GrenzeInternational Journal of Engineering and Technology, June Issue

Cloud-Based Resource Distribution Using a Blockchain Approach

Radha T. Deoghare[1] and Mrs. Sapana A. Kolambe[2]
[1-2]Department of Information Technology,
PCCOE, Assistant Professor
Email: radha.deoghare@pccoepune.org, sapana.kolambe@pccoepune.org

***Abstract*—It is difficult to divvy up and keep track of resources amongst several entities. This is particularly true for complex and ever-changing systems, such as those seen in cloud computing, software engineering, and the Internet of Things (IoT). Providing safe access control is crucial to the success of such a system. In particular, the safe, adaptable, and granular handover of privileges from one entity to another. Here, we introduce a blockchain-based multi-organizational delegation system. In our system, smart contracts on the blockchain specify how the consortium's member organizations interact and how their shared resources are divided up.**

***Index Terms*— Resource Allocation, IoT, blockchain, Security.**

I. Introduction

Cloud computing is a method of remote, scalable resource provisioning that uses utility-based computing models. Parallel computing, grid computing, and distributed computing are all realized on the cloud [1]. Users can access a shared pool of resources in the cloud and use them as needed using an "on-demand" model [2]. Users can use cloud services whenever and wherever they like thanks to the cloud's powerful computing capabilities and massive storage capacity. IT assets such as databases, servers, communication devices, networks, and software systems are housed in a cloud data Centre. As more customers use the cloud, more servers or other gear will be needed to meet demand. Thus, the creation of more physical nodes will result in an increase in data center power usage. Today, 2% of all electricity used in the globe goes toward powering data centers. By the year 2030, projections show it will have reached 8%. Data centers have three major power users: servers, data Centre networks, and cooling systems. The network uses 10% to 25% of the energy, the cooling systems use 15%-30%, and the servers use 40%-55%, respectively [3].
Computing resources such as RAM, CPU, Network, and Storage are provided by IaaS (Infrastructure as a Service) and their use is typically governed by Service Level Agreements (SLAs) (Service Level Agreement). Use of resources is also influencing energy requirements. One of the causes of the data center's energy insufficiency is the inefficient use of its resources [4]. Even at 10% CPU utilization, the workload is light enough to cause the energy consumption to be more than 50% of the maximum. This is where IaaS's virtualization techniques come into play, which helps maximize the usefulness of any given cloud's assets [5]. Due to the shared resources made available by virtualization, VMs can take the place of PMs in processing user requests. Separating virtual machines (VMs), moving VMs, and merging VMs are all examples of what may be done using virtualization. VM migration is a method for moving active virtual machines from one physical host to

Grenze ID: 01.GIJET.9.2.306

another. Consolidating virtual machines (VMs) that were previously spread across multiple hosts into a smaller number of hosts saves power by either shutting down the first host or placing it into hibernation [6]. One way to run virtual machines is through a method called Virtual Machine Placement (VMP). A powerful VMP method is required to improve energy productivity and maximize use of available resources [7]. When it comes to optimization, the VMP problem is NP-hard [8].

In this study, we combine the power of the genetic algorithm (GA) with that of the random forest (RF) algorithm to create a novel and effective hybrid VMP strategy. Our goal is to keep the load spread across a number of physical computers while decreasing the data center's energy consumption. One of the most important factors in determining how effective the proposed solution is is how well it makes use of the hardware's available resources. The goal of this study is to reduce the execution time, average start time, and average finish time required by the cloud, as well as the waiting time and request completion time, respectively. The proposed approach also aims to speed up the iterative metaheuristic algorithms like GA, ACO, PSO, and others by cutting down on the time it takes to identify the best solution. The goal of the model is to use the best possible optimal solution to train a machine learning model, which can then be used to forecast the optimal solution in a constant amount of time, bypassing the need for evolutionary processes to find the global best answer [9].

The genetic algorithm is one of the metaheuristic methods used to locate a truly optimal answer. First, using the mapping between virtual and physical machines as a training dataset, the GA creates an optimum schedule for resource allocation. The next step is to use the GA-created dataset to train the random forest algorithm, which then assigns virtual machines to physical machines based on the categorization it has made. With the GA-obtained data sample, the RF's classification accuracy may be evaluated.

A. Problem Statement

In this article, we take a look at the current state of blockchain-based cloud security and analyze its many benefits and drawbacks. The effectiveness of a smart contract can be measured in terms of its robustness, security, stability, and practicality. The model's capacity to generalize has proven superior. However, this paradigm needs to be implemented locally at each cloud data center. Attribute encryption using ciphertext has improved retrieval efficiency and validated the integrity of the data at rest. But the proposed model has poorer search efficiency. BIoTHR ensures the confidentiality of cloud data while providing advantageous pricing and accessibility. The model does not make use of low-power Internet of Things gadgets. As far as usability, safety, privacy, and reaction speed are concerned, EACMS ensures the best possible results in every category. When compared to traditional medical systems, this concept has proven to be far more effective. Contrarily, it necessitates a more capacious memory system. When it comes to delay and throughput, DBDH performs at its best, and it also offers top-notch security. However, this paradigm is vulnerable to attacks that happen in real-time. In terms of latency, throughput, and resources, the modified Merkle Tree data structure excels. Resource consumption, latency, transaction response time, and throughput are all analyzed to guarantee the proposed model performs well. However, as the system's user base grows, so does its latency. Safeguarding private health information in less time than conventional methods, the timestamped algorithm is a significant improvement over the alternatives. This methodology does not, however, process or provide privacy for the little data bits. Smart contracts have been shown to increase data integrity and privacy by providing security and access control. For smart contracts that rely heavily on locally stored data, another approach is necessary. Researchers might use this analysis as support for proposing a novel blockchain-based approach for cloud data security.

B. Contributions

The growing popularity of blockchain technology offers a potential answer to the cloud computing resource management issue. It ensures users' data security in the cloud computing environment [14] while also cryptographically guaranteeing the irreversible and unforgeable features of the data. Additional identifying attributes of the alliance chain members are shared by cloud service providers and cloud computing environment customers.

In order to better integrate the blockchain system into the cloud computing network architecture, the fundamental objective of this work is to propose a cloud computing resource contribution model based on an alliance chain. A solution to the cloud computing resource management challenge is found in the application of blockchain's incentive and disincentive mechanisms to encourage nodes to actively contribute to the pool of available computing resources. By recording the resource-contribution behavior of cloud nodes and the degree of satisfaction upon task completion in blockchain form, an uncontrollable assessment system is created, which can address issues like malicious poor reviews and brush in real-world applications.

II. Research Methodology

We propose Automatic software cloud resource allocation utilizing permission block, a policy-based and autonomic middleware that enables self-adaptiveness for data management in clouds, to address these issues. Therefore, the proposal combines three highly sought-after elements: Software cloud resource allocation is monitored in real-time, and the collected and aggregated metrics (such as write latency, read latency, uptime, free memory, etc.) Are secured on a blockchain for optimal privacy and integrity. Data management decisions are made based on what cloud service is best suited to help you satisfy your service level agreements (slas), and your data is transmitted securely. Moreover (iii), the cloud storage setup is automatically re-configured (based on the simple, reusable, and extendable configuration policies), meaning that a human operator is no longer needed to monitor and manually re-configure the cloud storage setup's security.

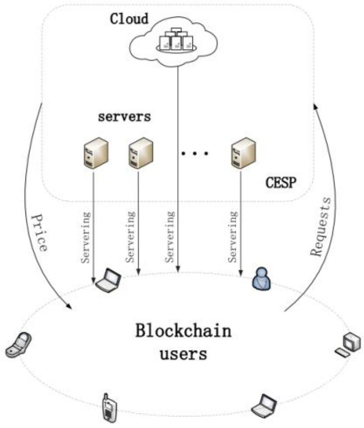

Figure 01: System model

III. Working

Each node in a distributed ledger maintains a chain of records called "blockchain." The Bitcoin network's consensus issue was proposed by S. Nakamoto. Each block in the blockchain, with the exception of the initial block, includes the hash of the prior block, as illustrated in Figure 2. (Genesis block). The former block is always produced ahead of the latter, and each block contains transactions, which are logs of acts taken on the blockchain, such as the transfer of assets. Figure 02 further elucidates the technique by which a blockchain is created. As shown in the diagram, step one of a transaction involving Node0 involves a user signing it with his private key. As a result, the digital signature improves security and data integrity, and the transaction can be tracked using the user's public key. Afterward, Node0's immediate neighbor receives the transaction broadcast (i.e., Node1 and Node2).

Node1 and Node2 ensure the broadcast transaction follows the transaction protocol before broadcasting it to Nodes3 and 4. If the transaction does not follow the protocol, it will be dropped.

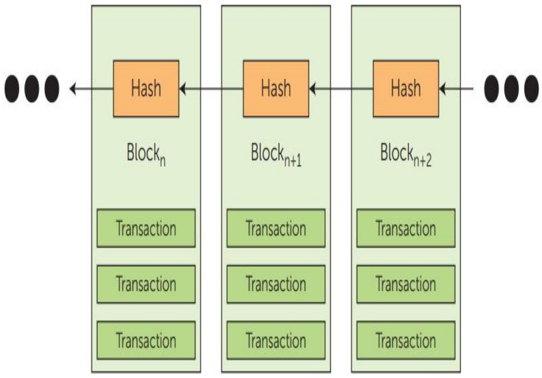

Figure 02: A blockchain network

Each network should make it clear to all participants what kind of protocol will be used for transactions before the blockchain is even created. Transaction protocol's primary goal is to maintain network order in the blockchain.

IV. Conclusion

This paper initially examines the privacy and security concerns surrounding edge computing-enabled IoT, before moving on to describe the features of blockchains that make them ideal for use in IoT applications. It was suggested to use a common framework for all Internet of Things (IoT) use cases that involve blockchain technology and edge computing. The entire process of a transaction was laid out in minute detail under the proposed framework. Additionally, the edge computing resources allocation problem was addressed by developing a smart contract in a private blockchain network that utilized the cutting-edge reinforcement learning, Asynchronous Advantage Actor-Critic algorithm. In particular, the efficiency of the suggested method is improved over the state-of-the-art edge computing resource allocation techniques by catering to various service users and differentiating between their Quality of Service (QoS) needs. That's an example of how AI and blockchains can work together. The simulation results were presented to prove the efficiency of the proposed resource allocation system for edge computing. Joint optimization of blockchain settings and edge computing resource allocation is something we plan to investigate more in future work.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the internet of things using big data analytics," Computer Networks, vol. 101, pp. 63–80, 2016.

[3] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, "Networking integrated cloud-edge-end in iot: A blockchain-assisted collective qlearning approach," IEEE Internet of Things Journal, 2020.

[4] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchainbased software-defined industrial internet of things: A dueling deep q-learning approach," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4627–4639, 2018.

[5] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, "Edge-centric computing: Vision and challenges," ACM SIGCOMM Computer Communication Review, vol. 45, no. 5, pp. 37–42, 2015.

[6] J. Du, L. Zhao, J. Feng, and X. Chu, "Computation offloading and resource allocation in mixed fog/cloud computing systems with min-max fairness guarantee," IEEE Transactions on Communications, vol. 66, no. 4, pp. 1594–1608, 2018.

[7] S. Shen, Y. Han, X. Wang, and Y. Wang, "Computation offloading with multiple agents in edge-computing–supported iot," ACM Transactions on Sensor Networks (TOSN), vol. 16, no. 1, pp. 1–27, 2019.

[8] X. Wang, Y. Han, V. C. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 869–904, 2020.

[9] X. Wang, C. Wang, X. Li, V. C. Leung, and T. Taleb, "Federated deep reinforcement learning for internet of things with decentralized cooperative edge caching," IEEE Internet of Things Journal, 2020.