International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-12, Special Issue-1, March-2024
https://doi.org/10.55524/CSISTW.2024.12.1.6
Computing for Sustainable Innovation: Shaping Tomorrow's World (CSISTW-2024) on 16th-17th February, 2024
Organized by B.N. College of Engineering and Technology, Lucknow, India

A Survey Paper on Fault Tolerance in Cloud Computing Environment

Shreya Rai[1], RamPratap[2], and Shaba Irram[3]

[1]B.Tech Scholar, Department of IT, Babu Banarsi Das Northern India Institute of Technology, Uttar Pradesh, India
[2]Associate Professor, Department of IT, Babu Banarsi Das Northern India Institute of Technology, Uttar Pradesh, India
[3]Assistant Professor, Department of IT, Babu Banarsi Das Northern India Institute of Technology, Uttar Pradesh, India

Correspondence should be addressed to Shreya Rai: 2000560130050@bbdniit.ac.in

ABSTRACT- The capital cost of purchasing hardware, software and setting up and maintaining on-site data centers—including the server racks, round-the-clock electricity for power and cooling, and the IT professionals for managing the infrastructure—is eliminated by using cloud computing. Cloud computing allows IT to respond to business needs faster. If an application needs more resources or capacity, It can be rapidly and simply modified in the cloud. Another essential aspect of cloud computing is fault tolerance, which measures how well a system can continue to function in the face of mistakes or failures. This survey will help acknowledge the main fault tolerance issues and the loopholes in the traditional fault tolerance techniques that still need attention. This survey gives us insight into several methods that can be used to cater the challenges regarding fault tolerance.

KEYWORDS- Cloud Computing, Fault Tolerance, IaaS, PaaS, SaaS

I. INTRODUCTION

Instead of using local servers or personal devices to manage apps, cloud computing focuses on sharing computer resources. These are the three main categories of cloud computing services- Infrastructure-as-a-Service(IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). These services are offered on demand since they are given to end customers via the Internet. Cloud computing eliminates the need for hardware and software investments by enabling businesses and individuals to access apps, data and other resources from any Internet-connected device. Cloud computing provides On-Demand Self-Service, scalability, elasticity, pay-as-you-go pricing, high availability, security and automation. It is a sort of computing that keeps track of data and applications using the internet and centralized remote servers. With cloud computing, users can utilize any Internet-connected device to access files, programs and other digital resources. Instead of a local server or a personal computer, it uses a network of remote servers that are hosted on the Internet to store, manage and process data. Additionally, without the need to install or maintain complicated software, organizations can access their apps and data at anytime from anywhere [2]. There is always a chance that data is stored in the cloud will become compromised. Cloud computing presents an opportunity for service providers and users to benefit from the increased availability and reliability of systems[1]. However, the potential for service availability and reliability is limited by various issues. A cloud computing system's potential for a single point of failure is one problem. A system component known as a single point of failure is one that if it malfunctions puts the entire system at risk. Without proper redundancy, such a failure can cause an entire system to cease functioning. Fault tolerance is a system design approach that enables a system to continue functioning even when some of its components fail [4]. In order to provide fault tolerance in cloud computing systems, data must be saved in numerous copies across multiple servers and various approaches must be used to guarantee that in the event of a system failure, the data can still be retrieved from another server. Additionally, the survey document is divided into the following sections: A description of a cloud computing environment is given in Section II. The conventional fault tolerance strategies employed in distributed systems are elaborated in Section III and IV. The fault tolerance strategies now in use in the world of cloud computing are discussed in Section V. The final computation is done in Section VI.

CLOUD SERVICE DELIVERY MODELS (SaaS, PaaS, IaaS, XaaS)
CLOUD DEPLOYMENT MODELS (Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud)
CLOUD COMPUTING INFRASTRUCTURES (Virtualization, Storage, Network, Servers, Security, Management, Backup and Recovery services)

Figure 1: Insights of Cloud Computing

II. INSIGHTS OF CLOUD COMPUTING

Numerous research areas including distributed computing, grid computing and virtualization technologies have contributed to the evolution of cloud computing. In this part, we will discuss the various aspects of cloud computing.

A. Cloud Computing Infrastructures

The infrastructure for cloud computing consists of a number of virtualized hardware and software resources that are utilized to provide cloud services such as servers, storage, networking, software and other elements for delivering computing services through a network. Cloud computing infrastructure allows businesses to rapidly provision resources on demand and scale their operations up or down as needed. It provides an alternative to in-house IT resources and can reduce costs associated with hardware maintenance and IT staffing. Following is the infrastructure for cloud computing:

- ***Servers:***
  The physical equipment known as a server serves as a host for one or more virtual machines. A cloud server is a distant server that stores, controls and maintains data for other connected computers or devices.
- ***Virtualization:***
  Technology that abstracts away physical elements like networks and storage to make them available as logical resources. It lets several virtual machines (VMs) to run on a single physical server, which helps businesses to lower hardware costs, boost productivity and use less energy.
- ***Storage:***
  In the form of disk drives, Network Area Networks (NAN), Storage Area Networks (SAN), etc. are part of the cloud computing architecture that gives customers the ability to archive and back up data as well as store, manage and retrieve it online.
- ***Network:***
  It helps in providing interconnection between physical servers. It is responsible for providing secure, reliable and high-performance communication between servers.
- ***Management:***
  Cloud management provides tools and services that enable organizations to configure, administer and manage cloud resources as well as monitor usage and performance metrics.
- ***F Security:***
  Integrity, availability and privacy-promoting components.

B. Cloud Deployment Models

The different methods that cloud services can offer to clients are referred to as cloud deployment models. It enables companies to cut back on the price of purchasing, maintaining and upgrading hardware and software. It gives companies the option to easily and swiftly scale up or down as their needs change. Cloud deployment models gives businesses the flexibility to access their data and applications from anywhere at any time, enabling more agile working methods. They also enable businesses to always keep their data and applications available, minimizing downtime and boosting customer satisfaction[6]. The main cloud deployment models are public cloud, private cloud, hybrid cloud, community cloud and multi-cloud.

- ***Public cloud:***
  In a public cloud, services are hosted on a shared infrastructure that is controlled and owned by a different service provider. The services security and availability are the provider's responsibility [5]-[8].
- ***Private cloud:***
  In a private cloud, services are hosted on infrastructure that the company itself owns and is in charge of maintaining. The organization is in charge of the upkeep security and accessibility of the services [6]-[8].
- ***Hybrid cloud:***
  Public and private cloud services that can be employed jointly or separately make up a hybrid cloud. In order to benefit from the best of both worlds, it enables enterprises to transfer workloads between the public and private cloud.[6]-[8].
- ***Community cloud:***
  In a community cloud computing paradigm, various organizations share a single cloud infrastructure. This enables businesses to take use of the public cloud's cost benefits and scalability while still maintaining control over their data and applications[8].
- ***Multi-Cloud:***
  Using numerous public cloud services from various cloud providers, a company uses a multi-cloud cloud computing model. As a result, businesses can take advantage of the cost reductions, scalability and flexibility offered by various cloud providers[8].

C. Cloud Service Delivery Models

User cost savings are offered by cloud service delivery models. Users may be able to cut costs on the hardware, software, and upkeep expenses related to conventional IT platforms, depending on the model selected. To safeguard user's data and apps from illegal access, it offers better security choices including data encryption and authentication. It also enables users to automate some procedures and processes, like provisioning and setup to improve efficiency. According to Fig.2, three fundamental service models are used to divide up cloud service delivery models.

- ***Software as a Service (SaaS):***
  This is the most well-liked form of cloud computing, in which internet-accessible apps are made available to consumers by cloud service providers. Typically subscription-based SaaS applications are managed and maintained by the cloud provider. Users can get access to a number of cloud-hosted applications. This makes the deployment procedure simpler and eliminates the need to install and maintain software on each end-user's device[1],[7]. SaaS also gives businesses the ability to scale up because customers can access the program whenever they need it and only pay for what they really use.

- ***Infrastructure as a Service (IaaS):***

  The most fundamental cloud computing model is this one. Users are in charge of deploying, operating and maintaining their apps and data, while IaaS providers manage and maintain the underlying infrastructure and software. Businesses can access all the advantages of cloud computing with the help of IaaS, which offers cloud infrastructure that comprises servers, storage, networking and other elements [1],[3],[9]. Scalability, cost reductions, and enhanced agility are IaaS's major benefits.

- ***Platform as a Service (PaaS):***

  In the PaaS paradigm, users have access to a development and deployment environment through cloud providers. PaaS is frequently used for web applications and cloud providers usually give users access to the frameworks and tools required for development and deployment. PaaS offers a platform for businesses to create, host and control cloud-based applications [1],[6],[9]. As a result, developers are free to concentrate on the application code without having to worry about maintaining the physical infrastructure. Because services like databases are already set up and ready to be used, PaaS also lessens the complexity of development.

- ***Anything as a Service:***

  Access to services, applications and resources can be obtained through the internet using this cloud service delivery architecture. It provides a range of services, including infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS) and storage as a service.

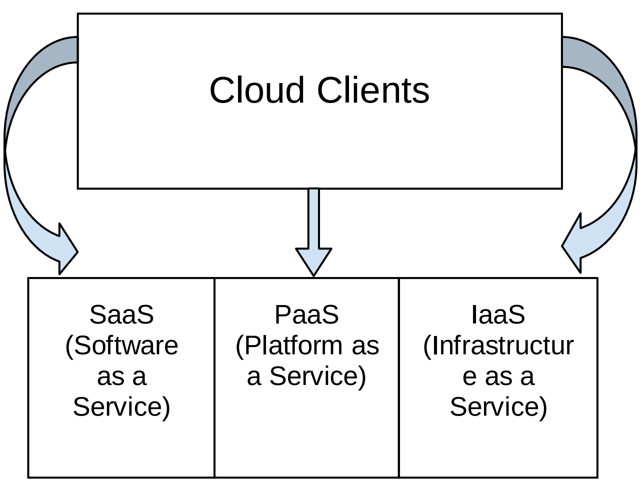

Figure 2: Cloud Service Delivery Models

D. Fault Tolerance

- ***Faults:***

Faults in cloud computing cause errors or interruptions in the normal operation of a cloud-based system. They can be caused by hardware issues, software bugs, or misconfigurations. Faults can lead to decreased performance and outages, as well as data loss and security vulnerabilities. Fault detection and recovery are important components of cloud computing, as they enable the cloud system to detect and respond to any errors or disruptions in its operations[3],[10]. Fault tolerance and resiliency are also important aspects of cloud computing, as they enable the system to continue to function despite any unexpected events.

- ***Classification of Faults:***

  - ***Omission Faults:*** Omission faults refer to errors or problems caused due to the lack of a certain feature, process, or action. These kinds of errors can happen when a person doesn't have access to a certain process or feature because they don't have the necessary rights or permissions, or when the process or feature isn't offered by the cloud service.

  - ***Aging Related***: Aging-related faults can be defined as any type of fault or failure caused by the gradual deterioration of cloud computing resources due to wear, usage, and other environmental factors such as Denial of services and Disk space full.

  - ***Response Faults:*** Response faults are software-related errors that occur when an application, service, or device fails to respond to a request in a timely manner. When a response fault occurs, users may experience slow loading times, timeouts, or errors such as Value faults and State transmission.

  - ***Software Faults:*** Software faults are errors, bugs, or issues that can occur in the cloud software during its execution or due to incorrect configuration, incorrect code and other causes. These faults can cause applications to crash and become vulnerable to security attacks, or produce incorrect results such as transient and intermittent.

  - ***Timing Faults:*** Timing faults occur when a cloud service does not deliver expected performance within the specified timeframe. These can include delays in service delivery, slow response times, or service unavailability due to system overload. They may result in a variety of problems, including degraded customer experience, decreased revenue and lost productivity such as early faults and late faults.

  - ***Miscellaneous:*** Miscellaneous faults are errors or problems that are not directly related to a specific system. They can range from user errors to hardware failures and may affect multiple systems such as permanent faults and incorrect design.

E. Fault Tolerance Approaches:

Fault tolerance is a crucial requirement for cloud computing environments. When designing a cloud system, fault tolerance is essential for increasing availability, scalability, and reliability. Fault tolerance approaches can include redundancy, replication, load-balancing and fault-tolerant algorithms in order to maintain the robustness of cloud computing [2],[3],[11],[13]. These techniques help to ensure that the cloud system is resilient and reliable, even in the face of faults and failures. The primary category of fault tolerance approaches identified in the literature are mentioned below:

- ***Reactive Fault Tolerance:*** Reactive fault tolerance (RFT) is a technique used in cloud computing to ensure the availability of services even when unexpected errors occur[3]. It maintains the robustness of the system and works by proactively detecting and repairing faults before they become service-impacting. Some of the reactive fault tolerance techniques are elaborated below:

- ***Check Pointing:*** It is based on the concept of saving the current state of an application periodically and restoring it when needed. [14],[15].
- ***Job Migration**:* If a job is not capable enough to complete its execution on some current physical machine, then the job can be migrated to another machine for the completion of its execution [16].
- ***Replication:*** With this technique, a cloud service provider creates multiple identical copies of data and applications and stores them on different servers [11],[15]. This ensures that if one server fails, the other copies are still available.
- ***S-Guard:*** It is based on the concept of recovery and rollback process for the successful execution at the time of failure[17].
- ***Retry**:* It involves the system retrying an operation in the event of a failure or timeout until it doesn't get successfully executed and use the same resources to retry[16].
- ***Task**: Resubmission:* This technique works by resubmitting the failed task multiple times until it reaches the desired result [11],[14].
- ***Rescue Workflow:*** It helps to ensure that any faults in the system are isolated from the rest of the system in order to prevent them from causing a system-wide failure and the system continues to work even after any job fails[16].
- ***Proactive Fault Tolerance**:* It is a technique that proactively detects potential fault conditions and takes corrective measures to prevent system outages. Some of the proactive fault tolerance techniques are elaborated below:
- ***Self-Healing:*** Self-healing technique uses divide and conquer approach to fault tolerance in cloud computing. It works by dividing the system into smaller parts and handling each part independently [3],[14],[18].
- ***Software Rejuvenation:*** It is a process of restarting the system periodically.For example, after a specific time interval or after a certain number of requests have been processed. With software rejuvenation, the system will automatically restart, refresh itself and begin from a new state every time, removing any potential bugs or errors[11],[16].
- ***Pre-emptive Migration:*** In this technique, applications are monitored for performance degradation and potential failures with the help of a feedback loop control approach and are preemptively migrated to other resources or instances in the cloud in order to reduce the impact of any failure[17].
- ***Load Balancing**:* Load balancing is a technique used to distribute workloads evenly across multiple processing nodes. In cloud computing, this technique is used to ensure that no single node is overloaded by transferring the extra load from the CPU to another CPU that doesn't exceed its maximum limit, thus improving performance and reliability[18].

III. MISCELLANEOUS FAULT TOLERANCE APPROACHES BASED ON MACHINE LEARNING

Table1: Advantages & Disadvantages of Miscellaneous Fault Tolerance Approaches based on Machine Learning

ML APPROACH	ADVANTAGE	DISADVANTAGE
Neural Network [21]	• Neural networks can handle complex patterns and relationships in data, making them suitable for fault prediction and detection. • They can adapt to changing environments and learn from experience, potentially improving fault tolerance over time.	• Training neural networks can be computationally expensive, especially for large datasets. • Neural networks are often considered black-box models, making it difficult to interpret their decisions, which can be a drawback in critical systems where transparency is necessary.
KNN (K-Nearest Neighbor)[22]	• KNN is simple to understand and implement, making it suitable for quick prototyping. • It can handle both classification and regression tasks and can be effective for fault prediction in distributed systems.	• KNN requires storing all training data, which can be memory-intensive, especially for large datasets. • Prediction time can be slow, particularly in high-dimensional spaces or with large training sets.
SVM (Support Vector Machine) [21, 23]	• SVMs work well in high-dimension spaces and are effective for both classification and regression tasks. • They are less prone to overfitting compared to some other algorithms.	• SVMs can be sensitive to the choice of kernel parameters and regularization. • They may not perform well with noisy data or when classes are heavily overlapping.
Reinforcement Learning [24]	• It can adapt to dynamic environments and learn optimal strategies through trial and error. • It can handle complex, multi-step decision-making	• Often require significant computational resources and time for training, especially for complex tasks. • They can be sensitive to the choice of reward

	processes, making it suitable for fault recovery and fault-tolerant control.	functions and exploration strategies, leading to suboptimal performance if not properly tuned.
Clustering [25, 26]	● It can uncover hidden patterns and structures in data without requiring labeled examples, making it suitable for unsupervised fault detection. ● It can provide insights into system behavior and identify potential fault clusters.	● Results can be sensitive to the choice of distance metrics and clustering algorithms. ● Determining the optimal number of clusters can be challenging, and the interpretation of clusters may require domain expertise.
Meta-Heuristics [27, 28]	● Can efficiently explore complex solution spaces and find near-optimal solutions to combinatorial optimization problems. ● They can be applied to a wide range of optimization problems without requiring explicit problem-specific knowledge.	● It may not guarantee finding global optimum and can stuck at a local one. ● Often require fine-tuning of parameters and may not scale to very large problem instances.

IV. RELATED WORK

ASSERTED MODEL	PROPOSED BY	TYPE OF APPROACH	STRENGTH	WEAKNESS
SVM-Grid Fault Detection	Pie Yun Zhang et al.[44]	Proactive Approach	● Effectively combines feature selection and classifier learning for fault detection in cloud computing systems.. ● Utilizes SVMs to accurately detect and predict abnormal behaviors, improving fault prediction performance.	● Requires careful tuning of SVM parameters and grid selection, which may affect detection accuracy. ● Dependency on the quality of training data for SVM model construction.
PCFT (Proactive Co-ordinated Fault Tolerance)	Jialei Liu et al. [45]	Proactive Approach	● Automatically migrates virtual machines to ideal target physical machines, improving service availability and reducing downtime. ● Outperforms alternative strategies in terms of execution speed and transmission overhead.	● Complexity in coordinating and harmonizing VM migrations may introduce overhead. ● Dependency on accurate monitoring and prediction of system faults for proactive measures.
EDCKP (Edge Switch Failure Aware Checkpointing)	Zhou et al. [46]	Reactive Approach	● Improves the dependability of cloud computing services by creating checkpoint records at the edge of the cloud infrastructure. ● Effective in minimizing downtime and ensuring service continuity in the event of switch failures.	● Relies on the accurate detection and handling of edge switch failures, which may not cover all potential failure scenarios. ● Deployment and management of check pointing infrastructure may introduce additional complexity and resource overhead.
ICFWS (Fault Tolerance Workflow Scheduling)	G. Yao et al. [47]	Reactive Approach	● Combines replication, fault detection, recovery, and load balancing techniques for fault tolerance in large-scale distributed computing systems. ● Offers flexibility in choosing replication or resubmission strategies based on task-specific sub-deadlines.	● Complexity in task breakdown and fault tolerance strategy selection may increase computational overhead. ● Reliance on accurate task-specific deadlines and workload distributions for effective scheduling.
OPVMP (Optimal Redundant Virtual Machine Placement)	S. Wang et al. [48]	Reactive Approach	● Maximizes cloud service availability and resiliency by optimally placing redundant virtual machines. ● Efficiently balances load across cloud	● Requires heuristic algorithms for optimal placement, which may not always guarantee the best solution.

			services and facilitates rapid service recovery in case of failures.	● Complexity in managing redundant VMs and resource allocation may increase management overhead.
KNF (k-out-of-n Reliability Framework)	Chen et al. [49]	Reactive Approach	● Provides fault tolerance and energy efficiency by structuring systems with redundant components. ● Ensures system operation even if a subset of components fail, improving overall system reliability.	● Dependency on the appropriate choice of k and n values may lead to under or over-provisioning of resources. ● Increased complexity in system design and management due to redundancy and fragmentation of data.
ROCloud (Reliability-based Design Optimization)	W. Qiu et al. [50]	Reactive Approach	● Enables reliable migration of legacy applications to the cloud by providing fault-tolerant design patterns and automated reliability analysis tools. ● Facilitates efficient and reliable cloud application design through fault-tolerant strategy selection and component assessment.	● Dependency on accurate reliability analysis and design optimization may require substantial computational resources. ● Complexity in selecting and implementing fault-tolerant strategies for different application components and architectures.

V. FUTURE AREAS FOR RESEARCH

- Developing methods to improve fault tolerance of applications running in the cloud, such as by leveraging checkpoint-restart techniques, distributed computing, and other approaches.
- Developing distributed protocols to increase the fault-tolerance of cloud services, such as those related to replication and self-healing.
- Developing software-defined infrastructure for cloud platforms that are resilient to faults and can quickly detect and respond to various types of failure.
- Developing methods and algorithms that can dynamically adapt the fault-tolerance strategies of cloud services based on changing workloads and system requirements.
- Developing methods to detect faults in cloud services and automatically recover from them without manual intervention.
- Developing approaches to incorporate security into the fault-tolerance mechanisms of cloud services.

Some Domains on which the research need to be done so that we can increase the performance level and efficiency of the system are as follows:

A. Deep Learning [40][41]:

It is the process of training a computer to recognize patterns and make decisions about complex data sets. It is predicated on the notion of a neural network, which is a collection of algorithms that resembles the composition and operation of the human brain. Deep learning algorithms are extremely accurate and effective tools for AI applications because they process data using numerous layers of neurons. Deep learning has several applications including machine translation, natural language processing and picture recognition. Enhancing cloud computing fault tolerance can benefit greatly from deep learning. Deep learning algorithms can be used to identify and detect errors, anomalies and potential failures in a cloud computing system. This helps to prevent and mitigate unexpected outages, ensuring the high availability of cloud services. Deep learning can also be used to detect malicious activities, helping to secure cloud infrastructure from cyber-attacks. Deep learning algorithms such as convolutional neural networks (CNNs) is used to analyze large datasets like log files and system performance metrics to detect anomalies in the system. Using deep learning algorithms, root cause of an issue can be diagnosed. This could include natural language processing (NLP) methods to analyze customer feedback, or unsupervised learning algorithms to find patterns in log files. Deep learning algorithms such as recurrent neural networks (RNNs) are used to predict when faults are likely to occur in the future. This could help to identify potential problems before they become an issue. Additionally, deep learning can be utilized to optimize resource allocation in cloud computing, enabling efficient utilization of resources and minimizing downtime.

B. Blockchain [42][43]:

A blockchain is a distributed digital ledger that records transactions across many computers. It is used to store and track data such as financial transactions and digital assets. The data stored on a blockchain is cryptographically secured and immutable, meaning it can't be changed or manipulated. This makes it an ideal medium for recording and tracking data that needs to be secure and trustworthy. Blockchain technology can be used to provide fault tolerance for cloud computing by using smart contracts. Smart contracts can be used to trigger automated processes in the event of a system failure such as data replication, failover and rollback. By leveraging the decentralized, immutable and transparent nature of blockchain, cloud computing can be made more reliable and secure. Smart contracts can also be used to ensure that data is not tampered with and to ensure that the cloud computing system is running as expected. Additionally, blockchain technology can be used to provide access control and authentication to cloud computing resources, ensuring that only authorized users can access the system. It can be used to check the authenticity of each block details even when no centralized authority is present. It allows cloud service providers to detect and record faults in the cloud environment in a transparent and secure manner. This allows cloud service providers to detect and respond to faults quickly and accurately to minimize disruption and downtime.

VI. CONCLUSION

Cloud computing is spreading across many industries because of its ability to provide computing services like servers, storage, databases, networking, software and analytics. These services enable speedier innovation, adaptable resources and scale economies. It does this by providing computing services such as servers, storage, databases, networking, software and analytics. It provides an agile, cost-effective way to build and manage applications but there still exist failures that need to be encountered. Fault tolerance in Cloud computing is to ensure that the system and applications are protected from hardware or software failures, ensuring continuous service availability and data integrity. By enabling redundancy, which enables the system to continue operating even when a component fails. Fault tolerance raises the reliability of a cloud system. It also helps to ensure that data is protected from potential corruption and loss.

The principle components, service models and deployment strategies of cloud computing have all been looked at in this survey study. Several different sorts of faults, fault tolerance techniques, and models have been covered in this study in order to overcome the faults to make computing more trustworthy for the users. Further, to increase the working of fault tolerant systems, some of the approaches have also been covered. The survey also marked some future directions of research as well as the related work in this domain to exponentially increase the efficiency and effectiveness of computing systems.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] M. U. Bokhari, Q. M. Shallal, and Y. K.Tamandani, "Cloud computing service models: A comparative study," in 2016 3rd International Conference on Computing for Sustainable Global Development(INDIACom). IEEE, 2016, pp. 890–895.B. Rieder, Engines of Order: A Mechanology of Algorithmic Techniques. Amsterdam, Netherlands: Amsterdam Univ. Press, 2020.

[2] M. K. Gokhroo, M. C. Govil, and E. S. Pilli, "Detecting and mitigating faults in cloud computing environment," in 2017 3rd International Conference on Computational Intelligence & Communication Technology(CICT). IEEE, 2017, pp. 1–9.

[3] L. P. Saikia and Y. L. Devi, "Fault tolerance techniques and algorithms in cloud computing," International Journal of Computer Science & Communication Networks, vol. 4, no. 1, pp. 01–08, 2014.

[4] E. Dubrova et al., "Fault tolerant design: An introduction," Department of Microelectronics and Information Technology, Royal Institute of Technology, Stockholm, Sweden, pp. 22–3, 2008.

[5] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp.200–222, 2016.

[6] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in 2009 Fifth International Joint Conference on INC, IMS and IDC. IEEE 2009, pp. 44–51.

[7] S. Patidar, D. Rane, and P. Jain, "A survey paper on cloud computing," in 2012 second international conference on advanced computing & communication technologies. IEEE, 2012, pp. 394–398.

[8] L. Savu, "Cloud computing: Deployment models, delivery models, risks and research challenges," in 2011 International Conference on Computer and Management (CAMAN). IEEE, 2011, pp. 1–4.

[9] E. AbdElfattah, M. Elkawkagy, and A. El-Sisi, "A reactive fault tolerance approach for cloud computing," in 2017 13th International Computer Engineering Conference (ICENCO). IEEE, 2017, pp. 190–194.

[10] Y. M. Essa, "A survey of cloud computing fault tolerance: techniques and implementation," International Journal of Computer Applications, vol. 138, no. 13,2016.

[11] Z. Amin, H. Singh, and N. Sethi, "Review on fault tolerance techniques in cloud computing," International Journal of Computer Applications, vol. 116, no. 18, 2015.

[12] Z. Amin, H. Singh, and N. Sethi, "Review on fault tolerance techniques in cloud computing," International Journal of Computer Applications, vol. 116, no. 18, 2015.

[13] M. N. Cheraghlou, A. Khadem-Zadeh, and M. Haghparast, "A survey of fault tolerance architecture in cloud computing," Journal of Network and Computer Applications, vol. 61, pp. 81–92, 2016.

[14] S. M. Ataallah, S. M. Nassar, and E. E. Hemayed, "Fault tolerance in cloud computing-survey," in 2015 11th International computer engineering conference (ICENCO). IEEE, 2015, pp. 241–245.

[15] I. Mahallat, "Fault-tolerance techniques in cloud storage: a survey," Int J Database Theory Appl, vol. 8, no. 4, pp. 183–190, 2015.

[16] S. Prathiba and S. Sowvarnica, "Survey of failures and fault tolerance in cloud," in 2017 2nd International Conference on Computing and Communications Technologies (ICCCT). IEEE, 2017, pp. 169–172.

[17] A. Bala and I. Chana, "Fault tolerance-challenges, techniques and implementation in cloud computing," International Journal of Computer Science Issues (IJCSI), vol. 9, no. 1, p. 288, 2012.

[18] J. Park, G. Yoo, and E. Lee, "Proactive self-healing system based on multi-agent technologies," in Third ACIS Int'l Conference on Software Engineering Research, Management and Applications(SERA'05). IEEE, 2005, pp. 256–263.

[19] Macskassy, S.A., Provost, F., 2007. A brief survey of machine

learning methods for classification in networked data and an application to suspicion scoring. In Statistical network analysis: models, issues, and new directions. Springer, Berlin, Heidelberg, pp. 172–175.

[20] Li-qun, Z., Shu-chen, L., Cheng-li, S., Chun-yan, Z., 2011. Fault-tolerant control algorithm of neural network based on Particle Swarm Optimization. In: Control and Decision Conference (CCDC), 2011 Chinese. IEEE, pp. 700–704.

[21] Trivedi, M., 2016. A survey on resource provisioning using machine learning in cloud computing. Int. J. Eng. Dev. Res. 4 (4), 546–549.

[22] Sharma, S., 2017. Enhance data security in cloud computing using machine learning and hybrid cryptography techniques. Int. J. Adv. Res. Comput. Sci. 8 (9), 393–397.

[23] [23] He, Z., Zhang, T., Lee, R.B., 2017. Machine learning based DDoS attack detection from the source side in the cloud. In: Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on. IEEE, pp. 114–120.

[24] Shaw, R., Howley, E., Barrett, E., 2017. An Advanced Reinforcement Learning Approach for Energy-Aware Virtual Machine Consolidation in Cloud Data Centers, pp. 61–66.

[25] Buyya, R. et al., 2009. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Futur. Gener. Comput. Syst. 25 (June 2009), 17.

[26] Patil, A., Shah, A., Gaikwad, S., Mishra, A.a., Kohli, S.S., Dhage, S., 2011. Fault Tolerance in Cluster Computing System. In: 2011 Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput., pp. 408–412.

[27] Frincu, M.E., Craciun, C., 2011. Multi-objective meta-heuristics for scheduling applications with high availability requirements and cost constraints in multi-cloud environments. In: Proc. - 2011 4th IEEE Int. Conf. Util. Cloud Comput. UCC 2011, pp. 267–274.

[28] Umamakeswari, P.V.M.D.A., Shaileshdheep, S.G.B.G., Aishwarya, V.,Subramanian, E.R.S., 2017. A study of various meta heuristic algorithms for scheduling in cloud. Int. J. Pure Appl. Math. 115 (7), 205–208.

[29] Blum, C., Roli, A., 2003. Metaheuristics in combinatorial optimization: overview and conceptual comparison. ACM Comput. Surv. 35 (3), 189–213.

[30] Liu, H., Xu, D., Miao, H., 2011. Ant colony optimization based service flow scheduling with various QoS requirements in cloud computing. In: First ACIS International Symposium on Software and Network Engineering. IEEE, pp. 53–58.

[31] Pandey, S., Wu, L., Guru, S.M., Buyya, R., 2010. A particle swarm optimization-based heuristic for scheduling workflow applications in cloud computing environments. In: 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 400–407.

[32] Kruekaew, B., Kimpan, W., 2014. Virtual machine scheduling management on cloud computing using artificial bee colony. Proc. Int. MultiConf. Eng. Comput. Sci. 1, 12–14.

[33] Liu, Y., Muppala, J.K., Veeraraghavan, M., Lin, D., Hamdi, M., 2012. Data center networks: topologies, architectures and fault-tolerance characteristics. Springer Science & Business Media.

[34] https://www.slideshare.net/AnujaJoshi6/cuckoo-o-ptimization-ppt (available online 2018).

[35] Yang, X.S., He, X., 2013. Firefly algorithm: recent advances and applications, pp. 1–14. arXiv preprint arXiv:1308.3898.

[36] Haider, S., Nazir, B., 2017. Dynamic and adaptive fault tolerant scheduling with QoS consideration in computational grid. IEEE Access 5, 7853–7873.

[37] Hamad, S.A., Omara, F.A., 2016. Genetic-based task scheduling algorithm in cloud computing environment. Int. J. Adv. Comput. Sci. Appl. 7 (4), 550–556.

[38] Rani, A., 2016. Proposed model for multi-objective differential evolution (mode) in cloud computing. Int. J. Adv. Res. Innovative Ideas Educ. 3, 4119–4124.

[39] Tsai, J.T., Fang, J.C., Chou, J.H., 2013. Optimized task scheduling and resource allocation on a cloud computing environment using an improved differential evolution algorithm. Comput. Oper. Res. 40 (12), 3045–3055.

[40] Qiu, F., Zhang, B., Guo, J., 2016. A deep learning approach for VM workload prediction in the cloud. In: 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE, pp. 319–324.

[41] Cheng, M., Li, J., Nazarian, S., 2018. DRL-cloud: deep reinforcement learning-based resource provisioning and task scheduling for cloud service providers. In: Proceedings of the 23rd Asia and South Pacific Design Automation Conference. IEEE Press, pp. 129–134.

[42] Tosh, D.K., Shetty, S., Liang, X., Kamhoua, C.A., Kwiat, K.A., Njilla, L., 2017. Security implications of blockchain cloud with analysis of block withholding attack. In: Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press, pp. 458–467.

[43] Park, J.H., Park, J.H., 2017. Blockchain security in cloud computing: use cases, challenges, and solutions. Symmetry 9 (8), 164.

[44] P. Zhang, S. Shu, and M. Zhou, “An online fault detection model and strategies based on svm-grid in clouds,” IEEE/CAA Journal of Automatica Sinica, vol. 5, no. 2, pp. 445–456, 2018.

[45] J. Liu, S. Wang, A. Zhou, S. A. Kumar, F. Yang, and R. Buyya, “Using proactive fault-tolerance approach to enhance cloud service reliability,” IEEE Transactions on Cloud Computing, vol. 6, no. 4, pp. 1191–1202, 2016.

[46] A. Zhou, Q. Sun, and J. Li, “Enhancing reliability via checkpointing in cloud computing systems,” China Communications, vol. 14, no. 7, pp. 1–10, 2017.

[47] G. Yao, Y. Ding, and K. Hao, “Using imbalance characteristic for fault-tolerant workflow scheduling in cloud systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 28, no. 12, pp. 3671–3683, 2017.

[48] A. Zhou, S. Wang, B. Cheng, Z. Zheng, F. Yang, R. N. Chang, M. R. Lyu, and R.Buyya, “Cloud service reliability enhancement via virtual machine placement optimization,” IEEE Transactions on Services Computing, vol. 10, no. 6, pp. 902–913, 2016.

[49] C.-A. Chen, M. Won, R. Stoleru, and G. G. Xie, “Energy-efficient fault-tolerant data storage and processing in mobile cloud,” IEEE Transactions on cloud computing, vol. 3, no. 1, pp. 28–41, 2014.

[50] W. Qiu, Z. Zheng, X. Wang, X. Yang, and M. R. Lyu, “Reliability-based design optimization for cloud migration,” IEEE Transactions on Services Computing, vol. 7, no. 2, pp. 223–236, 2013.

ABOUT THE AUTHORS

Shreya Rai is a dedicated Information Technology undergraduate currently pursuing a Bachelor's degree. Hailing from India, her early fascination with technology led her to explore the dynamic world of IT. At Babu Banarasi Das Northern India Institute of Technology, Lucknow Shreya Rai has excelled in coursework, focusing on areas such as Network Computing, Computer Architecture, Software Engineering, Compiler Design, Data Structures, and Database Management Systems. She has achieved Rank-1 in the Engineering College Case Study Competition of the CSI chapter in Lucknow city. Her idea for innovation was selected for the IDE boot camp organized by AICTE for our pitch presentation. In the college, she holds the post of Vice-Chair of IEEE responsible for organizing and managing events and Chairperson of Women in Engineering branch.

Ram Pratap received Ph.D. (Computer Science & Engineering) in 2019, M. Tech. (Information Technology) in 2011. He has teaching and research experience of 19 years. Presently he is working as a associate professor in the department of Information Technology at Babu Banarasi Das Northern India Institute of Technology, Lucknow since 2021. He has also worked as an Assistant Professor in the Depratment of MCA at Shri Ram Swaroop Memorial College of Engg. And Management, LKO from Jan 2013 to Aug 2021 and as a Senior Lecturer at Kali Charan Nigam Institute of Technology, Banda from Aug, 2004 to Jan 2013.His teaching interest includes Cloud Computing, Introduction to Automata Theory and Formal Languages, Database Management Systems, Software Engineering, Compiler Design, Data Mining and Warehousing, Mobile Computing and Internet of Things. His research interest includes Cloud Computing and Mobile Computing. He has 06 publications in journals and conferences of international/national repute.

Shaba Irram is M. Tech in Computer Science & Engineering from Integral University, Lucknow, U.P. 2019. She works as Assistant Professor in IT department of BBDNIIT, Lucknow. She has a working experience of 9 years. She has Published Research Paper: Shaba Irram " Research on Object Detection in Video Streaming Using Deep Learning" International Journal of Computational Engineering Research (IJCER), vol. 09, no.7, 2019, pp 34-43. She has Published Review Paper: Shaba Irram "Object Detection in Video Streaming Using Deep Learning" International Journal of Computer Science Trends and Technology (IJCST) – Volume 7 Issue 6, Nov - Dec 2019.