Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Integrating Honey Bee Load Balancing Algorithm with Role-Based Access Control in Blockchain Technology to Minimise Response Time in Cloud Computing

Daisy Sharmah[1*], Kanak Chandra Bora[2], Kshirod Sarmah[3], Hem Chandra Das[4], Deepak Hajoary[5], Alakesh Gogoi[6], Mir Kashem Ali[7], Kabyashree Buragohain[8]
[1*267]Department of Computer Science, University of Science & Technology Meghalaya, India
[3]Department of Computer Science, Pandit Deendayal Upadhyaya Adarsha Mahavidyalaya,Amjonga,Assam,India
[4] Department of Computer Science and Technology, Bodoland University, BTR, Assam, India
[5] Department of Management Studies, Bodoland University, BTR, Assam, India
[8] Department of Computer Science and Engineering, Tezpur University, India
*Corresponding author(s).E-mail(s): sharmah.daisy@gmail.com;
Contributingauthors:boopborabora@yahoo.in;
kshirodsarmah@gmail.com;hemchandradas78@gmail.com; hajoary.deepak@gmail.com;
gogoialakesh99@gmail.com; mirkashem787@gmail.com; buragohainkabyashree24@gmail.com

ARTICLE INFO

Received: 22 Dec 2024

Revised: 24 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

The RBAC is considered one of the best security mechanisms used in cloud computing to assign roles and grant specific permissions. The implementation of a RBAC mechanism for load balancing can enhance the overall performance of the server. In this paper, we are focusing on the significance of using the RBAC mechanism in the Honey Bee Load Balancing Algorithm to improve the security of the blockchain consortium system. We have proposed an algorithm using the concept of RBAC with Honey Bee Load Balancing Algorithm in Blockchain to minimize the response time in the Cloud computing. The proposed algorithm is simulated using CloudAnalyst and the results of simulation are shown in this paper. We have made a comparison study of our proposed algorithm with other four algorithms in blockchain technology.

Keywords: Virtual machine, cloud computing, access control, blockchain.

Abbreviations

LB	Load Balancing
HBBLB	Honey Bee Behaviour Inspired Load Balancing
HBLB	Honey Bee Load Balancing
HBA	Honey Bee Algorithm
TLB	Throttled Load Balancer
ATH	Advanced Throttled Algorithm
RR	Round Robin
ESCE	Equally Spread Current Execution
VM	Virtual Machine
VMID	Virtual Machine Identity Number
DC	Data Center
CC	Cloud Computing
MS	Milliseconds
UB	User Base
MBC	Modified Bee Colony
BFO	Bacterial Foraging Optimization
RBAC	Role Based Access Control
RT	Response Time
ORT	Overall Response Time
SBP	Service Broker Policy

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1 INTRODUCTION

In Cloud Computing (CC), Load Balancing (LB) is a methodology that offers methods to maximize throughput, optimize the utilization of resources, and better execution of the system [13]. The LB technique creates a method to store the data for the users based on its availability [9]. The main objective of Load Balancing is to distribute the load in the entire CC system [10]. LB in the cloud is the process of equivalently administering the functions on virtual machines (VM) for proper usefulness of all the hardware and software systems used [15]. There are different types of algorithms used based on different metrics [25]. As the demand for CC is increasing, therefore the workload of this system is also affected and as a result, the LB plays a very major role in the CC system [14]. Therefore, based on available research, the existing work has been identified and summarized in a systematic way that depicts issues and challenges for future research work [29]. The two versions of LB algorithms namely static and dynamic [11] where Static load balancing works best for systems with steady workloads and similar servers and Dynamic-based balancing algorithms are more adaptable and effective in both homogeneous and heterogeneous environments [30]. Load balancing in blockchain refers to the distribution of workload across multiple nodes in a blockchain network to ensure efficient resource utilization, improve performance, and maintain high availability. The Dynamic Load Balancing techniques can continuously monitor node performance and adjust the distribution of tasks in real-time based on current load and network conditions [26].

1.1 Role Based Access (RBAC) Mechanism

RBAC is a well-established approach for large-scale authorization, but the absence of a standardized general version creates uncertainty and confusion about its utility and implications, due to its relevance in merchandise and programs for the management of employer protection[1]. RBAC continually has been the focal point of standardization sports because the cloud server cannot be completely depended on by using information proprietors, they cannot depend upon servers to get entry to control [8]. Cipher text coverage attribute-primarily based Encryption is regarded as one of the maximum suitable technologies for information entry to control in cloud garage structures because it offers the data proprietor extra direct management on getting entry online[12][19]. The Structure Diagram of RBAC Mechanism is shown in Figure 1.

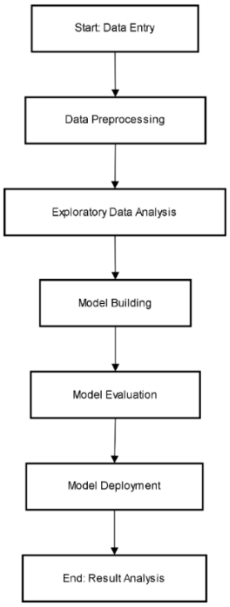

Fig. 1 RBAC StructureDiagram

1.2 Load Balancing (LB) Mechanism

LB plays an important role in maintaining activities in a CC environment. It helps in minimizing the response time to avoid system overload; also, it maximizes throughput as well as obtaining optimal resource utilization [5]. The purpose of LB is to avoid overloading and idleness of nodes in a cloud system. In CC platforms such as Windows Azure Platform, Amazon S3, etc., and usage in Artificial Intelligence [23] will enhance the development of many web searches with distinctive features, from cloud service providers. LB algorithms are necessary because they provide continuous services to users without service breaking.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1.3 Honey Bee Algorithm (HBA)

Honey Bee Algorithm is a nature-propelled decentralized load-balancing strategy that assists with accomplishing load adjusting across heterogeneous virtual machines of distributed computing environment through nearby server activity and expands the throughput [22]. The current workload of the VM is assessed to determine its state—whether it is overloaded, underloaded, or balanced. Based on this assessment, VMs are grouped accordingly. The priority of the task is taken into consideration after being removed from the overload VM which is waiting for the VM. Then the task is scheduled to the lightly loaded VM [30]. The earlier removed tasks help find the lightly loaded VM. These tasks are known as scout bees in the next step. Honey Bee Behaviour inspired LB technique reduces the response time of VM and also reduces the waiting time of task [32]. The search for food by honey bees from the bee hives to the food source is tracked using this algorithm. In bee hives, foraging bees give information about the food source they have visited to the other bees [19]. Honey Bee inspired LB is shown in Figure 2. In the figure, it is described as a potential newcomer bee starts as a naïve worker as it has no information about the food source. As the naïve bee starts starving for food, it becomes the Scout. When a scout gets information about the food source, it becomes a Recruit. The difference between the recruit and a scout is that a recruit has the memory of food sources, whereas, a scout does not have that information [31]. As soon as the bee finds a source, it performs a special dance known as "Waggle dance" with two purposes:

- **Distance Strategy:**It is used to distribute knowledge to other members about the distance of the food source.
- **Navigation Strategy:**It is used to distribute knowledge to other members about the direction of the food source.
    - Whenever the food source is found, the bees start to exploit the food source and subsequently, it becomes an exploiter or a forager.

This algorithm requires Scout and Forager agents LB Agents.

- **Scout Agents (Server Evaluators):** Similar to how scout bees search for food sources, scout agents in a network periodically assess each server's status. They evaluate server metrics like workload, processing power, and response time to identify which servers have the capacity for new tasks.
- **Forager Agents (Task Handlers):** Forager agents use the information gathered by scouts to handle incoming tasks. When a new task arrives, the forager agent assigns it to a server flagged by scouts as having sufficient availability or an optimal load level.

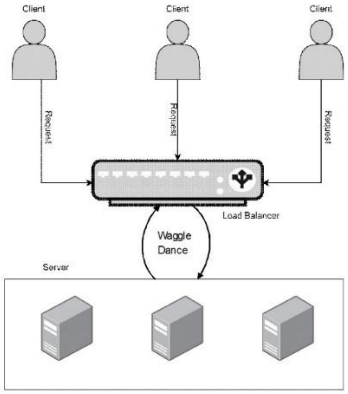

Fig. 2 Honey Bee Inspired Load Balancing Algorithm

1.4 Blockchain Mechanism

A blockchain is a decentralized approach that holds millions of data that are hashed in a deterministic hexadecimal number. This technology was introduced by Nakamoto to solve the double spending problem of bitcoin but soon this technology was being used in various applications [38]. Blockchain technology is merged and integrated with many types of applications such as the Internet of Things, healthcare, real estate, etc. It works in a block system [36]. Confirmation of the transaction should be approved and every single link of failure. This model does not cause the representative charges for approving exchanges such as broker fees.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2 LITERATURE REVIEW

Gupta et al.[36] reviewed different aspects of security in cloud computing using blockchain technology. The authors indicate the structure of blockchain the characteristics of blockchain and cloud computing security requirements are analysed.

Murthy et al.[37] dealt with some of the challenges of cloud computing like data security, server service, and user data management. The authors discussed the benefits of integrating blockchain in the cloud by developing architectures regarding blockchain integration.

Gai et al.[38] discussed three technical dimensions for reengineering cloud computing using blockchain. The authors indicated that blockchain-based cloud computing for powering up cloud data centers, has few technical dimensions for reengineering cloud datacentres using blockchain techniques. Three technical dimensions are involved namely, service, security, and performance. The authors mentioned several challenges of blending cloud computing using blockchain techniques.

Guo et al.[39] undertake a thorough study in this research, examining how to provide safe authentication and collaborative sharing, a trusted access mechanism must be established. As a result, in order to increase authentication efficiency, this study offers a distributed and trustworthy authentication system based on Blockchain and edge computing. An optimized practical Byzantine fault tolerance (PBFT) consensus mechanism is proposed to establish a consortium Blockchain for storing authentication data and logs over the Blockchain network.

Younis et. al [32] proposed in their paper an access control model to overcome the security issues in cloud security. The authors mentioned various access control models already been used for the cloud paradigm. They stated that their proposed model can fulfil all the requirements of cloud computing overcoming the drawbacks of existing models. They suggested that the model is easy to understand and dynamic.

Hashem et. al. [40] proposed an LB algorithm based on honey bee behaviour. Their main goal was to distribute the workload of multiple network links in a way that avoids underutilization and overutilization of the resources. The proposed algorithm calculation has been mimicked utilizing CloudSim. The proposed calculation is contrasted and both customary and SI-based LB calculations; RR, modified throttled, ant colony, and HBAs.

Ebadifard et. al. [41] stated that using an appropriate LB method can reduce response time and increase resource utilization proposed method reduces the makespan, increases the degree of LB, and improves the system`s reliability.

Kalaivani et.al. [42] mentioned that Feature selection plays an essential role in creating machine learning models. In this research work, they propose a technique for selecting container functions for IDS.

Rekha et. al. [35]proposed an enhanced model named Artificial Bee Colony Optimization (ABC) to multi-line the tasks whenever they are at the initial state. They compared their proposed model with the Shortest Job First (SJF) and Min-Min Best Fit (MMBF) algorithms. However, intrusion detection is not considered in their proposed work.

Zhou et. al [34] proposed a role-based encryption (RBE) scheme which integrates the cryptographic techniques with RBAC. Based on the proposed scheme, they presented a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud.

Sarmah S. [43] reviewed the applications of blockchain in cloud computing in the field of finance. The author reviewed the prior techniques for identifying challenges involving blockchain integration. However, the author stated that the communication between multi-party computations interrupts networks and results in unexpected financial loss and that creating fake accounts degrades the scalability of the system.

Zhao et al. [33] introduced the Improved Artificial Bee Colony (IABC) Optimization algorithm tailored for Flying Ad Hoc Networks (FANET) to enhance the convergence rate and exploitation capabilities. Their approach utilized a super mining node for block verification and processing.

3 IMPORTANCE OF RBAC IN DYNAMIC LOAD BALANCING

In the dynamic load balancing technique, RBAC ensures the users allocate the resources securely [21]. Based on the User logging into the application, the authentication is performed by the RBAC mechanism [27]. A particular role is provided to the user followed by a user request for the resource [6]. The dynamic load balancer checks the role of the user and also checks the best-suited server for

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the request [28]. After the selection of a server, the dynamic load balancer assigns the appropriate server to the user.

The assignment of tasks to the users can improve resource utilization and task efficiency in dynamic load balancing using the RBAC mechanism [7]. The available roles provided by RBAC for dynamic load balancing are [13]-

- **Admin**: These roles of users have to Create, Update, Delete, and Read permission. User access can be granted by this role.
- **Creator**: These roles users have to Create, Update, and Read permission. Delete permission is not accessed for this role.
- **Observer**: These roles of users have only Read permission.

4INTEGRATION OF RBAC WITH BLOCKCHAIN

Combining RBAC with blockchain technology creates a robust, transparent access management model with immutable transaction records [24]. In blockchain-integrated systems, access events can be recorded on a decentralized ledger, ensuring accountability and verifiability [3]. This transparency is essential in regulated industries, where strict access logs and audit trails are required for compliance with standards like HIPAA, GDPR, and SOX [37]. For example, an organization could record every access event associated with sensitive data on the blockchain. If an HR manager accesses an employee's records, the event is documented immutably, ensuring accountability. Blockchain's distributed ledger ensures that no single entity can alter these records, providing an added layer of security and trust in systems requiring auditable trails. Blockchain's role in RBAC can further extend to decentralized identity management. Users can verify their roles and credentials directly on the blockchain, reducing reliance on centralized identity systems and lowering risks associated with single points of failure [2].The RBAC and Blockchain integration is shown in Figure 3.

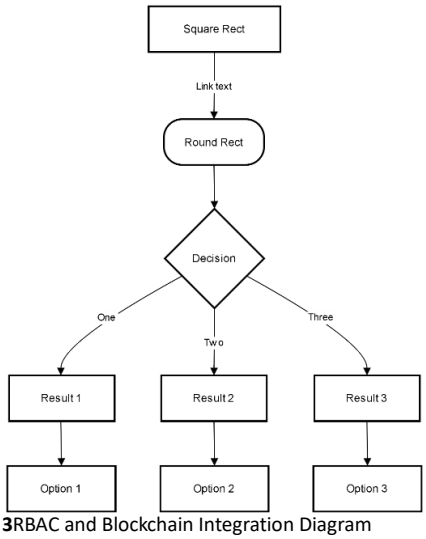

Fig. 3RBAC and Blockchain Integration Diagram

5IMPLEMENT RBAC AND THE HONEY BEE ALGORITHM IN CLOUD COMPUTING USING BLOCKCHAIN

RBAC can also enhance load balancing in cloud systems by aligning resource allocation based on roles [17]. A Honey Bee-inspired load balancing algorithm models the allocation of tasks similarly to how bees distribute foraging activities among worker bees [18]. In an RBAC environment, this model can prioritize resource allocation based on user roles and associated permissions, ensuring that critical tasks get the necessary resources during peak times [20]. Considering a healthcare application where doctors, nurses, and administrative staff have different roles with varying levels of access to patient data, scheduling systems, and reporting tools. During high-traffic periods, a load-balancing algorithm can prioritize requests from doctors, ensuring they receive timely access to patient records, thereby reducing response time and improving the quality of care [16]. This role-based load balancing could be adapted across various sectors where certain roles require rapid response times due to the critical nature of their tasks [34].

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Steps to Implement RBAC and the Honey Bee Algorithm in Cloud Computing Using Blockchain are given below-

Step 1. Deploy a cloud environment with distributed servers to accommodate resource allocation and load balancing.

Step 2. Create a blockchain-based ledger to store and manage RBAC policies, ensuring only authorized users can access specific resources.

Step 3. Define and store roles and access permissions for cloud resources on the blockchain, making these policies immutable and transparent.

Step 4. Implement the Honey Bee Algorithm to distribute incoming tasks dynamically across servers based on current load and capacity, using scout and forager agents.

Step 5. Log RBAC permissions and load-balancing decisions on the blockchain to ensure transparency, traceability, and security in access control and workload distribution.

Step 6. Continuously monitor system performance and blockchain transactions to optimize load distribution and RBAC rules as demand fluctuates.

The diagrammatic representation of the steps is given in Figure 4.

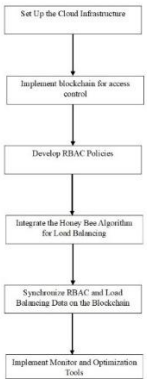

Fig. 4 Steps to implement RBAC and the Honey Bee algorithm in cloud computing using blockchain.

6PROPOSED HONEY BEE LOAD BALANCING WITH RBAC ALGORITHM USING BLOCKCHAIN

In the proposed model, the VM is always initialized to 0 and while the server sends the user requests, the user is checked using the RBAC Mechanism. After confirming the valid user, in the next phase, the load balancer selects a VM on a random basis. The load of the selected VM is compared with the threshold value and if the current VM value is less than or equal to the threshold value, then it will check the throughput of the current VM. Again, it is checked that if the throughput of the current VM is high, then the task is assigned to the current VM. Otherwise, the load balancer selects another VM on a random basis once again. If all the tasks are completed by VMs then the process stops and if not completed, then it waits for the server to send the next request.The Flowchart of our proposed HBLB with RBAC using Blockchain is shown in Figure 5.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

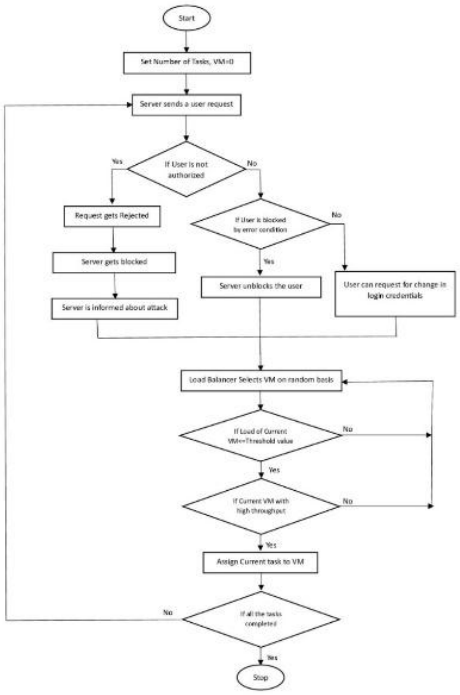

Fig.5 Flowchart ofProposed Honey Bee Load Balancing with RBAC using Blockchain

7 RESULT AND ANALYSIS

The calculation of throughput value is stated below.

$$T_p=M_t/P^t$$

Here, T_p is the throughput of a system, M_t is the Maximum completion time and P^t marks the initiation (or is the throughput of a system, Mt is the Maximum completion time and Pt marks the initiation (or commencement) of the first process. Based on the number of tasks, the Mt is calculated as

$$M_t = \sum_{t=1}^{n} T$$

Here t represents the number of tasks, T represents the sum of all the tasks. Throughput is the unit of information a system can process in a given amount of time. It is the calculation of several processes by the total scheduled time. Normally, a high throughput value is considered as the active VM. The VMs can be categorized based on their activity by giving priority to the throughput. The threshold value is a specific point or limit that serves as a boundary in decision-making processes. When an input crosses or meets this boundary, a certain action is triggered to meet this value.

7.1 Comparative Analysis

We have considered 4 different Scenarios considering the parameters- Data centers (DC), Virtual Machines (VM), User Bases (UB), and Time and Service Broker Policy (SBP). In the next step, we have created an arbitrary request in the blockchain environment. This step is followed by a selection of LB Algorithms and we have selected our Proposed Algorithm. In the same way, we have simulated the other four algorithms- Round Robin (RR), Equally Spread Current Execution (ESCE), Throttled Load Balancing (TLB), and Honey Bee Algorithm (HBA). The results of all the algorithms are analyzed later for comparison study. We have considered the average Response Time (RT), Maximum RT, and Minimum RT as performance metrics that are calculated in Milliseconds (MS). The experimental parameters for the four Scenarios are shown in Table 1.

Table 1 Experimental parameter

SCENARIO-1		***SCENARIO-2***	
PARAMETER NAME	**VALUE**	**PARAMETER NAME**	**VALUE**
USER BASES (UB)	6	USER BASES (UB)	4
DATA CENTER (DC)	6	DATA CENTER (DC)	4
VIRTUAL MACHINE	5 in each DC	VIRTUAL MACHINE (VM)	5 in each DC

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(VM)			
TIME	30 mins	TIME	30 mins
SERVICE BROKER POLICY (SBP)	Overall Response Time	SERVICE BROKER POLICY (SBP)	Overall Response Time
SCENARIO-3		***SCENARIO-4***	
PARAMETER NAME	**VALUE**	**PARAMETER NAME**	**VALUE**
USER BASES (UB)	6	USER BASES (UB)	2
DATA CENTER (DC)	2	DATA CENTER (DC)	1
VIRTUAL MACHINE (VM)	5 in each DC	VIRTUAL MACHINE (VM)	20 in each DC
TIME	60 mins	TIME	30 Hours
SERVICE BROKER POLICY (SBP)	Overall Response Time	SERVICE BROKER POLICY (SBP)	Overall Response Time

We have used CloudAnalyst for simulating the 5 algorithms namely, Round Robin (RR), Equally Spread Current Execution (ESCE), Throttled Load Balancing Algorithm (TLBA), Traditional Honey Bee Algorithm (HBA) and our Proposed Honey bee algorithm using RBAC mechanism in Blockchain to find the average, Minimum and Maximum Response Time. The simulation results for the four scenarios are shown in Table 2.

Table 2 Simulation Results for Scenario 1 to 4

SCENARIO 1				***SCENARIO 2***			
ALGORITHM	**AVG RT**	**MIN RT**	**MAX RT**	**ALGORITHM**	**AVG RT**	**MIN RT**	**MAX RT**
RR	50.11	37.62	61.65	**RR**	50.17	35.86	66.86
ESCE	50.11	37.62	61.65	**ESCE**	50.17	35.86	66.86
TLBA	50.11	37.62	61.65	**TLBA**	50.17	35.87	66.86
HBA	48.23	33.45	59.54	**HBA**	48.67	33.71	59.64
Proposed Algorithm	44.34	31.43	55.76	**Proposed Algorithm**	44.68	31.43	55.87
SCENARIO 3				***SCENARIO 4***			
ALGORITHM	**AVG RT**	**MIN RT**	**MAX RT**	**ALGORITHM**	**AVG RT**	**MIN RT**	**MAX RT**
RR	267.06	40.11	700.13	**RR**	127.02	38.51	239.17
ESCE	267.27	40.11	766.63	**ESCE**	127.02	38.51	239.17
TLBA	267.06	40.11	700.13	**TLBA**	127.08	38.51	239.17
HBA	262.57	38.09	655.67	**HBA**	123.98	36.73	235.21
Proposed Algorithm	256.65	34.16	651.13	**Proposed Algorithm**	119.32	28.26	229.31

The results of the simulations for the four criteria are represented graphically in Figure 6, Figure 7, Figure 8 and Figure 9.

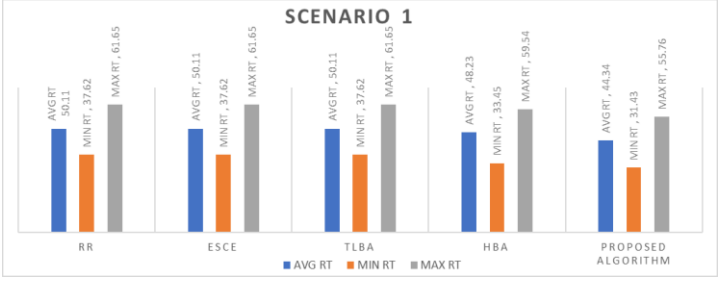

Fig. 6 Average, Maximum and Minimum RT for Scenario-1

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

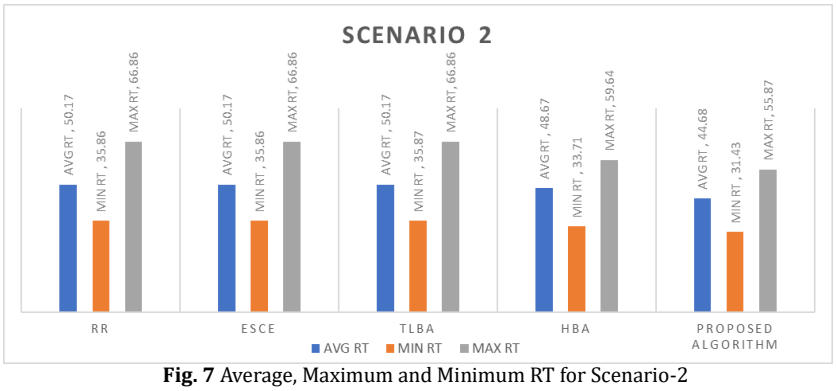

Fig. 7 Average, Maximum and Minimum RT for Scenario-2

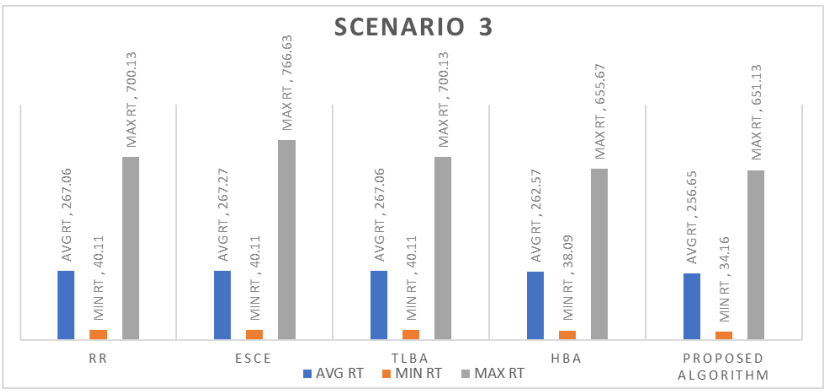

Fig. 8 Average, Maximum and Minimum RT for Scenario-3

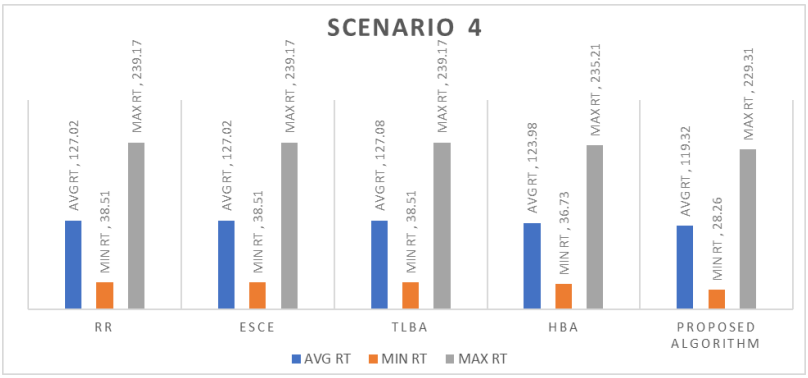

Fig. 9 Average, Maximum and Minimum RT for Scenario-4

From the above Figures it is clear that our proposed algorithm is taking less response time as compared with RR, ESCE, TLBA, HBA algorithms in the four scenarios. In Scenario 1 and Scenario 2, the Average RT our proposed algorithm performance is showing 11% better than RR, ESCE, TLBA and 8% better than Traditional HBA.In Scenario 3, the Average RT our proposed algorithm performance is almost 4% better than RR, ESCE, TLBA and almost 2% better than Traditional HBA. In case of Scenario 4, the Average RT our proposed algorithm performance is 6% better than RR, ESCE, TLBA and 4% better than Traditional HBA.

7 CONCLUSION AND FUTURE ENHANCEMENT

Load balancing is a critical component in blockchain networks, providing the necessary infrastructure to support high performance, reliability, and scalability [35]. Distributing tasks evenly across nodes, ensures the optimal functioning of the blockchain, making it robust and efficient[4][39]. While RBAC offers a powerful framework, implementing it in large, distributed environments poses challenges. Cloud systems with extensive roles and permissions can experience role explosion, where

the number of roles becomes difficult to manage. Balancing between too many and too few roles is a key challenge. In blockchain-integrated RBAC, scalability and interoperability also emerge as concerns since each access event added to the blockchain increases storage requirements and potentially impacts performance [43]. In our proposed work, we have found that the proposed algorithm is showing less response time in four scenarios. The response time is calculated in three categories like average, maximum and minimum response time.

Future developments could explore hybrid models combining RBAC with machine learning for automated role suggestion, enhancing scalability and adaptability. However, there are more dynamic LB algorithms that can be illustrated for our future work for multi-cloud and hybrid-cloud technology. Machine learning and artificial intelligence tools can be employed to analyze real-life congestion problems. The load balancers can be used in edge computing with the concept of edge load balancers to optimize the traffic. The concept of LB can be used together in CC as well as edge computing with the concept of blockchain.

CONFLICT OF INTEREST

There is no one involved for the conflict of interest in this paper.

REFERENCES

[1] Ahmed, T., Sandhu, R., & Park, J. (2017). Classifying and Comparing Attribute-Based and Relationship-Based Access Control. *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, 59–70. https://doi.org/10.1145/3029806.3029828

[2] Alshammari, M. A., Hamdi, H., Mahmood, M. A., & El-Aziz, A. A. A. (2023). Cloud Computing Access Control Using Blockchain. *International Journal of Intelligent Systems and Applications in Engineering*.

[3] Avik, S. C., Biswas, S., Ahad, A. R., Latif, Z., Alghamdi, A., & Bairagi, A. K. (2023).*Challenges in Blockchain as a Solution for IoT Ecosystem's Threats and Access Control: A Survey*.

[4] Baig, M. M. A. (2022). *Potential Challenges of Developing Large-Scale Computing Infrastructures over Distributed Clouds*. *71*(4).

[5] Balamurugan, B., Shivitha, N. G., Monisha, V., & Saranya, V. (2015). A Honey Bee behaviour inspired novel Attribute-based access control using enhanced Bell-Lapadula model in cloud computing. *International Confernce on Innovation Information in Computing Technologies*, 1–6. https://doi.org/10.1109/ICIICT.2015.7396064

[6] Banyal, R. K., Jain, V. K., & Jain, P. (2014). Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment. *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, 1–8. https://doi.org/10.1145/2677855.2677884

[7] Brahmam, M. G., & R, V. A. (2024). VMMISD: An Efficient Load Balancing Model for Virtual Machine Migrations via Fused Metaheuristics with Iterative Security Measures and Deep Learning Optimizations. *IEEE Access*, *12*, 39351–39374. https://doi.org/10.1109/ACCESS.2024.3373465

[8] Cha, B., Seo, J., & Kim, J. (2012). Design of Attribute-Based Access Control in Cloud Computing Environment. In K. J. Kim & S. J. Ahn (Eds.), *Proceedings of the International Conference on IT Convergence and Security 2011* (Vol. 120, pp. 41–50). Springer Netherlands. https://doi.org/10.1007/978-94-007-2911-7_4

[9] Choi, J., Choi, C., Ko, B., & Kim, P. (2014). A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. *Soft Computing*, *18*(9), 1697–1703. https://doi.org/10.1007/s00500-014-1250-8

[10] De, S. J., &Ruj, S. (2020). Efficient Decentralized Attribute Based Access Control for Mobile Clouds. *IEEE Transactions on Cloud Computing*, *8*(1), 124–137. https://doi.org/10.1109/TCC.2017.2754255

[11] Fischer, J., Marino, D., Majumdar, R., & Millstein, T. (2009). Fine-Grained Access Control with Object-Sensitive Roles. In S. Drossopoulou (Ed.), *ECOOP 2009 – Object-Oriented Programming* (Vol. 5653, pp. 173–194). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03013-0_9

[12] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and*

Communications Security, 89–98. https://doi.org/10.1145/1180405.1180418
[13] Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2015). Attribute-Based Access Control. *CO M P U T E R*.
[14] Jahid, S., Mittal, P., & Borisov, N. (2011). EASiER: Encryption-based access control in social networks with efficient revocation. *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 411–415. https://doi.org/10.1145/1966913.1966970
[15] Jayasankar, T., Bhavadharini, R. M., Nagarajanz, N. R., Mani, G., & Ramesh, S. (2021). Securing Medical Data using Extended Role Based Access Control Model and Two fish Algorithms on Cloud Platform. *European Journal of Molecular and Clinical Medicine*, *8*(1), 1075–1090.
[16] Lai, J., Deng, R. H., & Li, Y. (2012). Expressive CP-ABE with partially hidden access structures. *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, 18–19. https://doi.org/10.1145/2414456.2414465
[17] Luo, J., Wang, H., Gong, X., & Li, T. (2016). A Novel Role-based Access Control Model in Cloud Environments: *International Journal of Computational Intelligence Systems*, *9*(1), 1. https://doi.org/10.1080/18756891.2016.1144149
[18] Mohta, K. T., Panchal, K. J., & Student, P. G. (2016). *Improved Honey Bee Scheduling Algorithm for Load Balancing In Cloud Computing*. *2*(3).
[19] Oh, S., & Park, S. (2003). Task–role-based access control model. *Information Systems*, *28*(6), 533–562. https://doi.org/10.1016/S0306-4379(02)00029-7
[20] Oh, S., Sandhu, R., & Zhang, X. (2006). An effective role administration model using organization structure. *ACM Transactions on Information and System Security*, *9*(2), 113–137. https://doi.org/10.1145/1151414.1151415
[21] Park, J., & Sandhu, R. (n.d.). *Towards Usage Control Models: Beyond Traditional Access Control*.
[22] Peddi, D. P. (n.d.). *Data sharing Privacy in Mobile cloud using AES*. *7*(4).
[23] Peddi, P., & Arumugam, D. S. (2016). *Comparative Study on Cloud Optimized Resource and Prediction Using Machine Learning Algorithm*. *1*(3).
[24] Pereira, O. M., Regateiro, D. D., & Aguiar, R. L. (2014). Role-Based Access control mechanisms. *2014 IEEE Symposium on Computers and Communications (ISCC)*, 1–7. https://doi.org/10.1109/ISCC.2014.6912546
[25] Rani, P., Singh, P. N., Verma, S., Ali, N., Shukla, P. K., & Alhassan, M. (2022). An Implementation of Modified Blowfish Technique with Honey Bee Behavior Optimization for Load Balancing in Cloud System Environment. *Wireless Communications and Mobile Computing*, *2022*, 1–14. https://doi.org/10.1155/2022/3365392
[26] Sharmah, D., Bora, K. C., (2024).Utilizing Dynamic Load Balancing to Improve Private Cloud Paradigm, *International Journal of Information Technology*, 16(6), 3465-3474, https://doi.org/10.1007/s41870-024-01888-w
[27] Saunders, G., Hitchens, M., & Varadharajan, V. (2001). *Role-Based Access Control and the Access Control Matrix*.
[28] Sharmah, D., & Islam, A. U. (2022). *Implementation of Role Based Access Control and Dynamic Load Balancing in Model Analysis and Auditing Services*.
[29] Singh, J., & Kaur, B. (2015). Enhanced Load Balancing Architecture using EE-GA. *International Journal of Computer Applications*, *131*(7), 1–6. https://doi.org/10.5120/ijca2015905703
[30] Sharmah, D., Bora, K. C.,Alqahtani, A. S., Hakeem, T. R. (2024),Importance of Dynamic Load Balancing and Virtualization Role in Dynamic Load Balancing, *Software-Defined Network Frameworks Security Issues and Use Cases*, *CRC Press, Taylor & Francis Group*, 53-67, DOI: 10.1201/9781003432869
[31] Ullah, A. (2019). Artificial Bee Colony Algorithm used for Load Balancing in Cloud Computing: Review. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *8*(2), 156. https://doi.org/10.11591/ijai.v8.i2.pp156-167
[32] Younis, Y. A., Kifayat, K., & Merabti, M. (2015). A novel evaluation criterion to cloud based access control models. *2015 11th International Conference on Innovations in Information Technology (IIT)*, 68–73. https://doi.org/10.1109/INNOVATIONS.2015.7381517
[33] Zhao, L., Saif, M. B., Hawbani, A., Min, G., Peng, S., & Lin, N. (2021). A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET. *China Communications*, *18*(7), 103–116. https://doi.org/10.23919/JCC.2021.07.009
[34] Zhou,L., Varadharajan. V., Hitchens. M. (2013), Achieving Secure Role-based Access Control on Encrypted Data in Cloud Storage. *IEEE Transactions on Information Forensics and Security*, 8(12):1947-1960, DOI:10.1109/TIFS.2013.2286456

[35] Rekha, S., & Kalaiselvi, C. (2021). Secure And Energy Aware Task Scheduling in Cloud Using Deep Learning and Cryptographic Techniques. *ICTACT Journal on Communication Technology*, *12*(02).
[36] Gupta, A., Siddiqui, S. T., Alam, S., & Shuaib, M. (2019). *Cloud Computing Security using Blockchain*. *6*(6).
[37] Murthy, Ch. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access*, *8*, 205190–205205. https://doi.org/10.1109/ACCESS.2020.3036812
[38] Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain Meets Cloud Computing: A Survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 2009–2030. https://doi.org/10.1109/COMST.2020.2989392
[39] Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2020). Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System. *IEEE Transactions on Industrial Informatics*, *16*(3), 1972–1983. https://doi.org/10.1109/TII.2019.2938001.
[40] Walaa Hashem, Heba Nashaat, and Rawya Rizk. (2017). Honey Bee Based Load Balancing in Cloud Computing. *KSII Transactions on Internet and Information Systems*, *11*(12). https://doi.org/10.3837/tiis.2017.12.001
[41] Ebadifard, F., Babamir, S. M., & Barani, S. (2020). A Dynamic Task Scheduling Algorithm Improved by Load Balancing in Cloud Computing. *2020 6th International Conference on Web Research (ICWR)*, 177–183. https://doi.org/10.1109/ICWR49608.2020.9122287
[42] Kalaivani, S., & Gopinath, G. (2020). Modified Bee Colony with Bacterial Foraging Optimization Based Hybrid Feature Selection Technique for Intrusion Detection System Classifier Model. *ICTACT Journal on Soft Computing*, *10*(04).
[43] Sarmah, S. S. (2019). Application of Block chain in Cloud Computing. *International Journal of Innovative Technology and Exploring Engineering*, *8*(12), 4698–4704. https://doi.org/10.35940/ijitee.L3585.1081219.