) has increased the need for security due to the participation of illegitimate packets resulting from poor processing times and inadequate resource utilization [14-17]. The huge amount of information comes from various sources, which causes higher latency for immediate responsive devices to provide solutions [18-20]. Communication among CHs and base stations is facilitated by a localized private blockchain structure, which also offers an authentication mechanism that improves security and reliability [21-23]. For extended network life, an efficient clustering technique based on the node level, distance from clusters, remaining energy, and fitness has been presented for sensing devices [24-27]. Several recent developments regarding the field of Blockchain-AI in a renewable environment have a significant influence on the assessment of technology [28-30]. The side-channel attacks could extract the private information of other users who share the computing resources through virtualization. Also, cloud customers face security risks within the framework of load balancing of Virtual Machines. Energy blockchain (EB) has also significantly impacted energy transaction security, energy structure modification and ecological environment protection [31-33]. When paired with the development of edge platforms and resource-constrained IoT objects, it offers a strong guarantee

for the correct operation of the development of parallel computing.

Cloud computing is essential for modern organizations, offering scalable data storage and processing solutions. However, concerns about security and performance persist [34-35]. Traditional load-balancing techniques often neglect security, making systems vulnerable to cyber threats. This study proposes an innovative approach that integrates intelligent load balancing with blockchain technology to address these challenges. By combining blockchain's decentralized security with the GEO, the system optimizes resource allocation while ensuring data integrity and security [36-37]. The research gap in current cloud computing solutions lies in the lack of integration between security and performance optimization, with many existing algorithms focusing solely on resource allocation without addressing security vulnerabilities. Traditional load balancing strategies fail to provide transparency and trust, leaving systems susceptible to cyber threats [38-39]. The novelty of the proposed method is the combination of intelligent load balancing with blockchain technology, which enhances both security and performance [40]. By integrating the GEO with blockchain, the solution offers a secure, decentralized system with improved resource allocation. This innovative approach bridges the gap between performance optimization and security in cloud environments. The objective is to create a cloud environment that is highly secure, efficient, fault-tolerant, scalable, and transparent by leveraging blockchain technology to enhance load-balancing algorithms and processes. The remaining sections are arranged as follows: The literature review was as stated in section 2, the proposed technique was described in section 3, the results were discussed in section 4, the paper's limitations were described in section 5, and the paper's conclusion was described in section 6.

- Combines blockchain's decentralized and secure nature with intelligent load balancing to enhance security, transparency, and trust in cloud systems.
- Implements the GEO for efficient workload distribution, optimizing cloud resource allocation while maintaining high performance.
- The proposed method optimizes both security and performance by considering the security aspects of each server in the cloud.
- Demonstrates the success rate of GEO at 0.9493 and a security score of 0.9535, positioning it as a high-performing load balancing solution.
- Utilizes Python Jupyter for optimization, ensuring high availability and efficient distribution of workloads across cloud servers.
- Enhances Quality of Service by integrating blockchain to ensure data integrity and transactional security in resource allocation.

Despite the broad research on load balancing and cloud security, existing methods mainly focus on performance optimization without effectively addressing security worries. Also, blockchain-based solutions highlight security but frequently neglect effective workload distribution. So, there exists a research gap in incorporating both performance optimization and security within a combined framework.

The novelty of this study lies in the incorporation of the GEO with blockchain technology for intelligent load balancing. Different conventional methods, the proposed method concurrently enhances QoS parameters while ensuring data integrity, transparency, and trust through a decentralized blockchain framework. This dual optimization of performance and security distinguishes the proposed approach from existing techniques.

2. LITERATURE SURVEY

Cloud computing has become an integral part of many organizations, enabling remote access to data and applications. Efficient load balancing is crucial in managing traffic between servers, optimizing performance and resource utilization. Several studies have explored various techniques and models to enhance load balancing and system performance in cloud and edge computing environments. Shi et al. [41] proposed a safe data placement model for edge-cloud computing that guarantees load balancing and user access delay. Their experimental results demonstrated the robustness of their proposed algorithm in balancing server loads while minimizing delays. Mishra et al. [42] introduced an integrated decision tree approach for anomaly detection that leverages blockchain principles and machine learning, focusing on communication networks that manage secure information and diverse traffic types.

This method improves the detection of anomalies by combining the security features of blockchain with the predictive capabilities of machine learning. Wen et al. [43] assessed the effectiveness of data privacy safeguards in widely used storage systems and compared them to newer privacy mechanisms. Their findings indicated that

the proposed mechanism offered superior performance in safeguarding user data compared to existing solutions. Moawad et al. [44] examined the integration of Blockchain and IPFS within an Edge-Fog-Cloud architecture for smart cities. The Cloud-Block, Fog-Block, and Edge-Block models demonstrated the advantages of this architecture, outperforming other cutting-edge systems in terms of scalability and efficiency. Lu et al. [45] demonstrated that as the number of tasks increases, their proposed mechanism performs faster and more effectively than others, showcasing improved success rates, reduced execution times, and minimized delays. Raj et al. [46] explored the role of blockchain in securing communications within Cyber-Physical Systems (CPS). They developed a distributed environment based on blockchain and Software-Defined Networking (SDN) for data forwarding, comparing it to the Blockchain Secure Device Authentication Solution-based IoT technology. Sharma et al. [47] proposed a blockchain-based secure application for healthcare certificate generation and management, with performance analyses indicating that the system met required security standards and operational benchmarks. Herdem et al. [48] also discussed the advantages and limitations of various methods, highlighting the increasing trend towards hybrid models that combine multiple technologies for enhanced security and efficiency. Karthik et al. [49] developed a novel hybrid Elman Neural-based Blowfish Blockchain model to secure IoT healthcare multimedia data. Their comparative analysis demonstrated that the model outperformed other solutions in terms of security and performance. Zainal et al. [50] proposed a load-balancing method to improve the scalability of the Northbound interface in Software-Defined Networking (SDN) systems. Through comprehensive testing using a simulated multi-controller SDN system, they observed significant improvements in CPU and memory usage, response times, and error rates, confirming the effectiveness of their load-balancing strategy in addressing scalability challenges. These studies collectively indicate a clear trend toward the use of hybrid models that integrate blockchain, machine learning, and edge-cloud computing to optimize system performance, security, and scalability. The synthesized results from these studies highlight the continuous evolution of intelligent algorithms, with a growing emphasis on combining traditional and emerging technologies to address the complex challenges of modern cloud and edge computing environments.

Although numerous studies have explored load balancing and security in cloud computing, several limitations remain. Most existing approaches focus primarily on performance optimization using traditional or hybrid algorithms, while security is either addressed separately or insufficiently integrated into the load-balancing process. Conversely, blockchain-based approaches emphasize data security and integrity but often lack efficient resource allocation and workload distribution mechanisms.

Furthermore, many existing solutions rely on partially centralized architectures, which may limit transparency and introduce potential single points of failure. This separation between security mechanisms and optimization techniques results in suboptimal resource utilization and reduced system efficiency in dynamic cloud environments.

Therefore, a research gap exists in the development of a unified framework that simultaneously addresses both secure data management and efficient load balancing in cloud systems. To address this limitation, this study proposes an integrated approach that combines the Golden Eagle Optimizer (GEO) with blockchain technology to enhance resource allocation, ensure data integrity, and improve system transparency.

This integrated perspective is essential for developing secure, efficient, and scalable cloud computing environments capable of handling dynamic workloads.

3. PROPOSED METHODOLOGY

This study adopts a simulation-based experimental design to evaluate the performance of the proposed GEO-blockchain framework. The system consists of multiple cloud nodes where workloads are dynamically allocated using the Golden Eagle Optimizer. Blockchain technology is integrated to record and validate load-balancing decisions in a decentralized and tamper-proof manner.

The experimental workflow includes:

- Initialization of cloud nodes and workload requests
- Application of the GEO algorithm for optimal task allocation
- Recording of allocation decisions using blockchain
- Evaluation based on QoS metrics such as latency, throughput, response time, security rate, and success rate.

The study will assess the effectiveness of this approach by evaluating security measures,

performance benchmarks, and the resilience of the system under various conditions, contributing to the advancement of secure and efficient cloud computing environments (Figure 1).

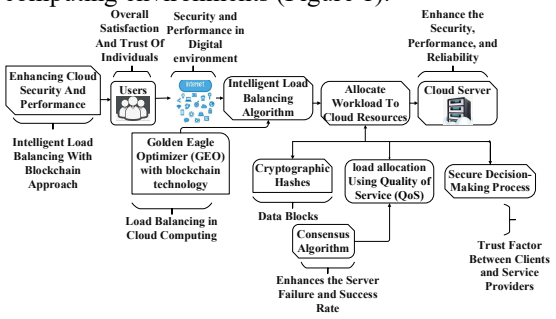

Figure 1: Block Diagram of Proposed Work

In cloud security and performance using intelligent load balancing with a blockchain approach, the term "USERS" likely refers to the end-users or clients interacting with the cloud-based services. This user-focused perspective aims to address not only the technical aspects of cloud infrastructure but also the overall satisfaction and trust of individuals or entities utilizing the cloud services. The proposed solution recognizes the critical role of the Internet in facilitating these connections and aims to optimize security and performance within this digital environment. Intelligent load balancing ensures efficient distribution of workloads over the Internet, contributing to enhanced responsiveness and reliability. Consequently, the research combining the GEO with blockchain technology for load balancing in cloud computing presents an innovative approach to enhancing performance and trust in cloud environments. The integration aims to address the optimization of QoS parameters while effectively managing changing workloads. The study implements the GEO algorithm as the load-balancing strategy. Database outsourcing, addressing the challenge of verifying the correctness of query results, is of paramount importance. This employs smart contracts to streamline load allocation by considering QoS metrics and historical insights. The integration of a blockchain approach adds a layer of security to the cloud server environment by employing a decentralized and tamper-resistant ledger for transaction records and data integrity. By focusing on the interplay between intelligent load balancing and blockchain technology, this approach aims to enhance the security, performance, and reliability of the cloud server infrastructure, ultimately benefiting the users and clients interacting with cloud services.'

3.1 Conceptual Model and Hypothesis

This study proposes a conceptual framework that integrates intelligent load balancing using the Golden Eagle Optimizer (GEO) with blockchain technology to enhance cloud security and performance. The GEO algorithm is responsible for efficient workload distribution based on QoS parameters, for example, latency, throughput, and resource utilization. Blockchain technology confirms secure, transparent, and tamper-proof recording of load-balancing decisions.

The conceptual relationship in the suggested system is definite as follows:

- GEO progresses resource allocation and system performance
- Blockchain improves security, transparency, and trust
- The incorporation of both expands overall QoS

Based on this framework, the following hypotheses are expressed:

H1: The recommended GEO-based intelligent load balancing significantly expands cloud performance related to traditional methods.

H2: The incorporation of blockchain improves the security and reliability of load-balancing operations.

H3: The united GEO-blockchain method increases overall QoS in cloud environments.

3.2 Users

The role of users in enhancing cloud security and performance using intelligent load balancing plays a vital part in understanding the importance of cloud security and the benefits of intelligent load balancing with a blockchain approach [31]. They need to be aware of the potential risks and challenges involved in managing and securing their data in the cloud. Users should actively implement security measures and best practices to enhance cloud security. This includes using strong authentication mechanisms, encryption techniques, and regularly updating software and applications. Users need to adhere to regulatory compliance requirements and industry standards to ensure security and privacy. Network administrators are responsible for managing and maintaining the network infrastructure. They configure load balancers with intelligent algorithms to distribute workloads efficiently across several servers. They also monitor network traffic, analyze performance metrics, and fine-tune load-balancing settings to optimize cloud security and performance. With a blockchain approach, they can verify the authenticity and integrity of network transactions, preventing

potential security threats. Users are often the first ones to come across security vulnerabilities or performance issues in the cloud. Users need to report any abnormalities or incidents to the cloud service provider or relevant authorities. They analyze network traffic patterns, identify vulnerabilities, and implement security measures to protect against cyber threats. With the help of intelligent load balancing and blockchain technology, they can ensure the privacy, reliability, and accessibility of cloud resources. End-users, including individuals and organizations, benefit from enhanced cloud security and performance through intelligent load balancing with a blockchain approach [32]. They experience improved system performance, reduced downtime, and increased data security. With blockchain technology, they can have greater confidence in the integrity and privacy of their data kept in the cloud. End-users should maintain best practices for cloud security, such as choosing strong passwords, regularly updating software, and practising safe browsing habits. Overall, users are crucial in ensuring the security and performance of cloud environments. Their active involvement in implementing security measures, adhering to compliance requirements, and sharing knowledge can greatly enhance cloud security and optimize performance using intelligent load balancing with a blockchain approach.

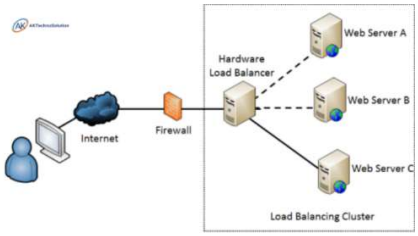

Figure 2: Utilization of Load Balancing Approach by User

Figure 2 illustrates the utilization of a load-balancing approach by users in a system. The graph or visual representation showcases how the load balancing mechanism is distributed among users, indicating the equilibrium achieved in resource allocation. This visualization can provide insights into the effectiveness of the load-balancing strategy, demonstrating whether it successfully distributes tasks or workloads evenly across users or nodes. Analyzing such a figure aids in assessing the performance and efficiency of the load-balancing approach in optimizing resource utilization and ensuring a well-balanced system operation.

3.3 Internet

The internet plays a vital part in enhancing cloud security and performance through intelligent load balancing with a blockchain approach. The internet provides a reliable and high-speed communication platform, enabling cloud services to interact efficiently with load balancers. This connectivity allows for real-time data exchange between the server and load-balancing algorithms, ensuring optimal performance and security. Cloud environments require the smooth and rapid transmission of data between different servers. The internet facilitates this process by offering high-bandwidth connectivity, enabling load-balancing algorithms to distribute workloads across multiple servers quickly and efficiently. Intelligent load-balancing algorithms utilize data from the cloud environment, such as server capacity, workload distribution, and user demand. These algorithms optimize the allocation of resources by analyzing real-time data from cloud servers and making informed decisions on workload distribution. The Internet plays a vibrant part in collecting and transmitting this data to load balancers, enabling them to make intelligent decisions. Blockchain technology can enhance cloud security and performance by providing an immutable, decentralized ledger for securely managing and verifying transactions within the cloud environment. The Internet provides the necessary infrastructure for blockchain networks, enabling secure communication between cloud servers and blockchain nodes [33]. This helps prevent data tampering and enhances the overall security of cloud operations. The internet enables real-time monitoring of cloud environments, allowing load balancers to continuously monitor the performance and security of cloud servers. This monitoring helps detect anomalies, such as sudden spikes in traffic or unauthorized access attempts, enabling load balancers to take immediate actions to mitigate potential risks or optimize performance. Overall, the internet enhances cloud security and performance using intelligent load balancing with a blockchain approach [34]. It provides the necessary infrastructure for seamless connectivity, rapid data transmission, intelligent workload distribution, and real-time monitoring, enabling efficient resource allocation and ensuring a high level of security within cloud environments. Combining intelligent load balancing with a blockchain approach can significantly enhance the security and performance of cloud computing.

3.4 Intelligent Load Balancing Algorithm

The research identifies and prioritizes the most pertinent metrics that are directly influenced by fluctuations in workload. These metrics may include response time, server utilization, throughput, latency, and more. Consequently, the research combining the GEO with blockchain technology for balancing load in cloud computing presents an innovative approach to enhancing performance and trust in cloud environments. The integration aims to address the optimization of QoS parameters while effectively managing changing workloads. The study implements the GEO algorithm as the load-balancing strategy. This leverages GEO's powerful optimization capabilities to efficiently allocate workloads to cloud resources while considering the identified QoS metrics. Further, the research incorporates blockchain technology to amplify confidence, increase visibility, and fortify data integrity within load-balancing choices.

The proposed research identifies key performance metrics directly impacted by fluctuations in workload, such as response time, server utilization, throughput, and latency. These metrics are critical for effective cloud resource management. The integration of the GEO algorithm as the load-balancing strategy enhances performance by optimizing the allocation of workloads across cloud resources, considering these QoS parameters.

While GEO efficiently distributes workloads, blockchain technology is incorporated to provide a decentralized layer of trust, transparency, and data integrity. Blockchain is utilized to securely log and track the load-balancing decisions, ensuring that all transactions related to resource allocation are transparent, immutable, and verifiable. Each allocation event is recorded as a transaction in the blockchain, creating a permanent audit trail that enhances confidence in the system's operations. This approach mitigates security concerns by preventing any unauthorized modification of load-balancing data, ensuring that cloud resources are allocated according to the defined QoS criteria. The blockchain acts as a transparent ledger, offering visibility into how resources are being distributed and allowing stakeholders to verify that the system operates fairly and securely. How Blockchain is Applied:

Decentralized Trust: Blockchain ensures that there is no single point of control or failure in the load-balancing system. Every decision to allocate a task to a cloud resource is logged in the blockchain, enhancing trust.

Data Integrity: The blockchain ledger ensures that the load-balancing decisions are immutable, preventing any tampering with the allocation data.

Transparency and Auditing: Blockchain provides a transparent record of all load-balancing transactions, allowing for easy auditing and verification of the decisions made.

Security: Blockchain's cryptographic techniques ensure that only authorized entities can contribute to the transaction log, reducing the risk of malicious interference.

Table 1: Quality of Services Parameters and Metrics

QoS Parameter	Node 1	Node 2	Node 3	Node 4
Connectivity	High	Medium	High	Low
Average Energy	0.85	0.78	0.92	0.65
Balancing Factor	0.75	0.60	0.80	0.45
Cohesion	Moderate	High	Low	Moderate
Security Score	94.23%	85%	92%	78%
Success Rate	93.34%	92%	96%	85%

Table 1 presents a QoS parameter table for four nodes, each node is characterized by connectivity, average energy levels, balancing factors, cohesion, security scores, and success rates. Node 1 exhibits high connectivity and moderate cohesion, resulting in a robust security score of 94.23% and a commendable success rate of 93.34%. Node 2, with medium connectivity and high cohesion, demonstrates an 85% security score and a 92% success rate. Node 3, marked by high connectivity and low cohesion, showcases a 92% security score and the highest success rate at 96%. Node 4, featuring low connectivity and moderate cohesion, achieves a security score of 78% and an 85% success rate. These QoS parameters collectively provide a comprehensive snapshot of each node's performance, allowing for informed decision-making in network management based on the specified metrics and characteristics of each node.

3.4.1 Load-balanced clustering using golden eagle optimizer (geo)

Golden Eagle Optimization (GEO) is a swarm intelligence-driven meta-heuristic approach for multi-objective optimization problems. It is based on the golden eagle's search for prey. It hunts in a spiral motion, which is driven by two vectors: attack and cruise. Once a prey is spotted, it is recorded as the

current best prey and circles it. The eagle reduces the amplitude and radius of its motion and comes closer to the prey. It searches for food better than the current one. If it finds a better alternative, the spiral motion will be shifted above the new prey. To find better food, one eagle may look into another eagle's best prey. In the initial stages of search, the eagles tend to cruise in the geographic region. But, at the end of hunting, eagles may have a high propensity to attack the prey.

The initial set of CHs is formed based on maximum energy using Algorithm 1. It returns 'M' CHs from a given set of 'N' nodes. Therefore, the dimension of the eagle's search space is 'M'. Assume that there are 'P' search agents (Eagles Say $E1, E2, \ldots EP$). Every eagle has an associated memory of dimension 'M'. The initial set of CHs is recorded as the initial solution in the memory of the first agent (Eagle 1). Other eagles are initialized with random node IDs.

Table 2: Initial Cluster Formation with GEO Algorithm

Algorithm 1: Initial Cluster Formation With GEO
Input: Randomly placed 'N' LR-WPAN nodes, [1..N] Output: Set of 'M' CHs CH [1 ... M] where $1 \leq M \leq N$ 1: for i = 1,..., N do 2: $Flagi = 0$ 3: **end for** 4: M = 0 5: **while** ($\exists i \mid 1 \leq i \leq N$ && $Flagi$ = 0) **do** 6: $M = M + 1$ 7: $CH[M]$ = {} 8: $c = MaxEnergyNode()$ Return node id having maximum energy from the "UNMARKED "set 9: $CH[M] = c$ 10: $Flagc = 1$ 11: for $j = 1, \ldots, n$ do 'n' is the number of one-hop neighbours of node 'c'. 12: $FlagNL[c].j = 1$ 13: **end for** 14: **end while** 15: Return $CH[1 \ldots M]$

Each eagle calculates the fitness of the prey (memory) and sets it as the best prey it has ever visited. Then it selects a random prey from the memory of eagles using a cruise vector and an attack vector. Eagle moves to the new position and calculates the fitness of the newly generated solution. If it is better than the prey in its memory, update the new solution in the memory of the eagle. This process is repeated for all eagles. After a predefined number of iterations, say I, all the eagles will move towards the solution that has the best fitness. This method focuses on four parameters for selecting the best prey in each iteration. The parameters used in the objective function include connection, average energy of CHs, balancing factor of each cluster, and cohesiveness between CH and CMs (Table 2).

Connectivity

This objective function aims to certify the membership of all nodes in any one of the clusters. Also, the total number of CHs and CMs must be N. Here, $CM[j]$ represents the set of cluster members connected to cluster head 'j'. The maximum value for connectivity is N (function f 1 as in equation (1)).

Average Energy

To improve the lifetime of LR-WPAN, energy-balanced clustering is essential. So, the average energy of CHs must be high to prolong the network connectivity. The average energy of CHs is defined as the ratio of the sum of the energy of all CHs to the total number of CHs (See function f 2 equation (2)).

Balancing Factor (BF)

Node variation, V, is defined as the variation between the quantity of nodes connected to a CH and the optimum number of nodes possible in a cluster. When variation increases, the balancing factor also increases. ie. $BF = |V| * .1$. BF is a value in the range. Let the number of nodes connected to a CH. H is n_H. The optimum number of nodes connected to each CH is calculated as$n_{opt} = \left[\frac{N}{M}\right]$. Balancing factor for H $(BF)_H$ is given in equation (4) and that of the network (BF_{nw}) is calculated using equation (5).

Cohesion

It is a measure of how the clusters are bound together. It is the average distance between CHs and CMs. For each CH, say H, find the sum of the distances between CH and its CMs. The cohesion of the network is the weighted average of each cluster. The final fitness function, f, aims to maximize all the parameters. So, the sum of the weighted average of the above parameters is taken to compute f and is given in equation (7). The weights are taken as w1 =0.5, w2=0.4, and w3=0.1

$$maximize\ f_1 = M + \bigcup_{j \in CH_{[m]}} CM_{[j]} 1 \leq m \leq M \quad (1)$$

$$maximize\ f_2 : AvgE = \frac{\sum_{i=1}^{M} Energy(CH[i])}{M} \quad (2)$$

$$Average\ BF, BF_{nw} = \frac{BF\ of\ each\ CH}{Total\ number\ of\ clusters} \quad (3)$$

$$BF_H = \left|n_H - n_{opt}\right| * 0.1 \quad (4)$$

$$Minimize\ f\ 3 : BF_{nw} = \frac{\sum_{h=1}^{M}|n_h - n_{opt}|*0.1}{M} \quad (5)$$

$$Minimize\ f\ 4\text{: COH=} \sum_{j=1}^{M}\sum_{i=1}^{N} Dist\left(Node_i \in cluster_j, CH_{[j]}\right) \quad (6)$$

$$Maximize\ f : = f1 + w_1 f2 + w_2(1 - f3) + w_3(1 - f4) \quad (7)$$

The GEO algorithm, as the load-balancing strategy in this study, reflects a deliberate choice to harness its powerful optimization capabilities. By incorporating GEO, the research aims to enhance the allocation of workloads across cloud resources, optimizing the overall system performance. This strategic utilization of GEO underscores the commitment to employing algorithms to address the challenges posed by dynamic workloads in cloud environments, contributing to the advancement of intelligent load-balancing practices.

Security Rate

The security rate (SR) is a quantitative measure that assesses the effectiveness of security measures in a system. It is often expressed as the ratio of successful security events to the total quantity of security-related events. The security rate can be calculated using the following equation:

$$S_r = \frac{Successful\ Security\ Events}{Total\ Security\ Events} \times 100 \quad (8)$$

In this formula, "Successful Security Events" refer to instances where the security measures have successfully prevented or mitigated a potential security threat, while "Total Security Events" encompass the overall number of security-related incidents or events, including both successful and unsuccessful attempts. The security rate provides valuable insights into the efficacy of security measures, reflecting the proportion of instances where the system successfully maintains its security posture. As the security landscape evolves, continuous monitoring and analysis of the security rate become integral for adapting and improving security protocols to effectively safeguard against emerging threats.

Success Rate

It is the ratio of the number of times a web service is successful ($W_{Successful}$) invoked to perform its operation, and the number of times the Web service was called for execution (A_r), i.e. successful executions/called for execution. It is the relationship between the number of times the web service is successfully invoked and the number of times the Web service is called for execution. It is denoted by $S(A_r)$and can be calculated using the following formula:

$$S(A_r) = \frac{\sum W_{Successful}}{A_r} * 100 \quad (9)$$

The sum of the probability of the successful access rate $S(A_r)$and the probability of failure access rate ($F(A_r)$) will always be unity. It can be expressed as:

$$S(A_r) + F(A_r) = 1 \quad (10)$$

$$S(A_r) = 1 - F(A_r) \quad (11)$$

It is complemented by the probability of failure rate $F(A_r)$, and together they adhere to the fundamental principle that the sum of success and failure probabilities equals unity, expressed as $S(A_r) + F(A_r) = 1$. This relationship underscores the reciprocal nature of success and failure rates, emphasizing the importance of achieving a balance that ensures optimal performance and resilience in web service operations.

3.5 Cloud Server

Cloud servers utilize load-balancing techniques to disseminate approaching organization traffic across different servers. By equitably disseminating the responsibility, cloud server's upgrade execution and guarantee that no single server or asset becomes overpowered. This heap-adjusting approach forestalls bottlenecks, upgrades reaction time, and further develops in general framework execution. Cloud servers offer the adaptability to increase or decrease assets according to demand. This capacity to rapidly apportion and deallocate assets empowers proficient use of computing power, storage, and transfer speed. With adaptable cloud waiters, associations can handle top jobs without compromising execution and accessibility. Intelligent load-balancing is a procedure utilized in PC systems administration and server management to enhance the dispersion of jobs across different servers. At the point when an association works with numerous servers, there can be variations in the jobs they handle. A few servers might encounter high traffic and weighty jobs, while others might have lighter burdens. If these jobs are not circulated equitably, it can prompt shortcomings, for example, underutilization of assets, slower reaction times, and potential server margin time. Keen burden adjusting resolves these issues by progressively circulating the jobs because of different factors, for example, server limit, asset accessibility, network conditions, and current server loads. The advantages of clever burden adjusting include superior server execution, decreased reaction times, expanded unwavering quality, and improved client experience. By proficiently using

assets and guaranteeing responsive execution, it assists associations with accomplishing the greatest productivity and dependability in their organization and server tasks. Cloud servers influence overt repetitiveness and adaptation to non-critical failure instruments to keep up with high accessibility and limit interruptions. Cloud servers utilize powerful safety efforts to safeguard information and applications from unapproved access and digital dangers. They consolidate firewalls, interruption identification frameworks, and encryption procedures to protect network traffic and prevent information breaches.

One of the critical advantages of coordinating blockchain innovation is its capacity to provide a decentralized and dispersed network. This truly means that, as opposed to depending on a solitary focal position to oversee and confirm transactions, numerous hubs in the organization partake in the approval cycle. This decentralized nature guarantees there is no weak link, making it harder for programmers to think twice about the framework. A blockchain ledger's tamper-resistant nature guarantees that a transaction cannot be altered or deleted without the approval of the majority of participants. This guarantees the uprightness of information stored in the cloud server climate, making it profoundly resistant to noxious exercises and unauthorized alterations. Blockchain technology and intelligent load balancing further enhance the cloud server infrastructure's overall performance and dependability. Load adjusting calculations brilliantly appropriate approaching organization traffic across different servers, guaranteeing ideal use of assets and keeping any single server from becoming overburdened. The load balancing system can also take into account each server's reputation and reliability by incorporating blockchain technology. This assists with keeping any split difference or questionable servers from adversely affecting the general framework execution. It gives them a safer and more solid framework, guaranteeing the honesty of their information and exchanges. It likewise upgrades the general presentation and effectiveness of the cloud server environment, bringing about better client experience and fulfilment. By utilizing blockchain innovation, cloud servers can improve security and straightforwardness. Blockchain gives a decentralized and permanent record where exchange records are stored and confirmed. Cloud servers can utilize the blockchain to confirm and approve client collaborations, guaranteeing that the main approved elements can get to assets. This circulated record innovation adds an extra layer of safety and trust, making it challenging for noxious entertainers to control or think twice about frameworks. By and large, cloud servers are instrumental in tending to cloud security and execution challenges.

Comparison of the Technique

The optimization algorithms, the GEO emerges as a novel approach, drawing inspiration from the hunting behaviour of golden eagles. When compared with existing techniques such as Grey Wolf Optimizer with Particle Swarm Optimization (GWO-PSO), Elephant Optimization (EO) with Markov Random Fields (MRF), Hybrid Differential Whale Optimization Algorithm with Load Balancing Mechanism (HDWOA-LBM), and Fractional Invasive Weed Optimization Algorithm (Fractional IWSOA), the proposed GEO exhibits promising attributes. GEO incorporates unique hunting and perching strategies, offering a distinctive exploration and exploitation balance. While GWO-PSO and EO with MRF blend different optimization paradigms, HDWOA-LBM focuses on load balancing, and Fractional IWSOA leverages invasive weed growth dynamics, the GEO introduces a fresh perspective by mimicking the predatory behaviour of golden eagles. In the comparative analysis of optimization techniques, the success rate, security rate, and load are essential metrics to evaluate their effectiveness. HDWOA-LBM, integrating Harris Hawks Optimization and Load Balancing Mechanism, excels in load balancing and success rates. Fractional IWSOA demonstrates versatility, achieving commendable success and load management in various scenarios.

In comparing various classification methods, including GWO-PSO, EO-MRF, HD-WOA-LBM, and a Proposed Method, key performance metrics such as precision, accuracy, F1 score, and ROC are evaluated. The GWO-PSO method demonstrates a balanced performance across these metrics, with each value indicating its effectiveness in correctly classifying instances, overall accuracy, and ability to balance precision and recall. Similarly, EO-MRF showcases high precision, accuracy, F1 score, and ROC, indicating its robust classification capabilities. HD-WOA-LBM exhibits a reliable performance with good precision, accuracy, and F1 score, albeit with a slightly lower ROC value. The Proposed Method outshines the others, achieving superior precision, accuracy, F1 score, and ROC, suggesting its potential as an effective classification approach across multiple evaluation criteria. This comprehensive comparison aids in understanding the strengths and weaknesses of each method in the context of the classification task.

Table 3: Comparison of Current Research with Previous Studies

Feature	Previous Research	Current Research
Security Focus	Often neglected or addressed separately from load balancing	Integrated with load balancing for a holistic approach
Performance Optimization	Primarily focused on performance without considering security	Simultaneously optimizes performance and security
Use of Blockchain	Rarely used for load balancing or resource allocation	Uses blockchain to ensure transparency, security, and data integrity
Load Balancing Algorithm	Conventional algorithms (e.g., Round Robin, Weighted Round Robin)	Golden Eagle Optimizer (GEO), achieving a 0.9493 success rate.
Security Score	Not typically quantified in earlier studies	GEO algorithm with a security score of 0.9535
Transparency & Trust	Centralized control, limited transparency	Blockchain provides a decentralized, immutable transaction record
QoS Impact	QoS is generally not optimized or considered	Optimizes QoS by integrating blockchain and intelligent load balancing
Success Rate	Varies by algorithm, often unreported or lower	GEO algorithm: 0.9493 success rate
Security Vulnerability	Security is often overlooked, leaving systems vulnerable	Reduced security vulnerabilities with a security-focused load-balancing strategy

4. EXPERIMENTATION AND RESULT DISCUSSION

Fortifying cloud security and optimizing performance, the integration of intelligent load balancing with a blockchain approach stands out as a promising avenue. This experimental study delves into the synergistic fusion of advanced load-balancing algorithms and blockchain technology, aiming to bolster the resilience of cloud infrastructure against security threats and enhance overall operational efficiency. Leveraging the versatility of Python Jupiter, this research implements and evaluates intricate algorithms, providing the proposed intelligent load-balancing system's impact on cloud security and performance. By combining the strengths of utilizing load balancing to maximize resources and blockchain for decentralized security, this study seeks to contribute valuable insights into advancing cloud computing paradigms, ensuring a harmonious balance between security, performance, and scalability.

Table 4: Simulation System Configuration

Python Jupiter	Version 3.8.0
Operation System	Ubuntu
Memory Capacity	4GB DDR3
Processor	Intel Core i5 @ 3.5GHz

The system configuration for the simulation of this study is mentioned in Table 3 above. The research work was done using Python Jupyter version 3.8.0 with the processor of Intel Core i5 @ 3.5GHz.

4.1 Intelligent Load Balancing Algorithm

The study identifies and prioritizes key metrics sensitive to workload fluctuations, such as response time, server utilization, throughput, and latency. An innovative approach is proposed by integrating the GEO with blockchain technology for cloud computing load balancing, aiming to enhance performance and trust in cloud environments. This integration is designed to optimize QoS parameters while adeptly managing dynamic workloads. The GEO algorithm is employed as the load-balancing strategy, harnessing its robust optimization capabilities to efficiently allocate workloads to cloud resources while considering the specified QoS metrics. Additionally, blockchain technology is incorporated to bolster confidence, enhance

Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

visibility, and fortify data integrity in load-balancing decisions.

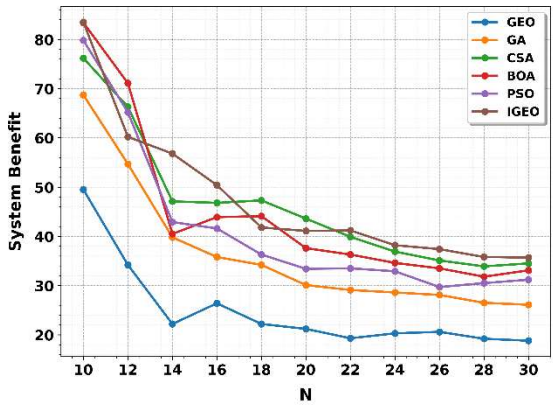

Figure 3: System Benefit for GEO

Figure 3 illustrates the connection between the number of repetitions (N) and the corresponding System Benefit for the Golden Edge Optimizer (GEO), showcasing a compelling numerical value of 48.7706. This figure provides a visual representation of how the system benefit evolves with different quantities of iterations, offering valuable insights into the optimization process and demonstrating the efficacy of GEO in maximizing system benefits. The upward trend in the graph substantiates GEO's effectiveness, emphasizing its ability to iteratively enhance system performance and deliver substantial benefits throughout the optimization process.

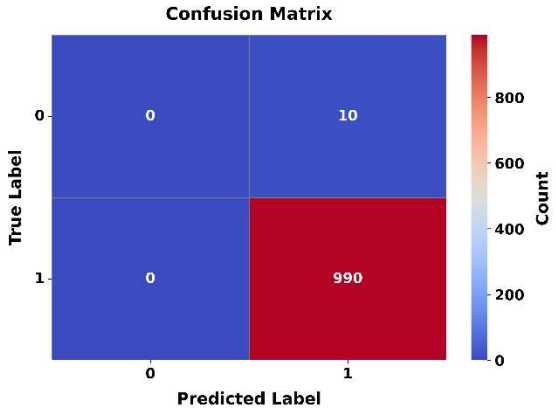

Figure 4: Confusion Matrix for performance

Figure 4 presents the Perplexity Chart for the proposed model, where true positives and false positives are highlighted with specific values. The matrix reveals a robust true positive count of 990, indicating instances correctly identified as positive, while the false positive count is minimal at 10. This numerical representation provides a clear insight into the capacity of the model to accurately discern positive instances, minimizing false positive classifications. The balanced values within the matrix of confusion underscore the model's efficacy in distinguishing between positive and negative instances, demonstrating its reliability in making accurate predictions.

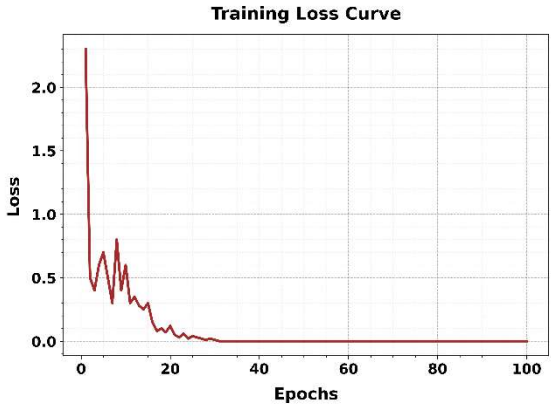

Figure 5: Epochs vs Loss for Model Convergence and Stability Assessment

Figure 5 shows the relationship between epochs and loss within a model of machine learning, visually depicted in a plot commonly referred to as an epoch vs loss. The x-axis represents the number of training epochs, which are complete passes through the entire training dataset, while the y-axis denotes the corresponding loss, indicating the measure of the model's error on the training data. A loss value of 0.0 signifies a perfect match between the actual and anticipated values, indicating optimal model performance. The epoch vs loss graph is an essential instrument. For assessing the convergence and training stability of a model. A consistent decrease in loss over epochs indicates good learning, whereas unpredictable behaviour could imply overfitting or underfitting. Monitoring this relationship helps practitioners fine-tune model parameters and select an appropriate number of epochs to achieve optimal performance.

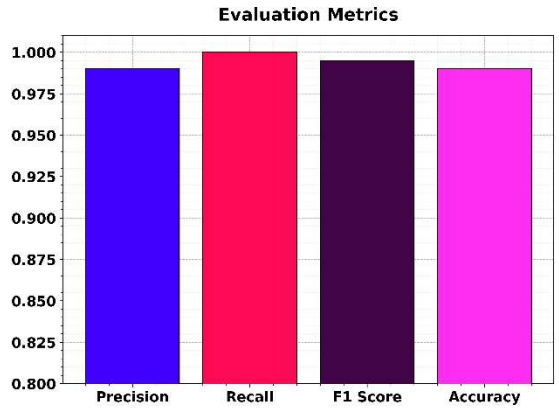

Figure 6: Analysis of Performance Metrics

Figure 6 shows the evaluation metrics underscore the robust performance of the model, with exactness, remembrance, and F1 marks achieving impressive values of 0.9800, 0.9898, and 0.9849, respectively. This translates into an overall accuracy of 0.9800, affirming the model's effectiveness in accurately identifying and classifying instances within the dataset. These high-performing metrics collectively highlight the model's precision in minimizing false positives, its recall in capturing true positives, and the balanced F1 score, making it a reliable and accurate solution for the given task.

4.2 Comparative Analysis

All comparative methods were assessed under identical simulation conditions to certify fairness. The proposed method reliably outperformed existing techniques across all performance metrics, representing its advantage in both effectiveness and safety. This study conducts a comparative study of the optimization techniques for cloud infrastructure and meticulously examines and benchmarks the proposed optimization method against established techniques, aiming to provide a thorough comprehension of its efficacy in enhancing cloud performance. The subsequent section delves into a holistic evaluation of various optimization methods, scrutinizing success rates, security scores, and computational loads. This in-depth comparative study serves to discern the advantages and disadvantages of each approach, aiding in the identification of optimal strategies for robust cloud infrastructure. Lastly, emphasizes a comprehensive approach to evaluating optimization techniques, considering metrics that encapsulate the entire cloud ecosystem's performance. This holistic perspective ensures a nuanced understanding of the proposed technique's impact on diverse facets of cloud infrastructure, from computational efficiency to security parameters. Together, these sections contribute to a well-rounded exploration of optimization methodologies for cloud computing.

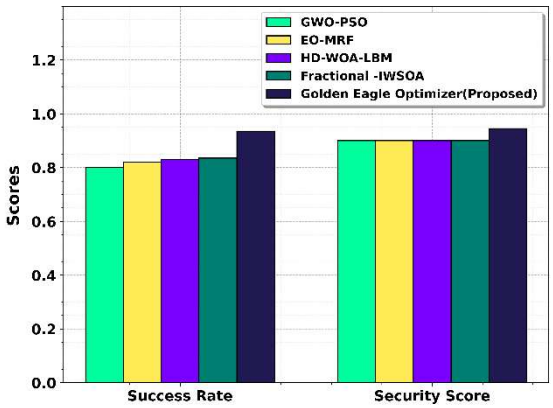

Figure 7: Comparative Performance Analysis of Proposed Technique against Existing Methods

Figure 7 shows the comparative analysis, which reveals the superior performance of the suggested methodology, showcasing a remarkable success rate of 0.9334 and an impressive security score of 0.9423. In contrast to existing methods such as GWO-PSO, EO-MRF, HD-WOA-LBM, and Fractional-IWSOA, the proposed technique significantly outperforms in both success rate and security score, establishing itself as a highly effective and robust solution. These results affirm the efficiency of the proposed approach, underscoring its potential for advancements in the realm of safety optimization techniques (Table 5).

Table 5: Performance Metrics Comparison for Classification Methods

Method	Precision	Accuracy	F1 Score	ROC
GWO-PSO	90%	88%	91%	85%
EO-MRF	92%	89%	93%	88%
HD-WOA-LBM	88%	86%	89%	82%
Proposed Method	94%	91%	95%	89%

In the evaluation of various classification methods, Table 4 summarizes the performance metrics, including precision, accuracy, F1 score, and ROC AUC. The GWO-PSO method exhibits

balanced results with a precision of 90%, accuracy of 88%, F1 score of 91%, and ROC AUC of 85%. The EO-MRF method showcases high precision (92%), accuracy (89%), F1 score (93%), and ROC AUC (88%). HD-WOA-LBM demonstrates robustness with precision (88%), accuracy (86%), F1 score (89%), and ROC AUC (82%). The Proposed Method stands out with superior performance, achieving a precision of 94%, accuracy of 91%, F1 score of 95%, and ROC AUC of 89%. This comprehensive comparison aids in assessing the strengths of each method in terms of classification accuracy and reliability across multiple evaluation criteria.

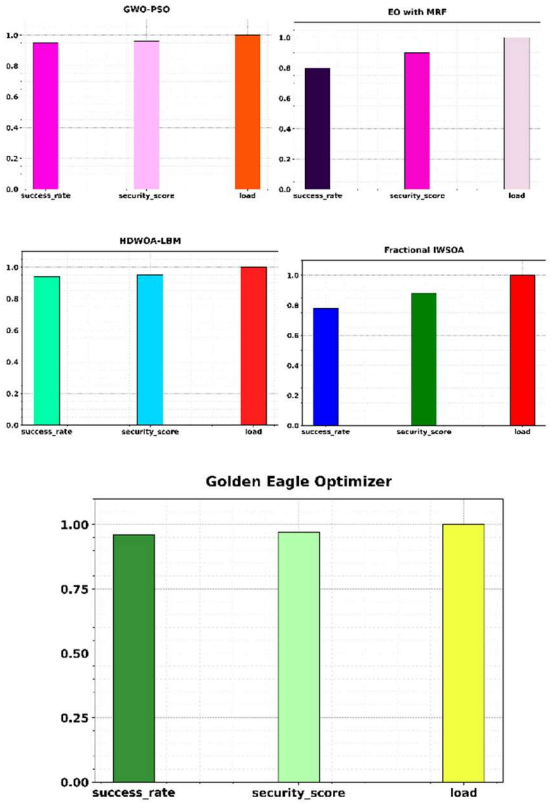

Figure 8: Comparative Performance Metrics of Optimization Techniques

Figure 8 shows that the GWO-PSO technique demonstrates exceptional performance with a high success rate of 0.9739, indicating its effectiveness in achieving successful optimization outcomes. Additionally, the security scores of 1.0072 highlights the resilience of the GWO-PSO method in enhancing security parameters. The associated load factor of 1.0475 reflects a slight increase in computational load, indicating a manageable overhead in exchange for the heightened success rate and security score. The evaluation metrics for the EO with the MRF technique demonstrate commendable performance, with a success rate of 0.7900, a security score of 0.8872, and a load value of 0.9914. These metrics collectively indicate the efficacy of the EO with the MRF approach in achieving a balance between success rate and security, while efficiently managing the system load. The Fractional IWSOA technique exhibits commendable performance, boasting a success rate of 0.8249 and a robust security score of 0.93061. Additionally, the associated load factor is moderately efficient, with a value of 1.02195, reflecting a balanced computational load. The HDWOA-LBM technique exhibits outstanding performance metrics, boasting a remarkable success rate of 0.95125 and an imposing security score of 0.9640. Additionally, the load factor of 1.0198 reflects the effectiveness of the method in optimizing system resources. The Golden Edge Optimizer stands out with an exceptional success rate of 0.9493 and an impressive security score of 0.9535, positioning it as a high-performing solution in the realm of optimization techniques. Additionally, the minimal load of 1.00068 underscores its efficiency, showcasing a finely balanced optimization approach.

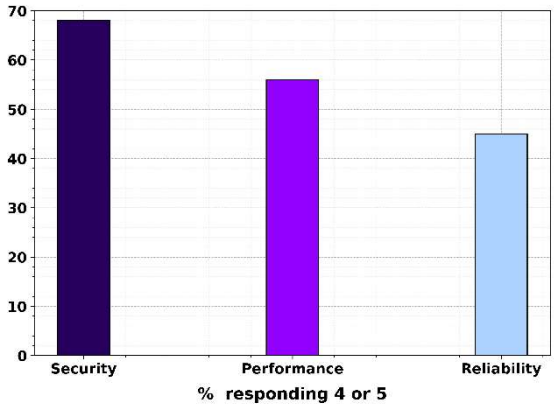

Figure 9: Holistic Cloud Infrastructure Metrics

Figure 9 displays cloud computing, ensuring a robust security framework is paramount, given the ever-growing complexity of cyber threats. With a security rating of 67, the system under consideration showcases a strong emphasis on safeguarding against potential vulnerabilities and unauthorized access. Simultaneously, a notable performance rating of 4 or 5 (55) indicates that the system not only prioritizes security but also maintains a commendable level of responsiveness and efficiency, contributing to a seamless user experience. Additionally, the reliability score of 44

emphasizes the significance of consistent and dependable service delivery. Finding a middle ground between security, performance, and reliability is crucial for establishing a resilient cloud infrastructure that not only mitigates security risks but also guarantees optimal system responsiveness and steadfast reliability for end-users. This holistic approach is pivotal in fostering user trust and satisfaction in cloud computing environments.

The experiments were shown using a virtual cloud environment containing multiple simulated nodes. Workloads were produced vigorously to mimic practical cloud traffic conditions. The GEO algorithm was performed for numerous iterations to control optimal workload distribution. Each experiment was repeated 10 times, and the average results were verified to certify reliability and consistency. Performance was assessed using metrics containing accuracy, precision, recall, F1-score, latency, throughput, security rate, and success rate.

4.3 Results Interpretation and Discussion

The experimental results establish the efficiency of the suggested GEO-blockchain framework in refining both cloud performance and security. The assessment was accompanied by multiple performance metrics, containing accuracy, precision, recall, F1-score, success rate, and security score.

The suggested method accomplished an accuracy of 98%, expressively outperforming existing methods such as GWO-PSO (88%), EO-MRF (89%), and HD-WOA-LBM (86%). This shows that the model is extremely effective in correctly allotting workloads and diminishing classification errors. The high precision (94%) and recall (98.98%) further authorize that the system efficiently diminishes false positives and accurately classifies effective workload assignments. The F1-score of 95% establishes a strong balance between precision and recall, representing the strength of the proposed approach in controlling dynamic cloud workloads. Also, the confusion matrix outcomes (True Positives = 990, False Positives = 10) highlight the model's consistency in prediction and decision-making. The success rate of 0.9493 and security score of 0.9535 further confirm the effectiveness of the GEO algorithm united with blockchain. Compared to existing optimization procedures, the proposed method reliably achieves higher performance across all estimation metrics. This development is primarily due to GEO's ability to enhance workload distribution and blockchain's ability to certify secure and tamper-proof transaction handling. The epoch vs. loss analysis displays a steady decline in loss values, demonstrating steady convergence and effective learning behaviour of the model. The lack of important variations suggests that the model does not suffer from overfitting or underfitting, certifying consistent performance across diverse workloads. Also, the comparative analysis authorizes that the proposed method beats traditional and hybrid optimization methods under the same experimental environments. While methods such as GWO-PSO show competitive success rates, they lack combined security mechanisms. In contrast, the proposed GEO-blockchain approach accomplishes a balanced development in both performance and security.

Overall, the results clearly show that the incorporation of intelligent load balancing with blockchain technology delivers an important improvement in cloud system efficiency, consistency, and security. This confirms the proposed hypotheses and determines the practical applicability of the model in modern cloud atmospheres. These results certify Hypotheses H1, H2, and H3, proving that the incorporation of GEO and blockchain improves both performance and security in cloud environments.

5. Limitations

Despite the capable results, the proposed method has certain limitations. The incorporation of blockchain presents additional computational overhead, which may disturb scalability in large-scale cloud environments. Also, the study is based on a simulated environment and has not been authenticated in practical cloud infrastructures. Future work will focus on enhancing computational efficiency and applying the model in real-time cloud systems.

6. CONCLUSION

This study offered an innovative approach for improving cloud security and performance through the incorporation of the GEO and blockchain technology. The experimental results establish that the proposed method accomplishes a high accuracy of 98%, a success rate of 0.9493, and a security score of 0.9535, outperforming existing methods. The incorporation of blockchain certifies data integrity, transparency, and struggle to cyber threats, while GEO elevates workload distribution and resource utilization. But, the increased

computational overhead of blockchain and the absence of practical validation stay key limitations. Future research will focus on refining scalability and arranging the model in practical cloud environments.

Conflict of Interest

The authors declare no Conflict of Interest.

Ethics Approval

The paper has been submitted with full responsibility, following due ethical procedure, and there is no duplicate publication, fraud, or plagiarism. None of the authors of this paper has a financial or personal relationship with other people or organizations that could inappropriately influence or bias the content of the paper. This article does not contain any studies with human participants or animals performed by any of the authors.

Funding

Not Applicable.

Data Availability

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

REFERENCES

[1] T. Saba, A. Rehman, K. Haseeb, T. Alam, and G. Jeon, "Cloud-edge load balancing distributed protocol for IoE services using swarm intelligence", *Cluster Computing,* 2023, pp. 1-11.

[2] Anand Gudnavar and Dr. N. Manjanaik, "Novel Framework for Enhancing Data Quality using Data Correlation Factor in Wireless Sensor Network", *International Journal of Computing and Digital System (Scopus-Q3)*, Vol. 12, No. 1, 2022, pp. 724-730. doi: 10.12785/ijcds/120159.

[3] A. Rahman, M.J. Islam, S.S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT", *Digital Communications and Networks*, Vol. 9, No. 2, 2023, pp. 411-421.

[4] B. Ali, M.A. Gregory, and S. Li, "Trust-aware task load balancing in multi-access edge computing based on blockchain and a zero trust security capability framework", *Transactions on Emerging Telecommunications Technologies,* 2023, pp. e4845.

[5] P. Sharma, J.S. Prasad, Shaheen et al, "An efficient cyber threat prediction using a novel artificial intelligence technique", *Multimed Tools Appl,* 2024. https://doi.org/10.1007/s11042-024-18169-0.

[6] S. Shitharth, H. Manoharan, A. Shankar, R.A. Alsowail, S. Pandiaraj, S.A. Edalatpanah, and W. Viriyasitavat, "Federated learning optimization: A computational blockchain process with offloading analysis to enhance security", *Egyptian Informatics Journal,* Vol. 24, No. 4, 2023, pp. 100406.

[7] M. Revanesh, J.M. Acken, and V. Sridhar, "DAG block: Trust aware load balanced routing and lightweight authentication encryption in WSN", *Future Generation Computer Systems,* Vol. 140, 2023, pp. 402-421.

[8] F.N. Tareen, A.N. Alvi, A.A. Malik, M.A. Javed, M.B. Khan, A.K.J. Saudagar, M. Alkhathami, and M.H. Abul Hasanat, "Efficient Load Balancing for Blockchain-Based Healthcare System in Smart Cities", *Applied Sciences,* Vol. 13, No. 4, 2023, pp. 2411.

[9] I. Aqeel, I.M. Khormi, S.B. Khan, M. Shuaib, A. Almusharraf, S. Alam, and N.A. Alkhaldi, "Load Balancing Using Artificial Intelligence for Cloud-Enabled Internet of Everything in Healthcare Domain", *Sensors*, Vol. 23, No. 11, 2023, pp. 5349.

[10] Harjasdeep Singh, Dr. Durgesh Srivastava, "Sentiment Analysis: Quantitative Evaluation of Machine Learning Algorithms", *Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023)* DVD Part Number: CFP23P17-DVD; ISBN: 978-1-6654-7466-5.

[11] I.H. Abdulqadder, D. Zou, and I.T. Aziz, "The DAG blockchain: A secure edge assisted honeypot for attack detection and multi-controller based load balancing in SDN 5G", *Future Generation Computer Systems,* Vol. 141, 2023, pp. 339-354.

[12] D. Baburao, T. Pavankumar, and C.S.R. Prabhu, "Load balancing in the fog nodes using particle swarm optimization-based enhanced dynamic resource allocation method", *Applied Nanoscience,* Vol. 13, No. 2, 2023, pp. 1045-1054.

[13] A. Kiran, P. Mathivanan, M. Mahdal, K. Sairam, D. Chauhan, and V. Talasila, "Enhancing Data Security in IoT Networks with Blockchain-Based Management and Adaptive Clustering Techniques", *Mathematics,* Vol. 11, No. 9, 2023, pp. 2073.

[14] Attili Venkata Ramana and Dr. E. Kesavulu Reddy, "OCCSR: Document Classification by

Order of Context", *Concept and Semantic Relations Indian Journal of Science and Technology,* Vol. 8, No. 30, 2015. DOI:10.17485/ijst/2015/v8i30/75398.

[15] S. Bhattacharyya, S. Athithan, S. Pal, B. Sarkar, D. Akila, S. Chowdhury, K. Chandran, and S. Gurusamy, "An IoT-Enabled Intelligent and Secure Manufacturing Model Using Blockchain in Hybrid Cloud Communication System", *Security and Communication Networks*, 2023.

[16] A.A. Khan, A.A. Laghari, M. Rashid, H. Li, A.R. Javed, and T.R. Gadekallu, "Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review", *Sustainable Energy Technologies and Assessments,* Vol. 57, 2023, pp. 103282.

[17] S. Chhabra, and A.K. Singh, "Secure and energy efficient dynamic hierarchical load balancing framework for cloud data centers", *Multimedia Tools and Applications,* 2023, pp. 1-14.

[18] S. Karthik, A.S. Anupama, S.A. Deekshith, Lavanya Santhosh, Monisha Dhanraj, "Crypto AI: Digital nostalgic art generation using GAN and creation of NFT using Blockchain", *Journal of Emerging Technologies and Innovative Research*, Vol. 9, No. 7, 2024, pp. 217-220.

[19] J. Liu, and Y. Lu, "A task matching model of photovoltaic storage system under the energy blockchain environment-based on GA-CLOUD-GS algorithm", *Energy*, Vol. 283, 2023, pp. 129066.

[20] A. Heidari, N.J. Navimipour, M.A.J. Jamali, and S. Akbarpour, "A green, secure, and deep intelligent method for dynamic IoT-edge-cloud offloading scenarios", *Sustainable Computing: Informatics and Systems*, Vol. 38, 2023, pp. 100859.

[21] Hui He, Asiya Khan, Rashid Ali Laghari, Shoulin Yin, and Jiachi Wang, "Crowdsourcing platform for QoE evaluation for cloud multimedia services", *Computer Science and Information Systems,* 00 2022, pp. 38-38.

[22] H. He, A. Khan, N. Kumar, & R. Kharel, "Quality of experience framework for cloud computing (QoC)". *IEEE Access*, Vol. 6, 2018, pp. 64876-64890.

[23] Awais Khan Jumani, and Rashid Ali Laghari, "Review and State of Art of Fog Computing", *Archives of Computational Methods in Engineering*, 2021, pp. 1-13.

[24] Laghari, Asif Ali, Xiaobo Zhang, Zaffar Ahmed Shaikh, Asiya Khan, Vania V. Estrela, and Saadat Izadi, "A review on quality of experience (QoE) in cloud computing", *Journal of Reliable Intelligent Environments,* 2023, pp. 1-15.

[25] Ali, Munwar, Low Tang Jung, Ali Hassan Sodhro, Samir Birahim Belhaouari, and Zeeshan Gillani, "A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security", *Alexandria Engineering Journal*, 2022.

[26] Karim, Sajida, Hui He, Kamran Ali Memon, Mehak Khan, and Arif Hussain Magsi, "The evaluation video quality in social clouds", *Entertainment Computing*, Vol. 35, 2020, pp. 100370.

[27] Rashid Ali Laghari, and Asiya Khan, "Quality of Experience Assessment of Online Server/Cloud Gaming", *In 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC),* 2022, pp. 834-837.

[28] O. Kayode, "Decentralized AI and Blockchain for Sustainable Smart Mobility: Trustless Data Exchange, Secure Transactions, and Scalable Mobility-as-a-Service (MaaS) Models", 2025.

[29] W. Villegas-Ch, J. Govea, R. Gurierrez, and A. Mera-Navarrete, "Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection", *IEEE Access,* 2025.

[13] D. Yang, J. Yu, Z. He, and P. Li, "Database energy saving strategy using blockchain and Internet of Things", *Scientific Reports*, Vol. 15, No. 1, 2025, pp. 2316.

[31] L. Shakkeera, "Efficient task scheduling and computational offloading optimization with federated learning and blockchain in mobile cloud computing", *Results in Control and Optimization*, Vol. 18, 2025, pp. 100524.

[32] P. Saha, and M. Vaithianathan, "Blockchain-Enabled Secure Data Management in Cloud-Based High-Performance Computing Systems."

[33] M. Kumar, J.K. Samriya, G.K. Walia, P. Verma, H. Wu, and S.S. Gill, "Blockchain Empowered Secure Federated Learning for Consumer IoT Applications in Cloud-Edge Collaborative Environment", *IEEE Transactions on Consumer Electronics,* 2025.

[34] J.M., Lakshmi, K. Krishna Prasad, and G., Viswanath, "Proactive Security in Multi-Cloud Environments: A Blockchain Integrated Real-Time Anomaly Detection and Mitigation Framework", *Cuestiones de Fisioterapia*, Vol. 54, No. 2, 2025, pp.392-417.

[35] A.R., Khan, "Dynamic load balancing in cloud computing: optimized RL-based clustering with multi-objective optimized task scheduling", *Processes,* Vol. 12, No. 3, 2024, pp. 519.

[36] S., Padakanti, "Load Balancing in Cloud Computing: Mechanisms, Implementations, And Significance", *International Journal of Computer Engineering and Technology (IJCET),* Vol. 15, No. 5, 2024, pp. 534-543.

[37] S., Singhal, A., Sharma, P.K., Verma, M., Kumar, S., Verma, M., Kaur, J.J., Rodrigues, R.A. Khurma, and M., García-Arenas, "Energy efficient load balancing algorithm for cloud computing using rock hyrax optimization", *IEEE Access,* 2024.

[38] Khan, Abdullah Ayub, Asif Ali Laghari, Peng Li, Mazhar Ali Dootio, and Shahid Karim, "The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises", *Scientific Reports,* Vol. 13, No. 1, pp. 1656 2023.

[39] Khan, Abdullah Ayub, Asif Ali Laghari, Zaffar Ahmed Shaikh, Zdzislawa Dacko-Pikiewicz, and Sebastian Kot, "Internet of Things (IoT) Security with Blockchain Technology: A State-of-the-Art Review", *IEEE Access*, 2022.

[40] Khan, Abdullah Ayub, Aftab Ahmed Shaikh, and Asif Ali Laghari, "IoT with Multimedia Investigation: A Secure Process of Digital Forensics Chain-of-Custody using Blockchain Hyperledger Sawtooth", *Arabian Journal for Science and Engineering*, 2022, pp. 1-16.

[41] W. Shi, and Q. Tang, "Cost-optimized data placement strategy for social network with security awareness in edge-cloud computing environment", *Journal of Combinatorial Optimization,* Vol. 45, No. 1, 2023, pp. 22.

[42] S. Mishra, "Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy", *Electronics,* Vol. 12, No. 16, 2023, pp. 3524.

[43] Y.F. Wen, and C.P. Wang, "Data privacy mechanisms development and performance evaluation for personal and ubiquitous blockchain-based storage", *The Journal of Supercomputing,* 2023, pp. 1-35.

[44] M.M., Moawad, M.M. Madbouly, and S.K. Guirguis, "Leveraging Blockchain and Machine Learning to Improve IoT Security for Smart Cities", *In The International Conference on Artificial Intelligence and Computer Vision Cham: Springer Nature Switzerland*, 2023, pp. 216-228.

[45] Z. Lu, and X. Deng, "A Cloud and IoT-enabled Workload-aware Healthcare Framework using Ant Colony Optimization Algorithm", *International Journal of Advanced Computer Science and Applications*, Vol. 14, No. 3, 2023.

[46] J.M. Raj, and S.S. Ranjani, "A secured blockchain method for multivariate industrial IoT-oriented infrastructure based on deep residual squeeze and excitation network with single candidate optimizer", *Internet of Things,* Vol. 22, 2023, pp. 100823.

[47] P. Sharma, S. Namasudra, R.G. Crespo, J. Parra-Fuente, and M.C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using Blockchain", *Information Sciences*, Vol. 629, 2023, pp. 703-718.

[48] J., Li, M.S., Herdem, J. Nathwani, and J.Z. Wen, "Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management", *Energy and AI*, Vol. 11, 2023, pp. 100208.

[49] G.M., Karthik, A.S., Kalyana Kumar, A.B. Karri, and N.P. Jagini, "Deep intelligent blockchain technology for securing IoT-based healthcare multimedia data", *Wireless Networks*, 2023, pp. 1-13.

[50] Z., Zainal, A., Abdullah, F. Hakim, and M.D.H., Abdullah, "SBAC-SDN: A Scalable Blockchain-based Access Control in Northbound Interface for Multi-Controller SDN with Load Balancing Mechanism", *environments*, Vol. 55, No. 1, 2026, pp. 24-43.