CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-6, Issue-2; DOI: 10.46860/cgcijctr.2024.06.10.381

Resource Allocation and Security Threat in Cloud Computing: A Survey

Neha Sharma[1]*, Lakshay Kumar[1], Namrata Dwivedi[1], Ashpinder Kaur[2], Gagandeep Kaur[1]
[1]CGC-College of Engineering
[2]Chandigarh Engineering College
*Email Id: neha.4815@cgc.edu.in

Abstract: Cloud computing is a cutting-edge technology with enormous commercial and enterprise potential. Apps and related data can be accessed from any location thanks to clouds. Companies can drastically lower the cost of their infrastructure by renting resources from the cloud for storage and other processing needs. They can also use pay-as-you-go application access available to the entire firm. Therefore, obtaining licenses for specific products is not necessary. However, allocating resources as efficiently as possible is one of the main challenges in cloud computing. Because the model is unique, resource allocation is done to lower its expenses. Meeting application and customer requirements and consumer needs presents additional issues in resource allocation. This study provides a detailed discussion of several resource allocation systems, security threats, and the difficulties they face. This work is anticipated to help researchers and cloud users overcome obstacles.

Keywords *- Resource Allocation, Cloud Computing, Cloud Models, Security threats, and Algorithms.*

I. INTRODUCTION

Cloud computing is storing, managing, and processing data instead of a local server or your home computer using a network of servers located online. Cloud provides computing services like servers, storage, databases, networking, software, analytics, intelligence, and many more[1]. The famous services that are provided by the cloud are Amazon Web Services, Google Cloud Platform, and Microsoft Azure. Cloud computing makes transferring data worldwide much easier just with an internet connection. Examples of Cloud Computing are Dropbox, Facebook, and Gmail [2]. Cloud computing means that you can exchange information and have access to a large number of resources. All users are required to pay for the services they use. The company provides users of online applications with on-demand services. Backup and restore of the data are not an issue. The essential cloud characteristics are On-demand self-service, universal network access, resource pooling, resilient elasticity, and measured service. Reducing operational costs is a goal of cloud computing, it improves the time to process data and reduces computing. The power requirements for small devices, enhance security and improve efficiency. In addition, it increases the stability of the system. Potential changes in the system, improving fault tolerance, increasing multiple data processing speeds, reducing costs of technology, software, and maintenance overheads: rationalizing energy and saving disk space[3].

1.1 TYPES OF CLOUD

Cloud computing is like having a magical computer that you can use whenever you want and make it as big or small as you need. It is super cool because of cloud service providers. Cloud computing is like having a magical computer that you can use whenever you want and make it as big or small as you need. It's super cool because cloud service providers can start with just a little bit of stuff and then add more if they need it, without having to buy a bunch of new computers[4].

1.1.1 Cloud Deployment Models

There are four different types of cloud computing: private, public, community, and hybrid clouds [4],[5].

a) Public cloud:-Public clouds are like big playgrounds that anyone can use. They are created by companies like Amazon AWS, Microsoft, and Google, who build and care for all the cool stuff in the playground. You can access these playgrounds through the Internet. The only downside is that you don't get to choose where the playground is located, and you can't see or control what's happening behind the scenes. But they, at least you get to play[5].

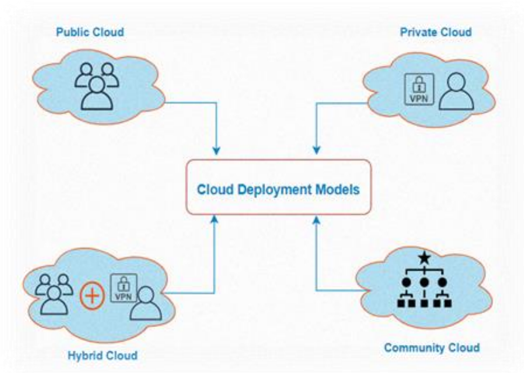

Fig 1. Cloud Computing Deployment Models.

b) Private cloud private cloud is like a secret hideout where companies keep all their important information safe. It's kind of like having your own personal storage space, but only people who work for the company can access it. Even though other companies might help take care of the private cloud, it's always kept in the same place as the company's office. This way, only the right people can get in and make sure everything is authorized and secure[5].

c) Hybrid Cloud:-Hybrid clouds are like a special kind of cloud computing that combines different types of clouds. It's like when you mix different flavors of ice cream to make a new yummy flavor! In a hybrid cloud, you can have a mix of private, public, or community clouds all working together, but they still stay separate. It's like having different pieces of a puzzle that fit together perfectly. Hybrid clouds are super cool

CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-6, Issue-2; DOI: 10.46860/cgcijctr.2024.06.10.381

because they can go beyond limits and connect different parts[5].

d) Community Cloud:-Hosting stuff on the internet called "community cloud." It's like a big party where lots of organizations, like banks and trading firms, come together and share the setup. They all chip in and help each other out, making it easier and cheaper for everyone. It's like having a big group project where everyone gets to benefit from each other's work. So instead of each organization doing their own thing, they create a cloud they can all use[5].

1.1.2 Cloud Service Models

Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are the three core models that make up cloud computing[6].

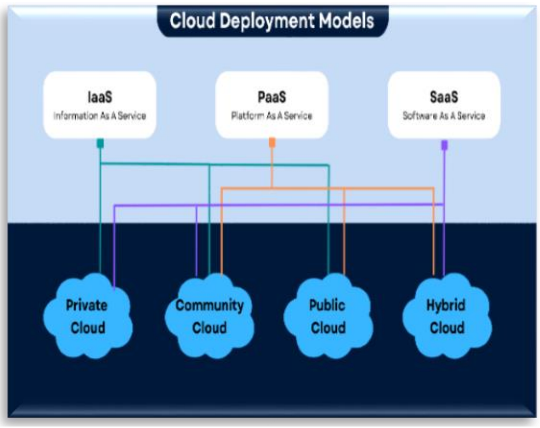

Fig 2. Cloud Deployment Model[1],[6].

a) IAAS (Infrastructure as Service)- IaaS stands for "Infrastructure as a Service". This is the ultimate service method of cloud stuff where you can get all the important things you need. It's got virtual servers, networks, operating systems, and storage drives. It's super flexible, reliable, and can grow with you[6].

b) SAAS (Software as a Service) -SaaS is short for "Software as a Service". It's like having a cool online store where you can find all sorts of software. Instead of buying and installing software on your computer, you can use it directly from the internet. This is possible because a company creates the software and lets you access it through the cloud. So, you don't have to worry about downloading or updating anything, just hop online and start using the software right away[6].

c) PAAS (Platform as a Service):- PaaS is a type of cloud service that gives you a special platform to create, run, and take care of your apps. You don't have to worry about all the boring stuff like building and keeping up with the infrastructure. It's like having your magical playground where you can make awesome things without any hassle**!**[6]**.**

II. RESOURCE ALLOCATION

The primary objective of resource allocation is to identify an efficient distribution of fog assets among various activities, applications, and services. This aims to maximize or minimize conflicting goals while adhering to imposed constraints. In this section, we will discuss various resource allocation algorithms**.** Resource allocation in cloud computing is a critical process that involves assigning available resources to cloud applications, meeting consumer requirements, and effectively managing software components. By implementing efficient resource allocation strategies, cloud providers can enhance the performance, scalability, and reliability of their services, ultimately benefiting both consumers and providers alike. Resource allocation plays a vital role in maintaining the overall stability and reliability of cloud computing systems. By efficiently distributing resources, providers can prevent bottlenecks and ensure a smooth and uninterrupted user experience[7].

2.1 Types of Resources:

The various types of resources offered in resource allocation in cloud computing are Computational resources, Network resources, and Storage resources.

a) Computational resources refer to the resources utilized for data processing and executing various tasks within robotic applications. These resources encompass cloud instances, local robots, and edge nodes, which serve as the fundamental components of computational infrastructure[8].

b) Network resources refer to the physical and logical components within a network that facilitate connectivity, communication, and data transmission. The allocation of network resources has been extensively studied in the literature, specifically in references [9]. In multi-agent cloud robotic systems, a mesh orchestration of networking nodes enables the sharing of network resources. To ensure a consistent data flow across the shared network, network resources such as bandwidth, network slices, and power transmitters are allocated.

c) Storage plays a crucial role in the realm of robotics, serving as a means to store data, facilitate information sharing, and enable collective learning during the execution of various robotic applications. In the context of multi-agent cloud robotics, storage facilities are provided by a combination of cloud-based data servers, frog lets, and the built-in memory of local robots. However, it is worth noting that while the majority of existing research in multi-agent cloud robotics emphasizes computational and network resource allocation, only a limited number of studies, such as delve into the allocation of storage resources[10]**.**

Advantages of Resource Allocation

Few advantages of resource allocation in fog computing are discussed below [11],[12],[13].

a) The primary advantage of resource allocation is that users do not need to install any software or hardware to access, develop, and host applications over the Internet.

b) Another significant benefit is the absence of limitations regarding location and medium. Our applications and data can be accessed from anywhere in the world, on any system.

c) Users are relieved from the financial burden of investing in hardware and software systems.

d) Cloud providers can share their resources over the internet during times of resource scarcity.

Limitation of Resource Allocation:

While cloud computing offers numerous benefits, it is important to be aware of its limitations. These limitations include the lack of control over resources, challenges in data migration, security vulnerabilities, compatibility issues with peripheral devices, and the need for

ISSN: 2582-0486 (online) Vol.-6, Issue-2; DOI: 10.46860/cgcijctr.2024.06.10.381

specialized knowledge in resource management. By understanding these limitations, users can make informed decisions and mitigate potential risks when utilizing cloud services[11],[12][14],[15],[37].

a) One limitation of using remote servers for resource rental is that users do not have control over their resources. This lack of control can restrict their ability to customize or optimize their resources to meet their specific needs.
b) Another limitation is the migration problem that arises when users want to switch to a different provider for better data storage. Transferring large amounts of data from one provider to another can be a complex and time-consuming process.
c) The use of public cloud services also poses a security risk, as clients' data can be vulnerable to hacking or phishing attacks. The interconnected nature of cloud servers makes it easier for malware to spread, increasing the potential for data breaches.
d) Additionally, peripheral devices such as printers or scanners may not be compatible with cloud services. Many of these devices require local software installation, which may not be supported in a cloud environment. However, networked peripherals generally have fewer compatibility issues.
e) Finally, effectively allocating and managing resources in the cloud requires a deeper level of knowledge and expertise. Users must rely on the cloud service provider to understand the intricacies of the cloud system, making it essential to have a comprehensive understanding of the provider's offerings.

2. Algorithms For Resource Allocation

The main algorithms for resource allocation in cloud computing include:

a) Round-Robin: It cyclically distributes resources, ensuring equal allocation to users or tasks. This approach cyclically assigns resources to ensure fairness by providing access, to all users. It works well in environments where tasks have resource requirements. However, it may not efficiently handle varying workloads. For example, if certain tasks require resources or have priorities Round Robin might not effectively optimize resource utilization [16].
b) First Come First Serve: It allocates resources based on the order of arrival, giving priority to tasks that arrive first. Resources are allocated based on the order of arrival. It is intuitive and easy to implement. Do not prioritize tasks based on their execution time or importance. Longer tasks may delay ones, which can impact the overall efficiency and responsiveness of the system [17].
c) Proportional Share Scheduling: This algorithm allocates resources proportionally based on assigned weights to users or tasks. This approach involves the allocation of resources based on assigned weights or shares to users or tasks. It ensures fairness by granting resources in proportion to these weights, thereby maintaining a balanced allocation and preventing any one user from dominating resources [18].
d) Priority-Based Scheduling: Assigns priorities to tasks or users, allowing higher-priority tasks to be allocated resources first. Tasks or users are assigned priorities that allow high-priority tasks to obtain resources before others. By assigning priorities to tasks or users, high-priority tasks are given precedence in receiving resources over lower-priority ones. Effective priority management is crucial to maintain fairness among tasks and ensure critical operations are handled promptly. It is extremely important to handle mission operations but it is necessary to effectively manage priorities to ensure fairness among all tasks [19].
e) Min-Min and Max-Min: Min-Min minimizes the completion time of the smallest task, while Max-Min maximizes the minimum completion time used in task scheduling. The Min-Min algorithm aims to minimize the completion time of the smallest task, thereby achieving quicker overall completion. On the other hand, the Max-Min algorithm maximizes the minimum completion time, enhancing fairness in task scheduling by preventing resource monopolization [20].
f) Ant Colony Optimization: Models resource allocation based on the foraging behavior of ants, optimizing path for efficiency. Inspired by the foraging behavior of ants, ACO models resource allocation for efficiency optimization. It employs decentralized algorithms to identify optimal resource paths or distributions in cloud environments, thereby enhancing resource utilization [12].
g) Genetic Algorithm: Evolves solution for resource allocation using genetic operators like mutation and crossover. These algorithms evolve solutions for resource allocation using genetic operators such as mutation and crossover. They explore potential resource allocation solutions and adapt over iterations to find optimal or near-optimal allocations [21].
h) Auction Based: Users bid for resources, and resources are allocated to the highest bidder, promoting efficient allocation. In this approach, users bid for resources, and the resources are allocated to the highest bidder. This promotes efficient allocation, ensuring that resources are assigned based on their perceived value to the bidder, thereby enhancing resource utilization[22].
i) QoS Based Scheduling: Considers quality of service requirements to allocate resources and meet specified performance metrics. This approach takes into consideration the requirements for quality of service in order to allocate resources effectively, ensuring that specified performance metrics or Service Level Agreements (SLAs) are met. By doing so, it guarantees that resources are allocated in a manner that aligns with defined service standards[23].
j) DVFS: Adjusts the voltage and frequency of processors dynamically based on workload to save energy. DVFS is an optimization technique that dynamically adjusts the voltage and frequency of processors based on the demands of the workload. The primary objective of this technique is to conserve energy while efficiently meeting computational demands [24].
k) Game Theory- Based Algorithm: Models resource allocation as a game when users compete for resources,

CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-6, Issue-2; DOI: 10.46860/cgcijctr.2024.06.10.381

seeking Nash equilibrium. These algorithms model resource allocation as a competitive game, where users compete for limited resources. The aim is to find equilibrium solutions, such as Nash equilibrium, which ensure fairness and optimize the distribution of resources among users[25].

l) Deadline-Based Scheduling: Allocates resources based on task deadline, ensuring that critical tasks meet their specified completion times. This scheduling approach allocates resources based on task deadlines, prioritizing critical tasks to ensure they meet specified completion times. By prioritizing tasks according to their deadlines, this method maintains adherence to time-sensitive operations. This scheduling approach prioritizes the allocation of resources based on task deadlines, ensuring that critical tasks meet specified completion [26].

Resource allocation in cloud computing is crucial for maximizing efficiency and cost-effectiveness. It involves assigning virtual machines, storage, and network bandwidth based on specific application and user requirements. Proper allocation leads to better performance, scalability, and cost savings, while poor allocation can result in underutilized resources and productivity issues. To optimize allocation, factors like workload analysis, elasticity, and automation should be considered to accommodate changing demands. Ongoing monitoring and optimization are essential to identify areas for improvement and ensure efficient allocation. Ultimately, resource allocation is a fundamental aspect of cloud computing that enables businesses to achieve optimal outcomes in a competitive environment

III. SECURITY THREATS

a) Data Breaches and Unauthorized Access: Data breaches occur when hackers gain unauthorized access to a company's cloud network and proceed to view, copy, and transfer data without permission. These breaches involve the unauthorized copying, communication, theft, alteration, or use of sensitive, protected, or confidential information. Data breaches can also be referred to as data spills, information leaks, information leakage, or unintended information disclosure. Data leaks are particularly concerning for organizations because cloud service providers store large amounts of data from multiple clients on shared infrastructure[19].

b) Data Loss and Recovery: Data loss is a critical concern faced by cloud service providers, stemming from a variety of factors such as hardware or software glitches, natural calamities, or unforeseen events. The unpredictable nature of these issues necessitates the implementation of robust disaster recovery and backup protocols. Consequently, certain institutions exhibit reluctance to adopt cloud-based data delivery, citing Apprehensions regarding its security when interacting with other systems [27].

c) Malware and Security Threats: Malware and hacking threats pose significant risks to cloud service providers. Malware refers to malicious software that grants attackers control over targeted machines. It includes viruses, worms, Trojans, ransomware, and spyware. Once infected, cloud systems become vulnerable to unauthorized access and control by cybercriminals. The consequences of malware attacks can be severe, compromising data integrity, confidentiality, and the trust of users. To mitigate these risks, cloud service providers must implement robust security measures such as advanced threat detection systems, regular software updates, security audits, and user education on safe browsing habits and strong passwords. By understanding malware types and implementing stringent security measures, cloud service providers can protect valuable data and safeguard their systems[20].

d) Insider threats and privileged user Abuse: While the percentage of these threats may not be high, they still pose a significant risk. Privileged users have the power to disrupt cloud services by improperly configuring vital components, disabling virtual machines, or bypassing security measures. These actions can result in service interruptions, financial losses, and damage to both the reputation of cloud service providers and their customers. In cases where unauthorized individuals gain access to a client's private information, the client must create a new account to prevent further data leakage. Overall, insider threats and privileged user abuse are major concerns in cloud computing. Nefarious actors with elevated privileges can wreak havoc on the system, leading to various detrimental consequences for all involved [28].

e) Denial of Service (**DoS) attacks:** Denial of Service (DoS) attacks are intentional actions taken by attackers to disrupt or impair cloud services. This is done by overwhelming the target web server with a large number of HTTP requests or by exploiting vulnerabilities. Some DoS attacks specifically target weaknesses in cloud applications or services. For example, attackers may exploit flaws in an application's input validation system, causing it to crash or use up excessive resources[29].

- Recognize characters on the license plate
- Analyze traffic density
- Authentication and Identity: Authentication of users and even of communicating systems is performed using various methods, with cryptography being the most common. User authentication can occur through passwords known individually, security tokens, or measurable quantities like fingerprints. However, traditional identity approaches face challenges in a cloud environment, particularly wheenterprise utilizes multiple cloud service providers (CSPs). Synchronizing identity information with the enterprise becomes unsalable in such cases. Additionally, traditional identity approaches encounter issues when migrating infrastructure to a cloud-based solution [30].

Fig3. Security threat [19].

ISSN: 2582-0486 (online) Vol.-6, Issue-2; DOI: 10.46860/cgcijctr.2024.06.10.381

Table 1. Comparative Analysis of Various Algorithms for Resource Allocation in Cloud Computing

Algorithm	Key Features	Use Cases/ Scenarios	Advantages	Disadvantages
Round Robin[16]	Equal distribution, simple implementation.	General-purpose, simple workloads.	Fairness, simplicity.	May not adapt well to varying task requirements.
FCFS(First Come First Serve)[17]	Allocation of resources based on task arrival order.	Non-critical, non-pre-emptive scenarios.	Easy to implement.	This can lead to inefficient resource utilization.
Proportional Share Scheduling[18]	Allocates resources based on proportional weights.	Environments with diverse user priorities.	Fairness allows priority adjustments.	Complexity increases with the number of users.
Priority-based Scheduling[19]	Assign priorities to tasks or users.	Real-time systems, critical task scenarios.	Priority management.	Lower-priority tasks may suffer starvation.
Min-Min and Max-Min Algorithms[20]	Optimizes task completion time by minimizing or maximizing the smallest task's time.	Task scheduling for make-span optimizing.	Make-span optimization.	Sensitive to task size and system conditions.
Ant Colony Optimization[12]	Models resource allocation based on ant foraging behavior.	Load balancing, optimizing network traffic.	Adaptive and effective for dynamic environments.	Computational overhead may be significant.
Genetic Algorithms[21]	Evolves solutions for resource allocation using genetic operators.	Complex and dynamic environments, optimization problems.	Adaptability, handles diverse problem spaces.	May require tuning of genetic operators.
Auction-Based Algorithms[22]	Users bid for resources, and the highest bidder gets the allocation.	Efficient resource allocation, market-driven scenario.	Efficient, allows users to express resource value.	Complexity in managing bidding processes.
QoS-based Scheduling[23]	Considers quality of service requirements for resource allocation.	Applications with specific metrics.	Meets performance criteria.	Complexity in defining and managing QoS metrics.
Dynamic Voltage and Frequency Scaling(DVFS)[24]	Adjusts processor voltage and frequency based on workload.	Energy efficient computing, dynamic workloads.	Energy savings adapts to varying workloads.	May impact performance under certain conditions.
Game Theory-based Algorithms[25]	Models resource allocation as a game, seeking Nash equilibrium.	Competitive scenarios, distributed systems.	Encourages fairness, Nash Equilibrium.	Complexity in modeling and analyzing game scenarios.
Deadline-based Scheduling[26]	Allocates resources based on task deadline.	Real time systems, critical tasks with time constraints.	Meets deadlines, suitable for time-sensitive applications.	Requires accurate estimation of task execution times and deadlines.

2.1.1 Techniques to overcome security challenges in the cloud

a) Information Integrity and Privacy: Cloud computing offers a wealth of information and resources to legitimate users. However, it also opens the door for potential threats from malicious attackers [2]. To address the issue of information integrity, establishing mutual trust between the provider and the user is crucial. Additionally, implementing robust authentication, authorization, and accounting controls can ensure that accessing information requires passing through multiple levels of verification, thus guaranteeing authorized use of resources [2]. To further enhance security, it is essential to incorporate secure access mechanisms such as RSA certificates and SSH-based tunnels[32].

b) Availability of Information (SLA): The lack of availability of information or data poses a significant challenge in the realm of cloud computing services. To address this issue, a Service Level Agreement (SLA) is employed to determine whether network resources are accessible to users. The SLA serves as a trust agreement between the consumer and the provider [2]. One approach to ensuring resource availability is to establish backup plans for both local resources and critical information. This allows users to access information about the resources even when they are temporarily unavailable[33].

c) Secure Information Management: Secure Information Management is a vital technique in ensuring the security of data. It involves the consolidation of data into a central repository, which is then monitored by agents running on various systems. These agents send the collected information to a server known as the "Security Console." The Security Console is managed by an administrator, who is responsible for reviewing the information and taking appropriate actions in response to any alerts. As the number of cloud users and the complexity of their dependency stack increases, so does the need for robust cloud security mechanisms. Secure Information Management is often referred to as Log Management, as it involves the management and analysis of logs generated by various systems [34].

d) Malware Injection Attack Solution: This solution involves the creation of multiple client virtual machines, which are then stored in a centralized storage system. It utilizes the File Allocation Table (FAT) that consists of virtual operating systems. The FAT table contains the applications that are executed by the clients. The management and scheduling of all instances are handled by the Hypervisor. Additionally, the Interrupt Descriptor Table (IDT) is utilized for integrity checking purpose.

e) Flooding Attack Solution: In the cloud computing environment, the servers are organized into fleets. Each fleet is dedicated to specific tasks, such as system type requests, memory management, and core computation. These servers within a fleet can communicate with each other seamlessly. When a server becomes overloaded, a new server is introduced to replace it. A name server keeps track of the current states of all servers and updates their destinations and states accordingly. This ensures smooth operation and efficient resource allocation[35].

IV. CONCLUSION

In this paper, we have conducted a comprehensive review of cloud computing technology, delving into various services, models, architecture, resource allocation, and associated algorithms. Additionally, we have explored the security challenges prevalent in the cloud computing environment and proposed measures to overcome them. While we have covered a range of crucial aspects, there remain several other significant areas that warrant attention. These include resource management, data backup and security, restoring procedures, storage management, and more. In our future endeavors, we intend to focus on these aspects, aiming to provide a deeper understanding and analysis. Furthermore, we plan to delve into specific cloud computing algorithms and endeavor to implement real-world scenarios utilizing publicly available rich datasets. By expanding our research in these directions, we aim to contribute to the advancement of cloud computing technology and its practical applications.

REFERENCES

[1] N. Sharma and C. Prabha, "Computing Paradigms: An Overview," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*, 2021, pp. 1–6.

[2] D. C. Marinescu, *Cloud computing: theory and practice*. Morgan Kaufmann, 2022.

[3] W. W. Mulat, S. K. Mohapatra, R. Sathpathy, and S. K. Dhal, "Improving Throttled Load Balancing Algorithm in Cloud Computing," in *Proceedings of International Joint Conference on Advances in Computational Intelligence: IJCACI 2021*, 2022, pp. 369–377.

[4] B. A. Alenizi, M. Humayun, and N. Z. Jhanjhi, "Security and privacy issues in cloud computing," in *Journal of Physics: Conference Series*, 2021, p. 12038.

[5] H. B. Patel and N. Kansara, "Cloud Computing Deployment Models: A Comparative Study," *Int. J. Innov. Res. Comput. Sci. \& Technol.*, 2021.

[6] R. Nazir, Z. Ahmed, Z. Ahmad, N. N. Shaikh, A. A. Laghari, and K. Kumar, "Cloud computing applications: a review," *EAI Endorsed Trans. Cloud Syst.*, vol. 6, no. 17, pp. e5--e5, 2020.

[7] N. Sharma, C. Prabha, and S. B. Goyal, "Resource allocation in FC environment: A review," in *AIP Conference Proceedings*, 2022.

[8] J. Bachiega Jr, B. Costa, L. R. Carvalho, M. J. F. Rosa, and A. Araujo, "Computational Resource Allocation in Fog Computing: A Comprehensive Survey," *ACM Comput. Surv.*, vol. 55, no. 14s, pp. 1–31, 2023.

[9] I. Martinez, A. S. Hafid, and A. Jarray, "Design, resource management, and evaluation of fog computing systems: a survey," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2494–2516, 2020.

[10] R. Rani, N. Kumar, M. Khurana, A. Kumar, and A. Barnawi, "Storage as a service in fog computing: A systematic review," *J. Syst. Archit.*, vol. 116, p. 102033, 2021.

[11] D. Alsadie, "Resource Management Strategies in Fog Computing Environment-A Comprehensive Review," *Int. J. Comput. Sci. \& Netw. Secur.*, vol. 22, no. 4, pp. 310–328, 2022.

[12] B. Jamil, H. Ijaz, M. Shojafar, K. Munir, and R. Buyya, "Resource allocation and task scheduling in fog computing and internet of everything environments: A taxonomy, review, and future directions," *ACM Comput. Surv.*, vol. 54, no. 11s, pp. 1–38, 2022.

[13] Himanshu and N. Mangla, "Analyzing Resource Allocation Methods in Fog Computing for Task Scehduling: A Study of Heuristic and Meta-Heuristic Approaches," *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, Bengaluru, India, 2023, pp. 1258-1264.

[14] M. Z. Hasan, M. Z. Hussain, Z. Mubarak, A. A. Siddiqui, A. M. Qureshi and I. Ismail, "Data security and Integrity in Cloud Computing," *2023 International Conference for Advancement in Technology (ICONAT)*, Goa, India, 2023, pp. 1-5.

[15] M. S. Sofla, M. H. Kashani, E. Mahdipour, and R. F. Mirzaee, "Towards effective offloading mechanisms in fog computing," *Multimed. Tools Appl.*, vol. 81, no. 2, p. 1997, 2022.

[16] S. K. Medishetti, G. Swapna, K. Anusha, G. R. Karri and K. P, "GEWO: An Efficient Prioritised Task Scheduling in Cloud Fog Computing Environment," *2024 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, Chennai, India, 2024, pp. 1-8.

[17] L. Hamid, A. Jadoon, and H. Asghar, "Comparative analysis of task level heuristic scheduling algorithms in cloud computing," *J. Supercomput.*, vol. 78, no. 11, pp. 12931–12949, 2022.

[18] S. Son, G. Oh, and S. Ahn, "Low-overhead Proportional-share I/O Scheduler in Multi-queue Block Layer for NVMe SSDs," *J. Semicond. Technol. Sci.*, vol. 20, no. 6, pp. 491–498, 2020.

[19] H. Ben Alla, S. Ben Alla, A. Ezzati, and A. Touhafi, "A novel multiclass priority algorithm for task scheduling in cloud computing," *J. Supercomput.*, vol. 77, no. 10, pp. 11514–11555, 2021.

[20] I. Syed, "HAMM: A hybrid algorithm of Min-Min and Max-Min task scheduling algorithms in cloud computing," *Int. J. Recent Technol. Eng.*, vol. 9, pp. 209–218, 2020.

[21] S. Kodli and S. Terdal, "Hybrid Max-Min Genetic Algorithm for Load Balancing and Task Scheduling in Cloud Environment.," *Int. J. Intell. Eng. \& Syst.*, vol. 14, no. 1, 2021.

[22] M. Zade, S. D. Lumpp, P. Tzscheutschler, and U. Wagner, "Satisfying user preferences in community-based local energy markets—Auction-based clearing approaches," *Appl. Energy*, vol. 306, p. 118004, 2022.

[23] G. F. Da Silva, F. Brasileiro, R. Lopes, F. Morais, M. Carvalho, and D. Turull, "QoS-driven scheduling in the cloud," *J. Internet Serv. Appl.*, vol. 11, pp. 1–36, 2020.

[24] H. Ahmadvand, F. Foroutan, and M. Fathy, "DV-DVFS: merging data variety and DVFS technique to manage the energy consumption of big data processing," *J. Big Data*, vol. 8, pp. 1–16, 2021.

[25] S. Medya, T. Ma, A. Silva, and A. Singh, "A game theoretic approach for k-core minimization," in *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems*, 2020.

[26] S. C. Nayak, S. Parida, C. Tripathy, and P. K. Pattnaik, "An enhanced deadline constraint based task scheduling mechanism for cloud environment," *J. King Saud Univ. Inf. Sci.*, vol. 34, no. 2, pp. 282–294, 2022.

[27] Komal, Goel, G. and Kaur, M. (2021) 'Hybrid scheduling strategy in cloud computing based on optimization algorithms', *CGC International Journal of Contemporary Technology and Research*, 4(1), pp. 226–234.

[28] N. Pitropakis, C. Lyvas, and C. Lambrinoudakis, "The greater the power, the more dangerous the abuse: facing malicious insiders in the cloud," *arXiv Prepr. arXiv2206.09834*, 2022.

[29] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput. Sci. Rev.*, vol. 39, p. 100332, 2021.

[30] A. Alsirhani, M. Ezz, and A. M. Mostafa, "Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing.," *Comput. Syst. Sci. \& Eng.*, vol. 43, no. 3, 2022.

[31] T. Hidayat and R. Mahardiko, "A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing," *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 49–57, 2020.

[32] Y. S. Abdulsalam and M. Hedabou, "Decentralized data integrity scheme for preserving privacy in cloud computing," in *2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)*, 2021, pp. 607–612.

[33] Y. Mo and L. Xing, "Efficient Analysis of Resource Availability for Cloud Computing Systems to Reduce SLA Violations," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 6, pp. 3699–3710, 2021.

[34] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, "PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms," *IEEE Access*, vol. 10, pp. 85777–85791, 2022.

[35] T. Raja Sree and S. Mary Saira Bhanu, "Detection of HTTP flooding attacks in cloud using fuzzy bat clustering," *Neural Comput. Appl.*, vol. 32, pp. 9603–9619, 2020.

[36] Gupta, A.K. (no date) 'Securing Cloud using Biometric Cryptographic Techniques', *CGC International Journal of Contemporary Technology and Research*, 5(1), pp. 331–335,2022.

[37] Sharma, R.K. and Pal Singh Brar, T. (2020) 'Proposed upbeat digital forensic method for cloud computing impression', *CGC International Journal of Contemporary Technology and Research*, 2(2), pp. 90–95.